Monedele virtuale: între obținerea datelor privind tranzacțiile financiare și luarea măsurilor asigurătorii în procesul penal

Conf. univ. dr. Andra-Roxana Trandafir
Facultatea de Drept, Universitatea din București

Dr. George Zlati
Cadru didactic asociat la Facultatea de Drept și Științe Sociale
Universitatea „1 Decembrie 1918" din Alba Iulia

Rezumat: *În prezentul articol sunt analizate aspectele de ordin tehnic și juridic relevante în contextul procesului de indisponibilizare a monedelor virtuale în procesul penal. În acest context, după clarificarea din punct de vedere conceptual a mai multor noțiuni, este mai întâi prezentat mecanismul prin intermediul căruia se pot obține, în cursul procesului penal, informații cu privire la tranzacțiile cu monedă virtuală sau titularul acestora. De asemenea, este abordată problematica indisponibilizării efective a monedelor virtuale, prin accesarea portofelului digital și efectuarea unei tranzacții cu monedă virtuală la o adresă publică aflată sub controlul organului de urmărire penală ori al ANABI, precum și modalitatea de valorificare a monedelor virtuale.*

Cuvinte cheie: *măsură asigurătorie, monede virtuale, criptoactive, blockchain, portofel digital, adresă publică, acces la un sistem informatic, percheziție informatică, instituție financiară.*

Virtual currencies: between obtaining data regarding financial transactions and freezing of assets during the criminal trial

Abstract: *The paper analyses the technical and legal aspects relevant during the complex process of freezing virtual currencies in a criminal trial. In this context, after the clarification of the relevant terminology, the authors explain the mechanism through which data and information regarding virtual currencies transactions or their owner can be obtained. The authors also explain the manner in which the freezing of virtual currencies can be implemented, by accessing the digital wallet and performing a transaction to a public address controlled by the criminal investigation body or by the National Agency for the Management of Seized Assets (ANABI), as well as the way in which virtual currencies can be sold later on.*

Key words: *freezing of assets, virtual currencies, crypto assets, blockchain, digital wallet, public address, access to a computer system, computer search, financial entity.*

Foarte multe dintre dezbaterile din ultima vreme au în vedere problematici legate de monedele virtuale. Fie că vorbim despre calificarea naturii juridice a acestora, despre necesitatea reglementării la nivel național sau internațional, despre caracterul speculativ al tranzacțiilor cu monede virtuale, multe conferințe, seminare ori lucrări de specialitate dedică acestui subiect timp generos. Științele penale nu scapă, în mod evident, acestei tentații. În acest context, ne-am propus să analizăm câteva probleme practice legate de monedele virtuale, în special în materia măsurilor asigurătorii.

Pentru a putea analiza respectivele probleme, vom realiza, mai întâi, câteva clarificări preliminare (**I**). Ulterior, vom arăta în ce condiții pot fi obținute date și informații despre tranzacțiile efectuate cu monedă virtuală (**II).** Pentru a putea vedea care este măsura asigurătorie care se înființează în concret asupra monedelor virtuale, vom aminti câteva aspecte despre natura și scopul măsurilor asigurătorii în procesul penal (**III**). În final, vom trata, în concret, cum se realizează aducerea la îndeplinire a măsurilor asigurătorii (**IV**), precum și modalitatea în care monedele virtuale supuse unor astfel de măsuri pot fi ulterior valorificate de organele competente (**V**).

Întrucât nu vom trage o concluzie la finalul acestui material, ne mărginim să afirmăm, încă de la acest moment, că, aflându-ne pe un tărâm nou, multe din aspectele ce vor fi tratate în cele ce urmează sunt încă sub semnul discuției și vor putea fi, cu siguranță, dezvoltate în materiale ulterioare.

I. CLARIFICĂRI PRELIMINARE

Pentru a înțelege complexitatea instituirii unei măsuri asigurătorii cu privire la monedele virtuale, este necesar să clarificăm mai întâi următoarele aspecte: ce sunt monedele virtuale (**1**), care este natura juridică a monedelor virtuale (**2**), unde este stocată și cum este tranzacționată moneda virtuală (**3**), cine este deținătorul monedelor virtuale (**4**), cum se poate cuantifica valoarea unei monede virtuale (**5**); ce informații pot fi vizualizate în blockchain (**6)** și ce date ar putea fi oferite de către CEX, DEX sau furnizorul de portofele digitale (**7**).

1. Raportul dintre moneda virtuală, criptoactive și moneda electronică

Precizăm încă de la început că doar monedele virtuale și monedele electronice beneficiază, de *lege lata,* de o definiție în dreptul intern.

A. Astfel, **monedele virtuale** sunt definite la art. 180 alin. (4) C.pen. și la art. 2 lit. t[1]) din Legea nr. 129/2019 pentru prevenirea și combaterea spălării banilor și finanțării terorismului, precum și pentru modificarea și completarea unor acte normative[1].

Cele două definiții sunt identice, fiind transpuneri *verbatim* a unor directive[2]. Potrivit acestor definiții legale, moneda virtuală înseamnă *o reprezentare digitală a valorii care nu este emisă sau garantată de o bancă centrală sau de o autoritate publică, nu este în mod obligatoriu legată de o monedă instituită legal și nu deține statutul legal de monedă sau de*

[1] Publicată în M.Of. nr. 589 din 18 iulie 2019.

[2] Art. 180 alin. (4) C.pen. a transpus Directiva (UE) 2019/713 privind combaterea fraudelor și a contrafacerii în legătură cu mijloacele de plată fără numerar și de înlocuire a Deciziei-cadru 2001/413/JAI. În schimb, art. 2 lit. t[1]) din Legea nr. 129/2019 a transpus Directiva (UE) 2015/849 privind prevenirea utilizării sistemului financiar în scopul spălării banilor sau finanțării terorismului, modificată prin Directiva (UE) 2018/843 [AML5 – n.n.].

bani, dar este acceptată de către persoane fizice sau juridice ca mijloc de schimb și poate fi transferată, stocată și tranzacționată electronic. Rezultă așadar următoarele trăsături ale monedelor virtuale:

i. Monedele virtuale sunt o **reprezentare digitală a valorii**.

ii. Monedele virtuale **nu sunt emise sau garantate de o bancă centrală sau de o autoritate publică**. Înțelegem de aici faptul că emitentul de monedă virtuală nu trebuie să fie în mod obligatoriu o bancă centrală sau o autoritate publică. Cu toate acestea, nu este exclusă posibilitatea ca aceste entități să emită monedă virtuală[3] – îndeosebi monede virtuale non-volatile sau stabile (în eng., *stablecoins*)[4].

iii. Monedele virtuale **nu sunt în mod obligatoriu legate de o monedă instituită legal**. Înțelegem de aici că unele monede virtuale pot să fie legate de o monedă fiduciară. Avem în vedere aici monedele virtuale non-volatile precum USD Tether (USDT) sau USD Coin (USDC). În cazul acestora discutăm despre o paritate de 1:1 cu dolarul american. Faptul că o monedă virtuală este legată de o monedă fiduciară nu îi schimbă natura juridică – aceasta nu devine monedă fiduciară. Așa cum urmează a arăta *infra*, între monedele virtuale (inclusiv cele non-volatile) și cele electronice există deosebiri clare.

Există inclusiv monede virtuale non-volatile legate de alte criptoactive (e.g. alte monede virtuale decât cele menționate anterior, instrumente financiare, mărfuri etc.). Un exemplu în acest sens este moneda virtuală non-volatilă DAI.

iv. Monedele virtuale **nu dețin statutul de monedă sau de bani**. Înțelegem de aici că monedele virtuale nu intră în categoria monedelor fiduciare, motiv pentru care nu reprezintă mijloace de plată general acceptate în circuitul civil. Aceasta nu înseamnă că în anumite jurisdicții, unele monede virtuale nu pot deveni prin efectul legii un mijloc legal de plată. Totuși, cel puțin în România, de *lege lata*, putem discuta despre monedele virtuale (inclusiv cele stabile) ca fiind exclusiv un mijloc de schimb.

v. Monedele virtuale **pot fi acceptate de către o persoană fizică sau juridică ca mijloc de schimb.** Raportat la cele menționate *supra*, la pct. iv, trebuie înțeles că monedele virtuale pot să fie utilizate ca mijloc de schimb, nu ca mijloc de plată. Acceptarea unor monede virtuale (e.g. bitcoin) ca mijloc legal de plată în unele jurisdicții ar putea genera complicații în ceea ce privește calificarea juridică. Totuși, cel puțin în momentul de față, o monedă virtuală poate face obiectul unei vânzări doar atunci când în schimbul monedei virtuale se primește o

[3] De altfel, se discută deja despre monedele virtuale CBDC (Cental Bank Digital Currency) ce urmează să fie emise în blockchain de către băncile naționale (e.g. BNR), federale sau regionale (e.g. Banca Centrală Europeană). A se vedea *F. Penetta*, A digital euro that serves the needs of the public: striking the right balance, 30 martie 2022, discurs disponibil pe pagina https://www.ecb.europa.eu/press/key/date/2022/html/ecb.sp220330_1~f9fa9a6137.en.html [ultima accesare în data de 02.04.2022].

[4] În esență, acestea sunt monede virtuale care au o paritate de 1:1 cu dolarul american sau o altă monedă fiduciară. Exemple de monede virtuale stabile sunt următoarele: USDT (USD Tether), USDC (USD Coin), DAI etc. Pentru o analiză *in extenso* a acestor monede virtuale se poate vedea *C. Calcaterra, W.A. Kaal, V. Rao*, Stable Cryptocurrencies: First Order Principles, în Stanford Journal of Blockchain Law & Policy, vol. 3, nr. 1/2020, pp. 62 și urm. Unele monede virtuale stabile sunt garantate de alte active (monede fiduciare, alte criptoactive, bunuri etc.), în timp ce altele folosesc un algoritm (monede virtuale stabile algoritmice) pentru menținerea valorii de referință. Aceste din urmă monede virtuale se pot dovedi riscante – de exemplu, moneda virtuală UST (US Terra) și-a pierdut paritatea cu dolarul american în contextul unor manipulări pe piața criptoactivelor, iar în mai puțin de 7 zile a generat o pierdere de aproximativ 10 miliarde de dolari (a se vedea *D. Van Boom*, Luna Crypto Crash: How UST Broke and What's Next for Terra, 25.05.2022 material disponibil pe pagina https://www.cnet.com/personal-finance/crypto/luna-crypto-crash-how-ust-broke-and-whats-next-for-terra/).

monedă fiduciară. În acest caz discutăm despre vânzarea unui activ, anume moneda virtuală, contraprestația cumpărătorului fiind plata prețului într-o monedă fiduciară. În toate celelalte cazuri vom discuta despre un contract de schimb – e.g. schimbul între o monedă virtuală (e.g. 1 bitcoin) și o altă monedă virtuală (e.g. 116.2 ether), sau între o monedă virtuală (e.g. 1 bitcoin) și un alt bun (e.g. o mașină).[5]

vi. Moneda virtuală **poate fi transferată, stocată și tranzacționată electronic**. Așa cum vom vedea *infra*, moneda virtuală este stocată în blockchain. De asemenea, aceasta poate să fie tranzacționată prin intermediul unor platforme de tranzacționare centralizate (CEX), descentralizate (DEX) sau direct prin intermediul unor portofele digitale non-custodiale (în eng., *non-custodial digital wallet*). Despre ipotezele particulare ce intră în accepțiunea noțiunii de *tranzacționare* vom discuta *infra.* Precizăm, încă de la acest moment, că avem unele rezerve cu privire la teza *transferului* de monedă virtuală. Chiar dacă inclusiv art. 250 alin. (1) C.pen. raportează la conduita de a transfera monedă virtuală, în realitate discutăm despre o tranzacționare ce nu implică o relocare a datelor informatice. Astfel, așa cum urmează a vedea *infra*, o tranzacție cu monedă virtuală de la adresa publică X la adresa publică Y nu se transpune într-un transfer de date informatice. Prin urmare, dacă dorim să discutăm despre un transfer, acesta se raportează mai degrabă la drepturile patrimoniale asociate monedei virtuale tranzacționate.

B. Monedele electronice sunt definite la art. 180 alin. (3) C.pen. și art. 4 alin. (1) lit. f) din Legea nr. 210/2019 privind activitatea de emitere de monedă electronică[6]. Potrivit definițiilor legale, moneda electronică reprezintă o *valoare monetară stocată electronic, inclusiv magnetic, reprezentând o creanță asupra emitentului, emisă la primirea fondurilor în scopul efectuării de operațiuni de plată și care este acceptată de o persoană, alta decât emitentul de monedă electronică*. Rezultă așadar următoarele trăsături ale monedelor electronice[7]:

i. Moneda electronică reprezintă **o valoare monetară stocată electronic sau magnetic**. Așadar, spre deosebire de monedele virtuale, nu discutăm doar despre reprezentarea digitală a unei valori, ci despre o veritabilă valoare monetară.

ii. Moneda electronică **reprezintă o creanță asupra emitentului**, emisă la primirea fondurilor. Înțelegem de aici faptul că deținătorul de monedă electronică dobândește un drept de creanță asupra emitentului monedei electronice, putând în orice moment să solicite conversia din moneda electronică în bani sau monedă de cont.

În cazul monedelor virtuale nu putem discuta despre un asemenea drept de creanță. Chiar dacă uneori am putea identifica emitentul de monedă virtuală,[8] titularul de monedă virtuală nu va avea un drept de creanță asupra acestuia. Un asemenea drept de creanță nu există nici măcar în raport cu emitentul de monedă virtuală non-volatilă. Dacă vrem să discutăm despre un drept de creanță, acesta ar putea exista doar în raport cu o platformă de

[5] A se vedea *L. Bercea*, „Prețul constă într-o sumă de bani". De la moneda de cont la „moneda" virtuală (și înapoi), în Revista română de drept privat, nr. 3/2017, p. 73.
[6] Publicată în M.Of. nr. 914 din 13 noiembrie 2019.
[7] A se vedea și A se vedea și *G. Zlati,* Tehnologia blockchain, monedele virtuale și dreptul penal, în Penalmente Relevant, nr. 1/2021, pp. 27-29.
[8] Afirmăm că „uneori" deoarece, cel puțin în cazul bitcoin, este dificil să discutăm despre un emitent persoană fizică sau juridică. De asemenea, în cazul recompenselor primite pentru participarea la mecanismul de consens proof-of-work (PoW) sau proof-of-stake (PoS), unitățile de valoare ale diferitelor monede virtuale sunt generate în mod automat în bazul unui algoritm prestabilit.

tranzacționare centralizată (CEX) ce deține monedele virtuale în custodie, în numele clientului.

iii. Moneda electronică este **emisă în scopul efectuării de operațiuni de plată**. Astfel, dacă moneda virtuală este un mijloc de schimb, moneda electronică este un veritabil mijloc legal de plată.

iv. Moneda electronică **este acceptată ca mijloc legal de plată**.

Dincolo de cele învederate *supra*, este important a preciza faptul că moneda electronică poate fi emisă doar de entitățile menționate la art. 2 alin. (1) din Legea nr. 210/2019. Discutăm așadar despre un regim strict cu privire la emiterea de monedă electronică, aplicabil instituțiilor de credit, diferitor instituții financiare ori autorități publice.

C. Criptoactivele nu se regăsesc definite de *lege lata* în legislația națională. Totuși, potrivit art. 3 alin. (2) din Propunerea de Regulament privind piețele criptoactivelor și de a modificare a Directivei (UE) 2019/1937 [propunerea de regulament MiCA[9]], un criptoactiv înseamnă *o reprezentare digitală a valorii sau a drepturilor care pot fi transferate și stocate electronic, utilizând tehnologia registrelor distribuite sau o tehnologia similară.*

Raportat la toate aceste definiții legale este necesar să concluzionăm, într-o primă fază, asupra următoarelor chestiuni:

i. **Toate monedele virtuale pot fi calificate drept criptoactive**, însă **nu toate criptoactivele sunt monede virtuale.** Cu titlu de exemplu, un NFT (*non-fungible token*) este un criptoactiv, dar nu este o monedă virtuală.[10] O asemenea delimitare rezultă din definiția criptoactivelor, ce se raportează nu doar la reprezentarea digitală a unei valori, ci inclusiv la drepturi transferabile – de e.g., în legătură cu exploatarea conținutului unui NFT.

ii. Monedele virtuale se deosebesc semnificativ de monedele electronice. Evitând o analiză *in extenso* pe acest subiect, prezintă relevanță următoarele:

- **o monedă virtuală nu este un mijloc legal de plată, ci un mijloc de schimb;**
- o monedă virtuală **nu reprezintă o creanță asupra emitentului acesteia**;
- **orice entitate fizică sau juridică poate emite monedă virtuală**.

Din perspectiva măsurilor asigurătorii, ar putea prezenta relevanță deosebită faptul că moneda virtuală poate fi emisă ori tranzacționată inclusiv de o entitate ce nu intră în categoria instituțiilor de credit sau financiare.

2. Natura juridică a monedelor virtuale

Fără a încerca să clarificăm aici natura juridică a monedelor virtuale, lăsând acest aspect pe seama doctrinei de drept civil, la nivel de principiu, am putea accepta că o monedă virtuală este un bun mobil incorporal. În acest sens, în literatura de specialitate recentă s-a arătat că *„drepturile pe care titularul le deține asupra unui criptoactiv sunt veritabile drepturi reale asupra unui bun incorporal. Or, prototipul drepturilor reale este dreptul de proprietate (privată). În consecință, criptoactivele sunt obiect al dreptului de proprietate și, deci, sunt lucruri (necorporale)”*[11]. Monedele virtuale accesate prin

[9] Precizăm faptul că, la data redactării prezentului material, propunerea de regulament era într-un continuu proces de modificare. Prin urmare, trimiterile făcute la propunerea de regulament MiCA s-ar putea să nu își mai regăsească corespondentul în forma finală a acestui instrument juridic.

[10] A se vedea și *G. Zlati,* Tehnologia blockchain..., cit. supra, p. 64.

[11] A se vedea *R. Rizoiu,* Umbra criptoactivelor. În Codul civil, în R.R.D.P. nr. 1/2022, p. 75 și urm.

intermediul portofelelor non-custodiale par a se plia pe această definiție, titularul având un drept real de proprietate asupra lor.

Însă, din punctul nostru de vedere, mai dificil este să calificăm din punct de vedere juridic monedele virtuale atunci când discutăm despre accesarea acestora prin intermediul unor portofele digitale aflate în custodia unei terțe persoane – de exemplu, o platformă de tranzacționare centralizată (CEX).

În acest caz, se poate pune problema în ce măsură nu se poate face o analogie cu moneda de cont și instituțiile bancare. În aceste cazuri s-ar putea argumenta că titularul de cont – care deține un cont client în vederea tranzacționării pe CEX – are un drept de creanță cu privire la unitățile valorice asociate unei anumite monede virtuale. Astfel, chiar dacă titularul de cont nu deține cheia criptografică privată prin intermediul căreia să exercite un control exclusiv asupra monedelor virtuale, acesta poate solicita CEX-ului să efectueze tranzacții în numele său, ceea ce se pliază pe definiția drepturilor de creanță care implică nu exercitarea nemijlocită a unor prerogative asupra bunului care face obiectul dreptului, ci doar posibilitatea de a-i cere unei alte persoane să dea, să facă sau să nu facă ceva.

Discuția rămâne problematică deoarece atunci când se achiziționează monedă virtuală prin intermediul unui CEX, în realitate clientul nu dobândește acea monedă virtuală, ci doar un drept de creanță în legătură cu unitățile valorice ce corespund prețului de achiziție[12]. CEX-ul va fi cel care va deține în continuare unitățile valorice achiziționate, în numele clientului. De altfel, în unele situații, achiziționarea de monedă virtuală nici nu se transpune într-o tranzacție la nivel de blockchain, aceasta fiind reflectată doar într-un registru intern (tranzacție *off-chain*). Oricum ar fi, în cazul CEX, este cert că moneda virtuală nu este un bun incorporal deținut de client. Relevanța acestei distincții va fi evidențiată atunci când vom analiza măsura asigurătorie efectivă care poate fi înființată cu privire la monedele virtuale[13].

3. De la stocarea de monedă virtuală la tranzacționarea acesteia

Vom arăta, în ceea ce urmează, că moneda virtuală este stocată în blockchain și este asociată unei adrese publice (**3.1**) și că accesarea acesteia se realizează prin intermediul unui portofel digital (**3.2**). Ulterior, vom vedea relația dintre contul client pe o platformă de tranzacționare centralizată (CEX) și portofelul digital în custodie (**3.3**), clasificarea tranzacțiilor cu monedă virtuală (**3.4**) și faptul că poate fi tranzacționată prin intermediul unui CEX, DEX sau a unui portofel digital non-custodial (**3.5**).

3.1. Moneda virtuală este stocată în blockchain și este asociată unei adrese publice

Atât în vorbirea curentă, cât și în literatura de specialitate, se susține în mod frecvent că monedele virtuale sunt stocate fie în portofelul digital, fie pe o platformă de tranzacționare centralizată (CEX).

[12] A se vedea și *M. Kluchenek*, Bitcoin and Virtual Currencies: Welcome to Your Regulator, în Harvard Business Law Review, vol. 7, 2016, p. 7.
[13] A se vedea *infra,* Cap. II.

În realitate, **moneda virtuală se regăsește în mod exclusiv în blockchain**[14], privit în acest context ca fiind o bază de date descentralizată[15] stocată la nivelul nodurilor (sisteme informatice) din rețea (e.g. rețeaua Bitcoin, Ethereum, Elrond, Cardano etc.).

Sub acest aspect, moneda virtuală se aseamănă cu moneda de cont. Cu privire la ambele discutăm despre o informație, ce ia forma unor date informatice, stocate într-o bază de date. Dacă în cazul monedei de cont discutăm despre o bază de date centralizată, stocată pe serverele bancare, în cazul monedei virtuale discutăm despre o bază de date descentralizată[16]. Această paralelă este edificatoare, deoarece așa cum moneda de cont nu este stocată pe cardul bancar, așa nici moneda virtuală nu este stocată în portofelul digital (fie acesta unul în custodie sau non-custodial).[17] De asemenea, așa cum moneda de cont nu este stocată în serviciul de Internet sau Mobile Banking, așa nici moneda virtuală nu este stocată pe o platformă de tranzacționare centralizată (CEX). De altfel, dacă prin intermediul unui atac informatic s-ar șterge bazele de date și datele informatice asociate CEX-ului, monedele virtuale ar rămâne în continuare stocate la nivel de blockchain.

Atunci când discutăm despre moneda virtuală stocată în blockchain este esențial să ne raportăm inclusiv la noțiunea de **adresă publică**. Aceasta este **echivalentul unui cod IBAN** din sistemul bancar tradițional[18]. Tocmai de aceea, este de preferat să discutăm despre efectuarea unei tranzacții cu monedă virtuală de la adresa publică X (a expeditorului) la adresa publică Y (a destinatarului). În schimb, este greșit să afirmăm că tranzacția cu monedă virtuală s-a realizat din portofelul digital aparținând lui X în portofelul digital aparținând lui Y. De altfel, prin intermediul aceluiași portofel digital se pot accesa și utiliza multiple monede virtuale, asociate unor multiple adrese publice, chiar din diferite rețele blockchain[19].

Încercând o simplificare din punct de vedere tehnic, precizăm faptul că adresa publică din blockchain este generată dintr-o cheie criptografică publică de mari dimensiuni, care este trecută printr-un proces de *hashing* în vederea obținerii unui șir de caractere de dimensiuni prestabilite. Cheia criptografică publică este derivată din cheia criptografică privată, aceasta din urmă fiind **echivalentului unei parole ori a unui cod PIN**. Tocmai de aceea, cunoașterea cheii criptografice publice de către o terță persoană nu generează *per se* riscuri de securitate. În schimb, cunoașterea cheii criptografice private se transpune în posibilitatea obținerii unui control nelimitat asupra monedelor virtuale asociate unei anumite adrese publice.

---

[14] În acest sens și *C. Shaik*, Securing Cryptocurrency Wallet Seed Phrase Digitally with Blind Key Encryption, în International Journal on Cryptography and Information Security, vol. 10, nr. 4/2020, p. 1.

[15] Sau un registru [în eng., ledger] descentralizat.

[16] Descentralizarea este însă relativă, deoarece pot există diferențe semnificativ de la un proiect blockchain la altul.

[17] Importanța distincției între portofelele digitale în custodie și cele non-custodiale ține de entitatea care deține cheia criptografică privată ce îi conferă un control exclusiv asupra monedelor virtuale stocate în blockchain.

[18] A se vedea în acest sens și *A. Pelker, C.B. Brown, R.M. Tucker*, Using Blockchain Analysis From Investigation to Trial, în DOJ Journal of Federal Law and Practice, vol. 69, 2021, p. 60; *A.W. Balthazor*, The Challenges of Cryptocurrency Asset Recovery, în FIU Law Review, vol. 13, 2019, p. 1212.

[19] Cu titlu de exemplu, portofelul digital tip aplicație *Trust Wallet* suportă, printre altele, următoarele monede virtuale: BTC (blockchain Bitcoin), ETH (blockchain Ethereum), eGLD (blockchain Elrond), BNB (blockchain Binance Chain), ADA (blockchain Cardano) etc.

Discutăm așadar despre o relație funcțională între moneda virtuală și adresa publică din blockchain. Precizăm faptul că formatul unei adrese publice poate să difere în funcție de blockchain.[20] De asemenea, în principiu, monede virtuale diferite nu pot fi asociate aceleiași adrese publice. Astfel moneda virtuală bitcoin va putea fi asociată doar unei adrese publice din blockchain-ul Bitcoin.[21] Excepție face situația în care într-un anumit blockchain avem o diversitate de monede standardizate (e.g. ERC20 în cazul Ethereum, ESDT în cazul Elrond etc.). Astfel, la o adresă publică Elrond vom putea identifica monede virtuale precum eGLD, MEX, LKMEX, RIDE etc.

Este posibil ca la o adresă publică din blockchain să nu identificăm doar monede virtuale. Astfel, o adresă publică poate fi asociată unei/unor monede virtuale, unor criptoactive (e.g. un NFT) sau chiar unui contract inteligent (în eng., *smart contract*).

3.2. Moneda virtuală este accesată prin intermediul unui portofel digital

Așa cum cardul bancar este folosit ca un mijloc de identificare și autentificare a titularului contului bancar, așa și portofelul digital reprezintă mijlocul prin care o persoană poate accesa și utiliza monedele virtuale asociate unei anumite adrese publice. Precizam *supra* faptul că în portofelul digital nu sunt stocate monede virtuale, acestea fiind stocate exclusiv în blockchain. În completare, precizăm faptul că **prin intermediul portofelului digital sunt gestionate cheile criptografice publice (din care sunt derivate adresele publice) și cheile criptografice private (din care sunt derivate cheile criptografice publice)**, necesare pentru accesarea fondurilor și semnarea tranzacțiilor cu monedă virtuală.

Portofelele digitale pot avea clasificări multiple. În primul rând, discutăm despre portofele digitale non-custodiale[22] și portofele digitale în custodie. De asemenea, portofelele digitale pot să fie online (*web digital wallet*), tipărite (*paper wallet*), tip aplicație (e.g. *mobile digital wallet*) sau tip dispozitiv (*hardware digital wallet*).

Raportat la măsurile asigurătorii, distincția esențială este între portofelele digitale non-custodiale și cele în custodie. Atunci când discutăm despre un CEX ne vom raporta, în principiu, la un portofel digital în custodie. Acest lucru se transpune în faptul că accesul la fonduri poate să fie restricționat de către CEX, acesta fiind cel care deține controlul asupra cheii criptografice private. De asemenea, atunci când se accesează un cont client pe un CEX, discutăm implicit despre accesarea unui portofel digital în custodie. Tocmai de aceea, restricționarea accesului la contul client se transpune într-o restricționare a accesului la portofelul digital în custodie.

[20] De exemplu, în Elrond, toate adresele publice încep cu „erd". Un exemplu în acest sens este adresa publică *erd1qqqqqqqqqqqqqpqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqplllst77y4l* la care se regăsește contractul inteligent (în eng., *smart-contract*) pentru procesul de *staking*. Această adresă publică poate fi analizată prin intermediul Elrond Explorer (www.explorer.elrond.com).

[21] Fără a intra în detalii, precizăm că există inclusiv WBTC (wrapped bitcoin) ce permite utilizarea acestei monede în alte rețele (e.g. ethereum). Cu toate acestea, în acest caz discutăm despre o monedă virtuală standardizată care va avea paritate de 1:1 cu moneda virtuală bitcoin. Acest proces este folosit pentru a permite utilizarea anumitor monede virtuale în mai multe rețele blockchain (în eng., *cross-chain*).

[22] Cu alte ocazii ne-am referit la portofele digitale personale, în încercarea de a transpune în limba română noțiunea „non-custodial wallet". În prezent, apreciem ca fiind mai edificator să ne raportăm la portofelul digital non-custodial pentru a evidenția mai clar distincția față de portofelele digitale în custodie (custodiale).

3.3. Relația dintre contul client pe o platformă de tranzacționare centralizată (CEX) și portofelul digital în custodie

În vorbirea curentă, noțiunea de „cont" este avută în vedere atunci când discutăm despre un cont bancar, cont de Internet Banking, cont de e-mail, cont de utilizator (asociat Facebook, Instagram, LinkedIn, Tinder etc.) etc. Pentru a utiliza serviciile oferite de o platformă de tranzacționare centralizată (CEX), utilizatorul trebuie să își creeze un cont client prin intermediul căruia se va realiza procesul de autentificare. Sub acest aspect, **accesarea contului pe o platformă de schimb centralizată poate fi considerată ca fiind echivalentul accesării unui cont de Internet Banking**.

Astfel, în sistemul bancar tradițional, titularul de cont își poate accesa fondurile (moneda de cont) asociate unui cont bancar inclusiv prin intermediul contului de Internet Banking. Prin accesarea acestuia să obțină acces la o interfață grafică ce permite titularului de cont să efectueze, printre altele, o serie de operațiuni financiare. În cazul CEX, prin autentificarea în contul client, se accesează de asemenea o interfață grafică ce permite utilizatorului să beneficieze de o gamă variată de servicii precum: achiziționare de monedă virtuală cu monedă fiduciară (e.g. se cumpără 0.2 bitcoin cu lei, euro, dolari etc.),[23] vânzarea de monedă virtuală (e.g. se vinde 0.2 bitcoin și obține lei, euro, dolari etc.),[24] schimb între două monede virtuale (e.g. se schimbă 0.2 bitcoin pentru valoarea corespondentă în ether), tranzacționare de monedă virtuală (se transferă monedă virtuală de la adresa publică X la adresa publică Y) etc.

Așa cum arătam, de regulă, dacă discutăm despre accesarea monedelor virtuale prin intermediul CEX, avem în vedere utilizarea unui portofel digital în custodie.[25] Fiind vorba despre un portofel digital în custodie, utilizatorul nu se autentifică în mod nemijlocit la acesta. În context, platforma de tranzacționare centralizată are calitatea de intermediar, fiind interpusă între utilizator și portofelul digital în custodie. De fiecare dată când utilizatorul dorește să efectueze o tranzacție cu monedă virtuală, transmite o instrucțiune în acest sens platformei de tranzacționare centralizate. Prin urmare, am putea concluziona că autentificarea în contul utilizator conferă doar un acces condiționat la portofelul digital în custodie[26], prin intermediul CEX.

Dacă furnizorul platformei de tranzacționare (CEX) restricționează accesul la contul client, se restricționează implicit accesul la portofelul digital în custodie. Aceasta se transpune în pierderea accesului la monedele virtuale, singura posibilitate de a redobândi acest acces fiind aceea de a redobândi accesul la contul client.

În cazul platformelor de tranzacționare descentralizare (DEX), autentificarea se realizează prin intermediul unui portofel digital non-custodial. Prin urmare, nu este necesară

[23] Discutăm în acest caz despre un proces denumit *on-ramp*.
[24] Discutăm în acest caz despre un proces denumit *off-ramp*.
[25] Din punct de vedere tehnic, nu este exclusă posibilitatea ca o platformă de tranzacționare centralizată să permită utilizatorilor folosirea unor portofele digitale non-custodiale (e.g. Ledger Nano).
[26] Ar trebui făcută așadar distincția între accesarea contului client (unde titularul de cont este clientul CEX) și accesarea portofelului digital în custodie (unde titularul este CEX). Astfel, dacă se va accesa în mod neautorizat contul client, se poate susține că subiect activ al infracțiunii prevăzute la art. 360 C.pen. este clientul CEX. Aceasta întrucât, clientul CEX are un drept de folosință consolidat asupra contului client. În schimb, dacă atacatorul identifică o breșă de securitate și accesează portofelul digital în custodie, s-ar putea argumenta că subiectul pasiv este entitatea juridică ce deține CEX-ul.

crearea unui cont client[27]. De asemenea, atunci când se creează un portofel digital non-custodial nu discutăm despre crearea unui cont client distinct, în ciuda faptului că procesul de autentificare la portofelul digital personal poate necesita introducerea unei parole, a unui cod PIN etc. Eventual, am putea susține că portofelul digital non-custodial este echivalentul contului client prin intermediul căruia se interacționează în mod nemijlocit cu rețeaua blockchain. Esențial este însă faptul că, spre deosebire de conturile client CEX, pentru crearea unui portofel digital non-custodial nu este necesară introducerea unor date cu caracter personal[28].

3.4. Clasificarea tranzacțiilor cu monedă virtuală

Printr-o tranzacție cu monedă virtuală vom înțelege orice operațiune în legătură cu aceasta: operațiune de „transfer" de la adresa publică X la adresa publică Y; operațiune de achiziționare monedă virtuală; operațiune de vânzare monedă virtuală; operațiune de schimb cu o altă monedă virtuală; operațiune de schimb cu un alt criptoactiv; operațiune de blocare sau deblocare a monedei virtuale într-un/dintr-un contract inteligent (e.g. în cazul procedurii de *staking* sau *unstaking*) etc. Necesită așadar observat că ceea ce se înțelege prin „transfer" de monedă virtuală reprezintă doar o operațiune specifică privind tranzacționarea cu monedă virtuală. În acest caz discutăm despre o tranzacție prin intermediul căreia se poate schimba titularul monedei virtuale ori al drepturilor asociate acesteia.

Tranzacția cu monedă virtuală are de asemenea o semnificație mai largă decât schimbul de monedă virtuală, motiv pentru care preferăm să ne referim la CEX ca fiind o platformă de tranzacționare centralizată și nu una de schimb – aceasta în ciuda trimiterii deficitare făcute de legiuitor în cuprinsul Legii nr. 129/2019.

O clasificare deosebit de relevantă a tranzacțiilor se raportează la modul în care aceasta este jurnalizată. Astfel, trebuie să facem distincția între **tranzacția în blockchain** [în eng., *on-chain transaction*] și **tranzacția internă** [în eng., *off-chain transaction*]. În cazul unei tranzacții în blockchain (on-chain), aceasta devine ireversibilă de la momentul înregistrării – ce implică un proces de validare – în următorul bloc de date. În cazul unei tranzacții interne discutăm despre o jurnalizare realizată în afara blockchain[29].

[27] Concluzia este din nou una relativă, deoarece nu este exclusă posibilitatea ca furnizorul serviciului de tranzacționare să impună utilizatorului o autentificare în sistem centralizat, înainte de a se autentifica prin intermediul unui portofel digital personal. Astfel, având în vedere că inclusiv o platformă de tranzacționare descentralizată este accesată prin intermediul unei pagini web (e.g. Maiar Exchange, SundaeSwap, ZilSwap etc.) ori a unei aplicații instalate pe un telefon mobil inteligent (e.g. Acala, Osmosis, Uniswap etc.), este posibilă integrarea unui sistem de autentificare centralizat.

[28] Pentru crearea portofelului digital *Maiar* este necesară introducerea unui număr de telefon. Cu toate că se susține că acesta este criptat în baza de date, nu poate fi ignorat faptul că la crearea portofelului digital se primește un cod SMS pentru validarea numărului de telefon. În schimb, pentru a se creat un portofel digital *Elrond Web Wallet* (www.wallet.elrond.com) nu este necesară introducerea de date cu caracter personal. Situația este identică pentru alte portofele digitale personale precum *Trust Wallet*, *Daedalus* etc.

[29] A se vedea în acest sens și *M. Mount*, Bitcoin off-chain transactions: Their invention and use, în Georgetown Law Technology Review, vol. 4, nr.2/2019, p. 685. A se vedea de asemenea o definiție a tranzacțiilor interne (off-chain) rețelei blockchain aici - https://academy.binance.com/en/glossary/off-chain [ultima accesare în 02.04.2022].

Cu titlu de exemplu, atunci când se „transferă" monedă virtuală între două conturi asociate aceluiași CEX, putem discuta despre o tranzacție internă (off-chain). În acest caz, tranzacția se poate realiza instant și fără costuri de tranzacționare, având în vedere că nu necesită o validare la nivel de blockchain. Discutăm așadar despre un transfer al dreptului patrimonial, în ciuda faptului că moneda virtuală rămâne în continuare asociată aceleiași adrese publice, fără să existe vreo modificare a informațiilor în blockchain[30].

De asemenea, tranzacția internă nu va putea fi verificată în blockchain deoarece aceasta nu este înregistrată în următorul bloc de date. Informațiile aferente tranzacției sunt înregistrate *off-chain*, adică într-un registru distinct aparținând unei terțe entități (e.g. CEX). Rezultă de aici că în cazul acestor categorii de tranzacții putem discuta inclusiv despre un caracter centralizat, aflat în opoziție cu tranzacțiile în blockchain[31]. Principala consecință ar fi aceea că, tranzacțiile interne pot să fie reversibile.

3.5. Moneda virtuală poate fi tranzacționată prin intermediul unui CEX, DEX sau a unui portofel digital non-custodial

Pentru a putea tranzacționa monedă virtuală, necesită folosit un serviciu ce permite efectuarea operațiunilor menționate *supra* (pct. 3.4). În context, trebuie să ne raportăm la noțiunile CEX, DEX și portofel digital non-custodial.

CEX este un furnizor de servicii de schimb (tranzacționare) între monede virtuale sau între monede virtuale și monede fiduciare[32]. În esență, când discutăm despre CEX avem în vedere o platformă de tranzacționare centralizată (e.g. Binance, Kraken, Gate.io, Gemini etc.) prin intermediul căreia se poate tranzacționa una sau mai multe monede virtuale. În schimb, DEX (e.g. Maiar Exchange, SushiSwap, Uniswap, PancakeSwap, 1inch Exchange etc.) este o platformă de tranzacționare descentralizată[33].

Este important să facem distincția între CEX și DEX având în vedere următoarele:

i. Pentru a tranzacționa monedă virtuală prin intermediul CEX **este necesară crearea unui cont client**. Or, acest lucru implică comunicarea unor date cu caracter personal (e.g., nume și prenume, adresă de email etc.). De asemenea, utilizarea contului client prin tranzacționarea de monedă virtuală poate necesita sau necesită (în funcție de jurisdicție) îndeplinirea unei proceduri de cunoaștere a clientelei [în eng., KYC] în scopul prevenirii și combaterii spălării banilor[34]. Prin urmare, CEX va putea comunica date cu privire la identitatea titularului de cont și va putea asocia diferitele tranzacții cu monedă virtuală cu

[30] M. Mount, op. cit., p. 688.

[31] În cazul *Lightning Network* discutăm însă despre o tranzacție peer-to-peer descentralizată.

[32] La art. 5 alin. (1) lit. g^1) din Legea nr. 129/2019 se face trimitere doar la furnizorii de servicii de schimb între monede virtuale și monede fiduciare.

[33] A se vedea o analiză a acestora în *L.X. Lin,* Deconstructing Decentralized Exchanges, în Stanford Journal of Blockchain Law & Policy, vol. 2.1., 2019, pp. 58 și urm. De *lege lata*, nu există o definiție legală sau un regim juridic aplicabil acestui tip de serviciu. În Legea nr. 129/2019 este menționat doar furnizorul serviciului de schimb între monede virtuale și monede fiduciare. Cu alte cuvinte, discutăm doar despre operațiuni specifice *on-ramp* (achiziționare de monedă virtuală) și *off-ramp* (vânzare de monedă virtuală). Astfel, dacă CEX ar furniza doar un serviciu de schimb între diverse monede virtuale, dispozițiile legii nr. 129/2019 nu ar fi aplicabile.

[34] A se vedea o analiză generală în *A.V. Popescu*, Cunoașterea clientelei pe piața criptoactivelor – între teorie și practică, în Analele Științifice ale Universității „Alexandru Ioan Cuza" din Iași, tom. LXVII, supliment 2, 2021, pp. 81 și urm.

identitatea unei persoane. În schimb, pentru a utiliza DEX nu este necesară crearea unui cont client[35], autentificarea fiind realizată în mod nemijlocit prin intermediul unui portofel digital non-custodial.

ii. În cazul unui CEX, regula este cea potrivit căreia **titularul contului client nu deține cheia criptografică privată asociată portofelului digital**, ceea ce se transpune în faptul că nu deține propriu-zis monedele virtuale. În schimb, în cazul DEX, discutăm despre utilizarea unor portofele digitale non-custodiale ce conferă titularului monedelor virtuale un control exclusiv asupra fondurilor. Chiar dacă monedele virtuale sunt blocate într-un contract inteligent[36], titularul monedelor virtuale rămâne persoana care deține cheia criptografică privată.

iii. În cazul CEX putem discuta despre **adrese publice comune ce echivalează cu un cont comun** [în eng., *omnibus account* sau *omnibus wallet*] ce are asociată o monedă virtuală în legătură cu care există drepturi de creanță aparținând unor terțe persoane. În concret, achiziționarea de monedă virtuală prin intermediul CEX nu implică *per se* asocierea unităților de valoare achiziționate cu o adresă publică personală – asociată titularului de cont (clientului). În momentul în care un titular de cont achiziționează unități valorice suplimentare dintr-o anumită monedă virtuală, soldul din contul client este actualizat pentru a reflecta întinderea dreptului de creanță. Important de reținut este însă faptul că moneda virtuală nu va fi tranzacționată obligatoriu de la o adresă publică la alta, ci va putea rămâne asociată unei adrese publice comune aflate sub controlul CEX. În acest caz, putem discuta inclusiv despre o tranzacție cu monedă virtuală internă sau *off-chain* (a se vedea *supra*).

iv. Având în vedere că CEX – prin intermediul cheii criptografice private – deține controlul exclusiv asupra monedelor virtuale, acesta **va putea în orice moment să restricționeze tranzacțiile cu monedă virtuală pentru orice utilizator**. Am putea discuta în acest sens despre echivalentul unei popriri. În schimb, în cazul DEX, o asemenea posibilitate este exclusă *de plano*[37].

O tranzacție cu monedă virtuală se poate realiza în mod direct prin intermediul unui portofel digital non-custodial, fără să fie așadar necesară utilizarea CEX sau DEX. În acest caz, furnizorul portofelului digital nu va putea restricționa accesul și utilizarea fondurilor. De asemenea, în principiu, așa cum vom vedea, acesta nu va putea oferi organelor judiciare informații cu privire la identitatea titularului portofelului digital.

---

[35] O asemenea posibilitate nu este exclusă din punct de vedere tehnic, din moment ce interacțiunea cu un DEX se realizează fie prin intermediul unei pagini web, fie prin intermediul unei aplicații (e.g. Iphone sau Android app). Astfel, furnizorul unui DEX ar putea implementa un sistem de autentificare în doi pași – înainte de autentificarea prin intermediul portofelului digital personal fiind necesară o autentificare prin intermediul unui cont de utilizator „tradițional".

[36] De exemplu, într-o procedură de *staking* se „deleagă" unități de valoare asociate unei monede virtuale în scopul participării la mecanismul de consens *proof-of-stake*. Chiar dacă titularul monedelor virtuale nu se schimbă în acest caz, acestea pot să fie blocate pentru o anumită perioadă de timp de la tranzacționare (perioada de unstaking).

[37] Aceasta întrucât, cel puțin în momentul de față, nu se folosește autentificarea în doi pași menționată *supra*. Dacă un DEX ar implementa inclusiv autentificarea prin intermediul unui cont de utilizator, restricționarea accesului la fonduri s-ar putea realiza prin intermediul restricționării accesului la contul client. Acest lucru nu ar echivala însă cu o poprire, ci cu o restricționare a accesului la datele informatice. Forțând o paralelă, este ca și cum o bancă ar restricționa accesul la serviciului de Internet Banking – blocând autentificarea la contul client.

4. Cine este deținătorul monedei virtuale ?

Se poate anticipa că acest subiect va genera o amplă dezbatere la nivel doctrinar și jurisprudențial. În acest context, apreciem că necesită făcută o distincție între ipoteza în care monedele virtuale sunt accesate prin intermediul unui portofel digital în custodie sau prin intermediul unui portofel digital non-custodial.

Astfel, așa cum arătam, atunci când discutăm despre monede virtuale accesate prin intermediul CEX, avem în vedere utilizarea unui portofel digital în custodie. În această situație, credem că monedele virtuale sunt deținute de către CEX, clientul având doar un drept de creanță în raport cu anumite unități valorice asociate acestora. Clientul poate transmite instrucțiuni către CEX cu privire la efectuarea unor tranzacții cu monedă virtuală, dar acesta nu deține un control exclusiv asupra acestora.

Concluzia se schimbă în mod radical în ipoteza în care monedele virtuale sunt accesate prin intermediul unui portofel digital non-custodial. În acest caz, cel care deține cheia criptografică privată este titularul portofelului digital care, implicit, este deținătorul monedei virtuale asociate unei adrese publice derivate din cheia criptografică privată[38].

5. Cum se poate cuantifica valoarea unei monede virtuale ?

Valoarea monedelor virtuale oscilează în timp[39] și este dificil de cuantificat prin raportare la o dată certă, având în vedere lipsa unui index valoric oficial. Astfel, pe fiecare CEX în parte, în funcție de cererea și oferta existentă la un moment dat, valoarea unei monede virtuale poate să difere semnificativ. În măsura în care moneda virtuală de referință este accesată prin intermediul unui CEX, o soluție ar fi aceea de a ne raporta la valoarea de piață ce corespunde cererii și ofertei pe respectivul CEX. Aceeași concluzie ar putea fi menținută cu privire la monedele virtuale tranzacționate prin intermediul unui DEX. Lucrurile se complică în mod semnificativ atunci când moneda virtuală este accesată prin intermediul unui portofel digital non-custodial, fără a se utiliza DEX. În acest caz, singura posibilitate ar fi aceea de a ne raporta la agregator de date precum CoinGecko[40] sau CoinMarketCap[41].

În orice caz, nu ar trebui făcută confuzie între valoarea de piață a monedei virtuale la data instituirii măsurii asigurătorii și valoarea pagubei produse prin comiterea unei infracțiuni. Astfel, „sustragerea" a 1 bitcoin (art. 250 C.pen.) va genera o pagubă constând în valoarea acestei monede virtuale la data consumării infracțiunii[42]. În schimb, la data instituirii măsurii asigurătorii, valoarea aceleiași unități valorice (e.g. 1 bitcoin) ar putea să difere în mod semnificativ în raport cu data consumării infracțiunii.

---

[38] Precizăm în contextul faptul că prin intermediul unui portofel digital se gestionează cheile criptografice (publice și private) necesare pentru semnarea unei tranzacții (semnătură electronică) cu monedă virtuală. Este bine de știut că din cheia criptografică privată este derivată cheia criptografică publică. De asemenea, din cheia criptografică publică este derivată adresa publică din blockchain, prin intermediul unui proces de *hashing* – fiind generat un șir de caracter de o dimensiune prestabilită după conținutul cheii criptografice publice.

[39] Excepție fac monedele virtuale stabile (non-volatile), în cazul cărora discutăm despre o valoare de referință (*e.g*. 1 dolar american) ce este menținută prin intermediul unui mecanism de compensare.

[40] www.coingecko.com.

[41] www.coinmarketcap.com.

[42] A se vedea în acest sens C.A. Brașov, s. pen., dec. nr. 219/2018, disponibilă pe sintact.ro.

6. Ce informații asociate tranzacțiilor cu monedă virtuală pot fi vizualizate în blockchain?

Proiectele blockchain existente prezintă multiple asemănări (e.g. existența unui mecanism de consens pentru validarea tranzacțiilor), dar la fel de bine se pot și diferenția în mod semnificativ (e.g. prin raportare la tipul mecanismului de consens folosit[43]).

Raportat la obiectul prezentului material, cea mai importantă diferență are în vedere transparența la nivel de blockchain. În cazul majorității proiectelor blockchain, orice adresă publică sau tranzacție cu monedă virtuală poate fi verificată în blockchain. Când discutăm despre o asemenea verificare avem în vedere utilizarea unui instrument denumit „blockchain explorer" (e.g. o pagină web, o aplicație pe telefonul mobil etc.) ce permite utilizatorului interogarea registrului public descentralizat și analizarea informațiilor stocate în blocurile de date validate și introduse în blockchain.[44] Exemple relevante în acest sens sunt următoarele:

- https://www.blockchain.com/ - permite analiza blocurilor de date în rețeaua Bitcoin, Bitcoin Cash și Ethereum.
- https://etherscan.io/ - permite analiza blocurilor de date în rețeaua Ethereum.
- https://explorer.elrond.com/ - permite analiza blocurilor de date în rețeaua Elrond.
- https://explorer.cardano.org/ - permite analiza blocurilor de date în rețeaua Cardano.

Astfel, chiar dacă nu se va putea face o asociere directă între o anumită adresă publică sau o anumită tranzacție cu monedă virtuală și identitatea unei persoane, se vor putea obține informații relevante precum:[45]

- **Adresele publice implicate în tranzacție** – adresa publică a expeditorului și a destinatarului. Dacă tranzacția cu monedă virtuală s-a efectuat prin intermediul CEX, necesită înțeles faptul că la nivel de blockchain s-ar putea să fie identificată o adresă publică comună.
- **Data și ora tranzacției**. Trebuie făcută aici o distincție între data și ora la care a fost inițiată tranzacția și cea la care tranzacția a fost validată în blockchain. De asemenea, este important a se face conversia orei indicate în raport cu fusul orar dorit.
- **Codul unic de identificare al tranzacției** (e.g. TXID, Hash etc.). Practic, o tranzacție va putea fi identificată în blockchain fie prin verificarea tuturor tranzacțiilor efectuate de la/către o anumită adresă publică (verificarea după șirul de caractere ce include adresa publică) sau după codul unic de identificare generat pentru fiecare tranzacție în parte (căutare după TXID sau Hash). Deosebit

[43] Cele mai cunoscute mecanisme de consens fiind Proof of Work (PoW) și Proof of Stake (PoS). Primul mecanism de consens este folosit în prezent de Bitcoin, Ethereum, Monero, Dogecoin, Litecoin etc. Al doilea mecanism de consens este folosit – în diverse variațiuni – de Elrond, Cardano, Zilliqa, Tron, Tezos etc. Inclusiv Ethereum urmează să facă tranziția de la mecanismul de consens Proof of Work la mecanismul de consens Proof of Stake – a se vedea o prezentare în *L.J. Kelly, R. Millman, S. Graves*, What is Ethereum 2.0? Ethereum's Consensul Layer and Merge Explained, material disponibil pe pagina https://decrypt.co/resources/what-is-ethereum-2-0 [ultima accesare în data de 03.04.2022].

[44] Există inclusiv posibilitatea copierii locale a registrului public descentralizat și efectuarea unei analize nemijlocite asupra acestuia.

[45] A se vedea și *A. Pelker, C.B. Brown, R.M. Tucker*, op. cit., pp. 60-61.

de relevant este faptul că tranzacțiile interne (off-chain) nu vor putea fi verificate în blockchain. Chiar dacă acestea vor avea de asemenea un cod unic de identificare (intern), acesta este stocat doar în registrul separat (off-chain) al entității care efectuează acest tip de tranzacției (e.g. CEX).

- **Tipul tranzacției** cu monedă virtuală. Așa cum am precizat deja *supra,* o tranzacție cu monedă virtuală nu se limitează la un „transfer" al acesteia de la o adresă publică la altă. În funcție de proiectul blockchain despre care discutăm, putem identifica tranzacții efectuate în mod nemijlocit de către titularul monedelor virtuale ori tranzacții efectuate în mod automat de un contract inteligent.

Analizarea acestor informații nu poate conduce *per se* la identificarea persoanelor implicate în tranzacția cu monede virtuale.[46] Totuși, aceste informații s-ar putea dovedi esențiale pentru a stabili trasabilitatea tranzacțiilor cu monedă virtuală și identificarea unor adrese publice asociate CEX sau a unui alt intermediar *on-ramp*[47] sau *off-ramp*. În măsura în care se identifică o asemenea adresă publică, există posibilitatea teoretică de a obține de la CEX sau de la intermediarul *on-ramp/off-ramp* datele de identificare ale titularului contului client – expeditor sau destinatar al fondurilor ce au făcut obiectul tranzacției respective.

La polul opus se află proiectele blockchain axate pe anonimitate (e.g. Monero, Mina Protocol, Secret Network, Zcash etc.). De exemplu, Monero nu oferă posibilitatea de a verifica în blockchain, de o manieră transparentă, informațiile asociate unei tranzacții cu moneda virtuală XMR[48]. În concret, Monero permite doar participanților la tranzacție să acceseze informațiile asociate unei tranzacții[49], ceea ce creează un obstacol pentru orice altă terță persoană în ceea ce privește posibilitatea efectuării unei analize la nivel de blockchain[50].

Distinct de proiectele blockchain axate pe anonimitate, inclusiv în cazul proiectelor ce oferă transparență la nivelul informațiilor accesibile în blockchain, există servicii prin intermediul cărora se poate îngreuna în mod semnificativ identificarea originii unei tranzacții. Discutăm în acest caz despre servicii ce poartă denumirea de „mixers" sau „tumblers" (e.g. CoinJoin, DarkWallet, Wasabi Wallet, Blender.io etc.). Prin intermediul acestora fondurile (e.g. unitățile valorile asociate monedei virtuale bitcoin) aparținând unor terți (între care nu există legătură) sunt agregate la o anumită adresă publică și redistribuite către alte adrese publice din blockchain[51]. În concret, dacă X transmite lui Y 0.2 bitcoin prin

[46] Idem, p. 61.

[47] Cum ar fi de exemplu Ramp Network (www.ramp.network), MoonPay (www.moonpay.com), Banxa (www.banxa.com), Mercuryo (www.mercuryo.io) etc. În cazul tuturor acestor intermediari *on-ramp*, achiziționarea de monedă virtuală este posibilă doar ulterior îndeplinirii procedurii de cunoaștere a clientelei. De asemenea, moneda virtuală este achiziționată prin intermediul unei monede fiduciare, ceea ce implică necesitatea efectuării unui depozit bancar sau folosirea unui card bancar.

[48] În ciuda faptului că ne referim de multe ori la Monero ca fiind o monedă virtuală, în realitate moneda virtuală asociată acestui blockchain este XMR.

[49] A se vedea în acest sens și C.P. Buttigieg, C. Efthymiopoulos, S. Cuyle, Anti-money laundering regulation of crypto assets in Europe's smallest member state, în Law and Financial Markets Review, vol. 13, nr. 4/2019, p. 213.

[50] Se poate compara în acest sens Monero Explorer (https://www.exploremonero.com/) cu orice alt blockchain explorer asociat Bitcoin, Ethereum, Elrond etc.

[51] A se vedea în acest sens și *C.P. Buttigieg, C. Efthymiopoulos, S. Cuyle*, op. cit., p. 213; *A. Pelker, C.B. Brown, R.M. Tucker*, op. cit., p. 63.

intermediul unui asemenea serviciu, în blockchain nu va exista o legătură directă între adresa publică asociată lui X și adresa publică asociată lui Y.

Nu în ultimul rând, în cazul tranzacțiilor interne sau *off-chain* (a se vedea *supra*), o analiză la nivel de blockchain se va dovedi inutilă. Având în vedere că în cazul acestor tranzacții nu discutăm despre introducerea unor informații în blockchain, ci despre păstrarea informațiilor asociate tranzacției într-un registru separat, informațiile relevante pot fi obținute doar de la intermediarul care realizează tranzacția internă (*off-chain*). Așa cum am precizat deja *supra*, aceste tranzacții sunt efectuate inclusiv de către CEX – ceea ce înseamnă că toate informațiile asociate respectivei tranzacții interne (*off-chain*) pot să fie obținute de către organele judiciare[52].

7. Ce date poate oferi CEX, DEX sau furnizorul unui portofel digital personal ?

Înainte de a discuta despre instituirea unor măsuri asigurătorii, este necesar să discutăm despre posibilitatea obținerii unor informații referitoare la deținătorul monedelor virtuale, soldul disponibil etc. Pentru a putea face această discuție și a vedea ce date pot fi obținute astfel, menționăm încă de la început că prezintă relevanță dacă persoana cercetată folosește CEX, DEX sau un portofel digital non-custodial.

Dacă discutăm despre un cont client creat pe CEX, este posibilă obținerea următoarelor informații:

- **Datele cu caracter personal folosite la crearea contului client** – nume de utilizator, adresă de email etc.
- **Datele cu caracter personal folosite în procedura de cunoaștere a clientelei** (în eng., KYC) – nume și prenume, codul numeric personal, adresa de domiciliu etc.
- **Denumirea monedelor virtuale** deținute și **cuantumul unităților valorice** asociate acestora (soldul disponibil).
- **Informații cu privire la tranzacțiile efectuate** – istoricul tranzacțiilor cu monedă virtuală, inclusiv cele interne (*off-chain*).

În cazul DEX, situația poate să difere în mod substanțial[53]. În primul rând, nu ne putem asuma o concluzie generală deoarece fiecare DEX poate să fie implementat în mod diferit, ceea ce se transpune în faptul că datele colectate și care ar putea să fie furnizate organelor judiciare diferă de la caz la caz. La nivel de principiu, având în vedere că procesul de autentificare la DEX se realizează prin intermediul unui portofel digital non-custodial, nu vor exista informații cu privire la identitatea titularului monedelor virtuale.

Concluzia își păstrează valabilitatea și cu privire la tranzacțiile efectuate în mod nemijlocit prin intermediul unui portofel digital non-custodial. Din moment ce pentru crearea acestuia nu este necesară comunicarea unor date cu caracter personal, furnizorul portofelului digital non-custodial nu cunoaște identitatea titularului acestuia.

[52] În concret, fiecare tranzacție efectuată prin intermediul CEX – inclusiv una off-chain – va genera o urmă digitală într-un fișier tip jurnal (în eng., log).
[53] A se vedea în acest sens și *A. Pelker, C.B. Brown, R.M. Tucker*, op. cit., p. 65 și nota de subsol nr. 10.

II. OBȚINEREA DE DATE ȘI INFORMAȚII ÎN LEGĂTURĂ CU MONEDELE VIRTUALE ÎN CADRUL PROCESULUI PENAL

Dacă, atunci când se instituie măsuri asigurătorii în procesul penal, nu este necesar să se indice sau să se dovedească ori să se individualizeze bunurile asupra cărora se înființează respectivele măsuri[54], aducerea la îndeplinire presupune, de multe ori, o procedură prealabilă de identificare a bunurilor care urmează a forma obiectul măsurilor. De pildă, în materia bunurilor imobile, organul care aduce la îndeplinire măsura va solicita informații de la Oficiul de Cadastru și Publicitate Imobiliară sau de la direcțiile de taxe locale (în acest din urmă caz, inclusiv pentru autovehicule), iar în cazul conturilor bancare, respectivele informații vor fi obținute de la instituțiile de credit sau - pentru anumite informații - prin consultarea sistemului informatic PatrimVen. Cum și de la cine va afla însă organul de urmărire penală ori cel care trebuie să aducă la îndeplinire o măsură asigurătorie dacă suspectul sau inculpatul deține monede virtuale pentru a putea înființa măsurile asigurătorii astfel cum au fost descrise mai sus? Desigur, dacă este cunoscută adresa publică, tranzacțiile pot fi verificate – în principiu[55] – direct în blockchain, fără a fi necesare alte proceduri suplimentare. În schimb, dacă adresa publică nu este cunoscută, este nevoie de demersuri suplimentare.

În concret, poate fi pusă în discuție posibilitatea folosirii metodelor de supraveghere sau cercetare prevăzute la art. 153 C.pr.pen. - obținerea de date privind situația financiară a unei persoane (**1**) sau art. 146[1] C.pr.pen. - obţinerea datelor privind tranzacţiile financiare ale unei persoane (**2**), precum și a predării obiectelor, înscrisurilor sau a datelor informatice - art. 170 alin. (2) lit. a) C.pr.pen. (**3**).

Cu titlu preliminar, menționăm că toate aceste metode ori procedee se subsumează, în realitate, necesității obținerii *probelor* în procesul penal. Astfel, dacă organul judiciar consideră că datele privind deținerea monedelor virtuale ori tranzacțiile efectuate cu acestea pot constitui probă în procesul penal, atunci este posibil ca, obținând respectivele date, să fie luată și decizia instituirii măsurii asigurătorii. Cele două aspecte (caracterul potențial de probă și instituirea măsurilor asigurătorii) pot fi ușor de conciliat în cazul infracțiunilor comise în legătură sau prin intermediul monedelor virtuale (ex. înșelăciune, efectuarea de operațiuni financiare în mod fraudulos, delapidare, fals informatic, șantaj etc.)[56], dar este mai greu de justificat folosirea metodelor pe care le vom descrie în cele ce urmează când unicul scop este luarea măsurilor asigurătorii (de exemplu, în vederea garantării executării pedepsei amenzii ori a garantării cheltuielilor judiciare).

Cu toate acestea, de multe ori, în urma obținerii datelor respective, este posibil ca organul judiciar să „profite” de informațiile astfel deținute pentru a decide luarea măsurilor asigurătorii. Totodată, având în vedere definiția largă a probei prevăzută de art. 97 alin. (1) C.pr.pen., ne putem întreba dacă „justa soluționare a cauzei” nu se referă și la luarea măsurilor asigurătorii. Mai mult decât atât, așa cum vom arăta în cele ce urmează, în realitate art. 153 C.pr.pen. este mai des (sau cel puțin se dorește a fi) folosit pentru a afla informații în legătură cu măsurile asigurătorii decât pentru a obține probe.

---

[54] A se vedea I.C.C.J., dec. nr. 19/2017 pronunțată în recurs în interesul legii (M. Of. nr. 953/04.12.2017).

[55] O asemenea analiză nu este posibilă în cazul proiectelor blockchain axate pe anonimitate – a se vedea în acest sens trimiterile făcute *supra* (pct. I) la Monero.

[56] Pentru infracțiunile care pot fi comise în legătură cu sau prin intermediul monedelor virtuale, a se vedea *G. Zlati,* Tehnologia blockchain..., cit. supra., pp. 53-62.

1. Obținerea de date privind situația financiară a unei persoane (art. 153 C.pr.pen.)

Potrivit art. 153 C.pr.pen. alin. (1) C.pr.pen., *„procurorul poate solicita unei instituţii de credit sau* ***oricărei altei instituţii care deţine date privind situaţia financiară*** *a unei persoane comunicarea* ***datelor privind existenţa şi conţinutul conturilor unei persoane****, în cazul în care există indicii temeinice cu privire la săvârşirea unei infracţiuni şi există temeiuri pentru a se crede că datele solicitate constituie probe”* (subl. ns.).

Reamintim, în acest context, că, în versiunea inițială din 2014, obținerea de date privind situația financiară implica autorizarea judecătorului de drepturi și libertăți. În contextul propunerilor de modificare a textului de lege, am arătat cu altă ocazie că, potrivit unei astfel de inițiative, formulată de DNA la 31.01.2014[57],*„solicitarea datelor financiare reprezintă o intruziune minimă în viaţa privată a unei persoane, care nu justifică autorizarea a priori de către judecător. Asigurarea accesului prompt al organelor de urmărire penală la aceste informaţii* ***este esenţială pentru a garanta recuperarea pagubelor produse prin infracţiuni, având în vedere că eficienţa măsurilor de indisponibilizare a bunurilor este determinată de identificarea în timp real a bunurilor deţinute de persoanele investigate****”* (subl. ns.).

În același sens, procurorul şef al DNA a declarat în anul 2014[58] că *„informaţiile referitoare la existenţa conturilor bancare reprezintă o intruziune minimă în viaţa privată a unei persoane, care nu justifică autorizarea de către judecător. Aceste date nu conţin rulajul conturilor bancare, ci numai date cu privire la existenţa lor (…) Astfel de informaţii* ***sunt esenţiale pentru a garanta recuperarea pagubelor, iar eficienţa măsurilor asigurătorii este determinată de identificarea în timp real a bunurilor deţinute de persoanele investigate, astfel încât este necesar să fie asigurat accesul prompt al organelor de urmărire penală la asemenea date***” (subl.ns.)[59].

Este evident, așadar, că obținerea de date privind situația financiară la care se referă art. 153 C.pr.pen. este folosită în special în legătură cu măsurile asigurătorii. De altfel, faptul că o persoană deține un cont care are un anumit sold constituie în puține cazuri probă în procesul penal. Practica organelor judiciare confirmă această concluzie, ordonanțele care au ca temei art. 153 C.pr.pen. menționând în general în mod generic că datele respective constituie probe, de multe ori infracțiunile cercetate neavând, în realitate, legătură cu conturile bancare[60]. În altă ordine de idei, mai ales în contextul operaționalizării sistemului informatic PatrimVen, existența unui cont, numărul IBAN, data deschiderii contului, data închiderii, tipul de cont, tipul de monedă, ID-ul contului, datele privind împuterniciții pe cont - adică acele categorii de date care pot fi obținute în temeiul art. 153 C.pr.pen. - pot fi obținute de o serie de organe de urmărire penală direct prin accesarea respectivului sistem

[57] Disponibilă la adresa http://media.hotnews.ro.

[58] A se vedea http://www.mediafax.ro/social/nitu-codurile-nu-sunt-scutite-de-critici-dar-practica-va-dovedi-care-sunt-problemele-11997491.

[59] A se vedea, pentru toate aceste aspecte, *A.R. Trandafir, G. Marin,* Obținerea de informații ori înscrisuri de la instituțiile de credit în cursul urmăririi penale, în *C. Mitrache, A.R. Trandafir,* In Honorem Nicolae Volonciu, Ed. Universul Juridic, București, 2017.

[60] Spre exemplu, s-a solicitat unei instituții de credit comunicarea datelor privind existența și conținutul conturilor unei persoane suspectate că ar fi comis infracțiunea de abuz în serviciu în legătură cu un teren, fapta respectivă nefiind comisă în niciun fel prin folosindu-se tranzacții sau operațiuni financiare.

informatic, cel puțin în cazul anumitor infracțiuni[61]. În aceste cazuri, recurgerea la art. 153 C.pr.pen. devine relevantă strict pentru cunoașterea soldului conturilor bancare[62].

Trecând peste aceste probleme, se ridică întrebarea dacă art. 153 C.pr.pen. poate constitui temei pentru obținerea datelor privind deținerea monedelor virtuale, mai ales că sistemul PatrimVen nu cuprinde, cel puțin la acest moment, informații privind deținerea acestor categorii de criptoactive.

În mod evident, textul de lege a fost creat pentru conturile bancare. Chiar dacă legiuitorul se referă la instituțiile de credit și la *alte instituţii care deţin date privind situaţia financiară a unei persoane,* având în vedere că datele vizează „existența și conținutul conturilor", este neîndoielnică trimiterea la conturile bancare.

Cu privire sintagma „situația financiară" folosită de legiuitor, nu credem că ea ridică probleme în mod special, întrucât este utilizat sensul comun al noțiunii, și anume acela de modalitate în care se prezintă patrimoniul unei persoane privind intermediul conturilor acesteia - adică, mai exact, care sunt sumele din conturile curente, din cele de depozit ori de altă natură, precum și valorile care exprimă, în realitate, datorii (contul de credit, o linie de credit etc.). Nu credem, așadar, că legiuitorul penal a avut în vedere noțiunea de „situație

---

[61] A se vedea, în acest sens, art. 61[1] alin. (5) C.pr.fisc., potrivit cu care autorităţile şi instituţiile prevăzute la art. 1 din Legea nr. 129/2019 (deci, potrivit lit. a), inclusiv organele de urmărire penală) au acces la informaţiile din Registrul pentru conturi de plăți și conturi bancare **pentru îndeplinirea obligațiilor care le revin acestora în temeiul Legii nr. 129/2019, respectiv în domeniul combaterii spălării banilor sau al finanţării terorismului**.
A se vedea, de asemenea, art. 4 din Anexa nr. 1 la Ordinul nr. 3746/2020 privind organizarea şi funcţionarea Registrului central electronic pentru conturi de plăţi şi conturi bancare identificate prin IBAN şi pentru aprobarea procedurii privind obligaţia instituţiilor de credit, instituţiilor de plată şi instituţiilor emitente de monedă electronică de a furniza informaţii conform art. 61 din Legea nr. 207/2015 privind Codul de procedură fiscală (M.Of. nr. 1015 din 2 noiembrie 2020) și Ordinul Ministrului Finanțelor nr. 109 din 31 ianuarie 2022 pentru aprobarea Procedurii de înrolare și modalitățile de acces în PatrimVen (M. Of. nr. 136 din 10 februarie 2022).
Din acest din urmă act normativ este relevant în special art. 1.2 din Anexa nr. 2 care indică accesul la Registrul electronic pentru conturi de plăți și conturi bancare prevăzut la art. 61[1] din Codul de procedură fiscală inclusiv pentru autoritățile prevăzute la art. 1 din Legea nr. 129/2019, adică, așa cum am văzut, potrivit lit. a), **și pentru organele de urmărire penală**, precum și pentru autoritățile prevăzute la art. 3 din O.G. nr. 9/2021 privind stabilirea unor măsuri de facilitare a utilizării informaţiilor financiare şi a analizelor financiare în scopul prevenirii, depistării, investigării sau urmăririi penale a anumitor infracţiuni (M.Of. nr. 831 din 31 august 2021), adică, printre altele, **pentru Poliţia Română, Direcţia Generală Anticorupţie din subordinea Ministerului Afacerilor Interne. Parchetul de pe lângă Înalta Curte de Casaţie şi Justiţie - Secţia de urmărire penală şi criminalistică şi Secţia parchetelor militare, Direcţia Naţională Anticorupţie și Direcţia de Investigare a Infracţiunilor de Criminalitate Organizată şi Terorism**. Potrivit art. 3 alin. (2) din O.G. nr. 9/2021, accesul celorlalte unități de parchet la registrul centralizat de conturi bancare, respectiv la informaţii financiare şi analize financiare oferite de Oficiu se face prin intermediul Parchetului de pe lângă Înalta Curte de Casaţie şi Justiţie - Secţia de urmărire penală şi criminalistică.
Informațiile pot fi accesate pentru prevenirea infracţiunilor grave, adică acele infracţiuni de competenţa Europol, astfel cum acestea sunt definite la art. 2 alin. (2) lit. c) din Legea nr. 56/2018 privind cooperarea autorităţilor publice române cu Agenţia Uniunii Europene pentru Cooperare în Materie de Aplicare a Legii (Europol).

[62] Din păcate, deși metodele prevăzute la art. 146[1] și art. 153 C.pr.pen. sunt cât se poate de diferite, aspect pe care l-am explicat pe larg în articolul menționat anterior (*A.R. Trandafir, G. Marin,* Obținerea de informații ori înscrisuri de la instituțiile de credit în cursul urmăririi penale, cit. supra), în practica organelor de urmărire penală sunt în continuare solicitate de la instituțiile de credit în temeiul art. 153 C.pr.pen., deși obiectul solicitării are natura unei intruziuni care atrage aplicarea art. 146[1] C.pr.pen., adică se dorește comunicarea datelor privind tranzacțiile financiare (în general, a extraselor de cont).

financiară" în sensul prevăzut de Legea contabilității nr. 82/1991[63] care se referă, printre altele, la bilanțul contabil sau contul rezultatului exercițiului [art. 28 alin. (6)] ori de Ordinul nr. 1802/2014 pentru aprobarea Reglementărilor contabile privind situaţiile financiare anuale individuale şi situaţiile financiare anuale consolidate[64] care vorbește, de exemplu, de bilanț, cont de profit şi pierdere, situaţia modificărilor capitalului propriu, situaţia fluxurilor de trezorerie, notele explicative la situaţiile financiare anuale[65] etc. Într-un limbaj mai puțin academic, așadar, *situația financiară* a unei persoane în contextul art. 153 C.pr.pen. se referă la sumele de bani de care dispune aceasta (și care pot face obiectul măsurilor asigurătorii).

Putem însă extinde sfera de aplicare a acestui text de lege, în contextul în care monedele virtuale reprezintă o *reprezentare digitală a unei valori* și deci să interpretăm art. 153 C.pr.pen. ca incluzând anumite informații privind deținerea monedelor virtuale? Ar însemna să admitem că monedele virtuale țin de *situația financiară* a unei persoane, deci că exprimă valoric sumele de bani de care dispune o persoană. Or, dacă monedele virtuale sunt (doar) mijloc de schimb, așa cum prevede art. 180 alin. (4) C.pr.pen. (cel puțin la acest moment în țara noastră), înseamnă că ele nu arată în mod direct situația financiară a unei persoane în înțelesul art. 153 C.pr.pen., ci pot fi asemănate oricăror altor bunuri deținute de o persoană (de pildă, pentru a rămâne în sfera bunurilor incorporale, sunt similare părților sociale sau acțiunilor).

În cazul în care am trece peste această problemă, cine sunt *instituţiile care deţin date privind situaţia financiară a unei persoane* în cazul monedelor virtuale (dat fiind că instituțiile de credit nu au, cel puțin la acest moment, asemenea date)?

Problema trebuie tratată distinct după cum vorbim despre platforme de tranzacționare centralizate (CEX) și descentralizate (DEX). Astfel, în cazul celor din urmă, dat fiind că autentificarea se face prin intermediul unui portofel non-custodial, cheia criptografică privată aparținând titularului acestuia, nu există o instituție care deține date privind situația financiară (chiar dacă am admite că această noțiune include și monedele virtuale).

În schimb, în cazul platformelor de tranzacționare centralizate (CEX), dacă au implementat politicile *know your customer*, așa cum prevede art. 13 și urm. din Legea nr. 129/2019, ar trebui ca, pe baza numelui și a CNP-ului/CUI-ului unei persoane, acestea să poată furniza adresa publică necesară pentru verificarea tranzacțiilor efectuate și deci situației contului persoanei vizate.

În fine, admițând aplicarea textului de lege în cazul platformelor de tranzacționare centralizate (CEX), la ce se referă *existența și conținutul conturilor* în situația monedelor virtuale? Cu titlu de exemplu, un CEX poate clarifica următoarele aspecte: în ce măsură o anumită persoană deține un cont-client; în ce măsură prin intermediul acelui cont-client poate accesa unități valorice asociate unei anumite monede virtuale; care sunt monedele virtuale în legătură cu care clientul are un drept de creanță în raport cu CEX; în ce măsură monedele virtuale în discuție sunt asociate unei adrese publice generate pentru uzul individual al clientului sau discutăm despre o adresă publică folosită în comun de mai mulți utilizatori etc. Analiza se poate extinde în mod evident la toate tranzacțiile (și tipul tranzacțiilor) efectuate de către client, prin intermediului contului-client.

[63] M.Of. nr. 454 din 18 iunie 2008.
[64] M.Of. nr. 963 din 30 decembrie 2014.
[65] A se vedea, de exemplu, pct. 20-21 din Reglementările contabile privind situaţiile financiare anuale individuale şi situaţiile financiare anuale consolidate din 29.12.2014, parte integrantă din respectivul Ordin.

Una din informațiile care poate fi furnizată este, așa cum am văzut, adresa publică, pe baza căreia pot fi verificate, așa cum am arătat, inclusiv tranzacțiile efectuate de suspect sau inculpat. În opinia noastră, având în vedere că pe baza acestei adrese pot fi vizualizate tranzacțiile, noțiunea trebuie analizată mai degrabă în legătură cu art. 146[1] C.pr.pen., așa cum vom arată în cele ce urmează. Totodată, așa cum am văzut, în afară de adresa publică, platforma centralizată (CEX) poate oferi date despre situația „contului" unui utilizator - adică despre monedele virtuale deținute de acesta (denumire și cuantumul unităților valorice). Desigur, exact ca în cazul conturilor bancare, între momentul comunicării acestor informații și cel al luării eventualelor măsuri asigurătorii, situația contului - dar mai ales cea a valorii monedelor virtuale - poate să fie complet diferită.

2. Obţinerea datelor privind tranzacţiile financiare ale unei persoane (art. 146[1] C.pr.pen.)

Art. 146[1] C.pr.pen. reglementează obţinerea datelor privind tranzacţiile financiare ale unei persoane. Reamintim, în acest context, că textul de lege de referă atât la tranzacțiile financiare *efectuate* [alin. (1)], cât și cele care *urmează a fi efectuate* [alin. (2)], în ambele situații fiind necesară obținerea unui mandat emis de judecătorul de drepturi și libertăți, în situația în care există o suspiciune rezonabilă cu privire la pregătirea sau săvârşirea unei infracţiuni, măsura este necesară şi proporţională cu restrângerea drepturilor şi libertăţilor fundamentale, date fiind particularităţile cauzei, importanţa informaţiilor sau a probelor ce urmează a fi obţinute ori gravitatea infracţiunii, iar probele nu ar putea fi obţinute în alt mod sau obţinerea lor ar presupune dificultăţi deosebite ce ar prejudicia ancheta ori există un pericol pentru siguranţa persoanelor sau a unor bunuri de valoare. Având în vedere condiția de subsidiaritate prevăzută de textul de lege, obținerea datelor privind tranzacțiile financiare este, în mod evident, mult mai legată de noțiunea de probă decât obținerea datelor privind situația financiară a unei persoane. Așa cum am arătat însă, este posibil ca datele privind tranzacțiile să constituie probe privind comiterea unei infracțiunii, iar obținerea lor să prilejuiască inițiativa luării măsurii asigurătorii. Conturând astfel discuția, se ridică problema dacă art. 146[1] C.pr.pen. poate constitui temei pentru obținerea de date privind tranzacțiile efectuate cu monede virtuale.

Reamintim, în acest sens, și dispozițiile art. 138 alin. (9) C.pr.pen., potrivit cu care *„prin obţinerea datelor privind tranzacţiile financiare ale unei persoane se înţelege operaţiunile prin care se asigură cunoaşterea conţinutului* ***tranzacţiilor financiare şi al altor operaţiuni efectuate*** *sau* ***care urmează să fie efectuate*** *prin intermediul unei instituţii de credit ori al* ***altei entităţi financiare****, precum şi obţinerea de la o instituţie de credit sau de la altă entitate financiară de* ***înscrisuri ori informaţii*** *aflate în posesia acesteia* ***referitoare la tranzacţiile sau operaţiunile*** *unei persoane"* (subl. ns.). În înțelesul Codului de procedură penală, tranzacțiile financiare includ așadar tranzacțiile financiare propriu-zise (cele care presupun transferuri de fonduri - ex. transferuri de sume de bani între două conturi bancare), cât și operațiunile (ex. cele cu instrumente financiare[66]). Și de această dată, textul de lege a fost creat în special pentru a obține informații în legătură cu conturile bancare, legiuitorul neavând în niciun fel intenția de a reglementa monedele virtuale.

[66] Așa cum am văzut, unele criptoactive pot fi calificate ca instrumente financiare.

În contextul actual însă, prima întrebare la care trebuie să găsim răspuns este dacă tranzacțiile cu monede virtuale[67] sunt *tranzacții financiare* în sensul acestor texte de lege (adică dacă reprezintă tranzacții sau operațiuni). Dacă răspunsul este afirmativ, cine sunt *entitățile financiare* în situația tranzacțiilor cu monede virtuale?

În legătură cu prima întrebare, credem că este indubitabil că monedele virtuale pot face obiectul unei *tranzacții,* aspect care rezultă de altfel și din dispozițiile art. 180 alin. (4) C.pen. care vorbește despre *tranzacționarea* (electronică) a monedelor virtuale. Dacă tranzacția este și *financiară* este însă mai delicat. În sensul Codului de procedură penală, așa cum am arătat, tranzacțiile financiare includ transferurile de fonduri (unde tranzacțiile cu monede virtuale nu se încadrează), precum și operațiunile. Dacă, în sine, nu am vedea o problemă pentru a include tranzacțiile cu monede virtuale în categoria largă de *operațiuni*, art. 138 alin. (9) C.pr.pen. adaugă o condiție suplimentară, respectiv aceea ca tranzacțile să se desfășoare *prin intermediul unei instituții de credit ori al altei entităţi financiare.* Prima condiție alternativă este exclusă, cel puțin la acest moment neexistând, în țara noastră, *instituții de credit* prin intermediul cărora să se tranzacționeze monede virtuale. Nu am identificat o definiție general aplicabilă a sintagmei *entitate financiară*, însă probabil noțiunea cea mai apropiată este cea de *instituție financiară* prevăzută de art. 2 lit. g) din Legea nr. 129/2019, în mare parte preluată din Directiva nr. 2015/849[68]. Fără a reda aici întreaga definiție, extrem de vastă, a acestei noțiuni, din lecturarea textului de lege, se observă ușor că platformele prin intermediul cărora se tranzacționează monede virtuale nu se încadrează în niciuna din acele categorii de entități. De altfel, se observă că legiuitorul (nici cel național, nici cel european) nu a inclus în cadrul acestei noțiuni nici măcar furnizorii de servicii de schimb între monede virtuale şi monede fiduciare ori furnizorii de portofele digitale, care au doar calitatea de entitate raportoare, potrivit art. 5 lit. g^1) și g^2) din Legea nr. 129/2019.

Să presupunem însă că această problemă ar fi depășită (fie printr-o intervenție legislativă, fie pur și simplu printr-o interpretare largă a noțiunii de *entitate financiară*, care să nu se limiteze la cea prevăzută de Legea nr. 129/2019, mai ales că nivelul de intruziune în viața privată în cazul tranzacțiilor cu monede virtuale pare a fi similar cu cel existent în cazul conturilor bancare). Dacă organul de urmărire penală dorește deci să cunoască **tranzacțiile unei persoane, care au fost efectuate cu monede virtuale**, se va adresa platformei pe care acestea sunt tranzacționate. Și de data aceasta, cel puțin la acest moment, problema se pune doar în cazul platformelor de tranzacționare centralizate (CEX), întrucât cele

[67] Avem în vedere, în cele ce urmează, strict acele tranzacții efectuate cu monede virtuale, iar nu achiziționarea acestora cu moneda fiduciară, care se încadrează în mod evident în noțiunea de *tranzacții financiare* astfel cum aceasta este definită de art. 138 alin. (9) C.pr.pen. Pentru achiziționarea monedelor virtuale folosind moneda fiduciară, informațiile se pot obține însă de la instituțiile de credit. Obținerea unor asemenea informații de la platformele care permit direct și astfel de cumpărări de monedă virtuală (furnizorii de servicii de schimb între monede virtuale și monede fiduciare, potrivit art. 5 lit. g^1 din Legea nr. 129/2019) va depinde de calificarea noțiunii de „entitate financiară", așa cum va fi analizată în cele ce urmează.

[68] O altă definiție a instituțiilor financiare este cuprinsă în art. 4 alin. (1) pct. 26 din Regulamentul nr. 575/2013 privind cerinţele prudenţiale pentru instituţiile de credit şi firmele de investiţii şi de modificare a Regulamentului (UE) nr. 648/2012 (J.Of. al Uniunii Europene 176 din 27 iunie 2013). Nici această definiție nu acoperă situația platformelor de tranzacționare a monedelor virtuale, referindu-se, printre altele, la emiterea de monedă electronică.

descentralizate (DEX) nu dețin (sau nu sunt obligate să dețină) informațiile referitoare la titularii portofelelor non-custodiale[69].

În schimb, față de reglementarea obligațiilor furnizorilor de portofele digitale custodiale conținută în Legea nr. 129/2019, în special cele de înregistrare și *know your customer*, platformele centralizate ar putea comunica, pe baza numelui și a celorlalte date de identificare ale unei persoane, informații referitoare la tranzacții. Mai exact, aceste platforme ar putea furniza **adresa publică** pe baza căreia să poată fi vizualizate tranzacțiile efectuate de o anumită persoană. Chiar dacă s-a arătat că adresa publică este echivalentul contului IBAN[70], ceea ce este diferit este că simpla cunoaștere a contului IBAN (aspect permis de art. 153 C.pr.pen. sau, în cazurile analizate mai sus, direct prin intermediul sistemului PatrimVen) nu permite în niciun fel cunoașterea tranzacțiilor efectuare prin intermediul contului. În schimb, cunoașterea adresei publice conferă o astfel de posibilitate, ceea ce ne determină să o încadrăm în noțiunea de *informaţie referitoare la tranzacţiile sau operaţiunile unei persoane* astfel cum aceasta este prevăzută de art. 138 alin. (9) C.pr.pen. Prin urmare, în temeiul art. 146[1] C.pr.pen. astfel explicat, platformele de tranzacționare centralizate (CEX) ar putea oferi informații precum adresa publică ori direct cele privind tranzacțiile efectuate (dată, oră, destinatar, valoare etc.)[71]. Problema este aceea de a identifica acel CEX folosit de către suspect sau inculpat ca punct de intrare (on-ramp), punct de ieșire (off-ramp) sau ca mijloc de tranzacționare a monedei virtuale. Pentru aceasta, de multe ori va fi necesară o analiză complexă la nivel de blockchain (în eng., onchain analysis) pentru a urmări arborele tranzacțiilor cu monede virtuale și a putea concluziona în ce măsură una dintre adresele publice folosite în procesul de tranzacționare este sau nu asociată unui CEX. Fără a intra în detalii care excedează cu mult scopului acestui material, precizăm faptul că unele proiecte blockchain au dezvoltat instrumente software ce permit o astfel de analiză complexă de o manieră automată. În context, se poate pune problema în ce măsură organul de urmărire penală nu ar putea solicita entității din spatele unui anumit proiect blockchain să furnizeze aceste informații, în temeiul art. 170 CPP.

Cu privire la **tranzacțiile care urmează a fi efectuate**, o asemenea monitorizare ar putea fi realizată de oricare din cele două categorii de platforme, în măsura în care au implementat un astfel de mecanism de urmărire. Și în acest caz însă, cunoașterea adresei publice se poate dovedi suficientă pentru supravegherea respectivelor tranzacții[72].

---

[69] De altfel, Legea nr. 129/2019 se referă la *furnizorul de servicii de schimb între monede virtuale și monede fiduciare.* Or, având în vedere terminologia folosită de către legiuitor, credem că acesta a avut în vedere în mod exclusiv CEX-urile, nu și DEX-urile. Aceasta întrucât, accentul este pus pe schimbul (în realitate o vânzare sau o cumpărare) dintre o monedă virtuală și una fiduciară, nu pe schimbul între una sau mai multe monede virtuale. Cel puțin în momentul de față, DEX-urile operează doar cu monede virtuale (inclusiv cele stabile), nu și cu monede fiduciare.

[70] A se vedea *G. Zlati,* Tehnologia blockchain..., cit. supra., p. 38.

[71] A se vedea și *M.E. Peter,* cit. supra.

[72] O analiză la nivel de blockchain (on-chain) se poate realiza inclusiv de către un terț prin folosirea unor programe informatice specializate. Un exemplu relevant in acest sens este Chainanalysis (www.chainanalysis.com) ce folosește Chainanalysis Reactor pentru a genera o „hartă" a adreselor publice folosite în tranzacțiile efectuate în blockchain (on-chain), existând posibilitatea identificării „punctelor" de intrare (on-ramp) și de ieșire (off-ramp). A se vedea detalii în D. Srivasthav, L.P. Maddali, R. Vigneswaran, Sutdy of Blockchain Forensics and Analytics Tools, în 3rd Conference on Blockchain Research & Applications for Innovative Networks and Services, 2021, pp. 39-40.

3. Predarea datelor informatice [art. 170 alin. (2) lit. a) C.pr.pen.]

Un alt text de lege care ar putea fi, teoretic, invocat pentru solicitarea datelor privind monedele virtuale este art. 170 alin. (2) lit. a) C.pr.pen., potrivit cu care, în condițiile alin. (1) al textului de lege - adică în cazul în care există o suspiciune rezonabilă cu privire la pregătirea sau săvârşirea unei infracţiuni şi sunt temeiuri de a se crede că anumite date informatice pot constitui mijloc de probă în cauză - *„organul de urmărire penală sau instanţa de judecată poate dispune ca **orice persoană fizică sau juridică de pe teritoriul României** să comunice anumite **date informatice aflate în posesia sau sub controlul său**, care sunt stocate într-un sistem informatic ori pe un suport de stocare a datelor informatice*" (subl. ns.).

Două probleme principale se ridică în ceea ce privește posibilitatea de a folosi acest text de lege în legătură cu monedele virtuale. Astfel, în primul rând, cine sunt *persoanele de pe teritoriul României obligate să comunice anumite date informatice aflate în posesia sau sub controlul lor?* Având în vedere prevederile art. 30^1 din Legea nr. 129/2019, potrivit cu care furnizorii serviciilor de schimb între monede virtuale și monede fiduciare (din punctul nostru de vedere doar platformele de schimb/tranzacționare centralizate), cât și furnizorii de servicii de portofele digitale (din punctul nostru de vedere, doar cele în custodie) trebuie să fie autorizați și/sau înregistrați[73], obligația ar putea incumba acestor categorii de entități.

A doua problemă, și mai importantă, se referă la categoriile de date informatice care ar putea fi furnizate în temeiul art. 170 alin. (2) lit. a) C.pr.pen. De exemplu, tranzacțiile cu monede virtuale ori adresa publică sunt date informatice, însă, din punctul nostru de vedere, obținerea lor nu poate fi realizată în această procedură, ci, eventual, cu precizările arătate anterior, în cea prevăzută de art. 146^1 C.pr.pen. Avem în vedere, în acest sens, faptul că nivelul de intruziune în viața privată este similar celui avut în vedere de legiuitor în cazul tranzacțiilor cu moneda de cont, despre care Curtea europeană a drepturilor omului a afirmat în nenumărate rânduri că sunt protejate în temeiul art. 8 din Convenție[74]. De exemplu, într-una din cauze, s-a arătat că *„informațiile din documentele bancare conțin în mod indubitabil date personale privind o persoană fizică, chiar dacă sunt informații confidențiale sau nu. Aceste informații pot conține tranzacții profesionale și nu există nicio justificare pentru excluderea activităților care au natură profesională ori de afaceri din noțiunea de viață privată"*[75]. Pentru aceleași considerente, mai ales în contextul reglementării tot mai detaliate a tranzacțiilor cu monede virtuale și a posibilităților de comitere de infracțiuni prin intermediul acestora, apreciem că standardul de protecție trebuie să fie similar, ceea ce înseamnă, după cum am menționat, că art. 170 alin. (2) lit. a) C.pr.pen. nu poate constitui temei pentru obținerea datelor informatice de natura celor menționate anterior.

[73] A se vedea, pentru aceste aspecte, *G. Zlati,* Tehnologia blockchain..., cit. supra, p. 35.
[74] A se vedea CEDO, cauzele Sommer c. Germania, decizia din 27 aprilie 2017; M.N. și alții c. San Marino, decizia din 7 iulie 2015, Brito Ferrinho Bexiga Villa-Nova c. Portugalia, disponibile la adresa hudoc.echr.coe.int.
[75] A se vedea CEDO, cauza M .N. și alții c. San Marino, cit. supra, par. 51.

III. SPRE ADUCERE AMINTE: SCURTE CONSIDERAȚII PRIVIND OBIECTUL ȘI FINALITATEA MĂSURILOR ASIGURĂTORII ÎN PROCESUL PENAL

Așa cum am arătat cu altă ocazie[76], măsurile asigurătorii au fost definite de doctrină ca fiind măsuri procesuale care constau în indisponibilizarea, pe parcursul procesului penal, a bunurilor unor persoane, pentru ca acestea să nu le înstrăineze până la sfârşitul procesului penal şi să devină insolvabile[77]. Având în vedere extinderea obiectului măsurilor asigurătorii, am arătat că acestui scop trebuie să i se adauge şi altele, specifice finalităţilor acestor măsuri – de exemplu, asigurarea înlăturării unei stări de pericol ori a prevenirii săvârşirii de noi infracţiuni în cazul măsurilor de siguranţă.

Fără a relua discuțiile despre raportul dintre sechestrul asigurător și poprirea asigurătorie[78], în ceea ce privește **obiectul măsurilor asigurătorii**, subliniem concluzia potrivit căreia credem că, reglementând măsurile asigurătorii, legiuitorul a avut în vedere:

- **sechestrul penal**, înființat de regulă asupra bunurilor mobile corporale (art. 252 C.pr.pen.). Am arătat, într-o altă ocazie, că *„în principiu, în materie mobiliară, sechestrul se instituie asupra bunurilor corporale, dar poate avea ca obiect şi bunuri mobile incorporale, deoarece dispoziţiile legale, atât în materie civilă cât şi în penală, nu fac distincţie între bunurile corporale sau incorporale, stabilind numai că măsura se adoptă asupra bunurilor mobile. Atunci când bunurile mobile incorporale sunt datorate de un terţ, este aplicabilă poprirea”* [79];
- sechestrul asupra bunurilor imobile [**notarea ipotecară** – art. 253 alin. (4) C.pr.pen.];
- **poprirea** (art. 254 C.pr.pen.), care are ca obiect bunurile incorporale[80], adică de regulă o creanță, aspect care rezultă din formularea textului de lege: *„sumele de bani datorate cu orice titlu...”*. Desigur, art. 254 C.pr.pen. se completează cu cel al art. 781 C.pr.civ., potrivit căruia pot fi poprite, pe lângă sumele de bani datorate și *„titlurile de valoare sau alte bunuri mobile incorporale urmăribile datorate debitorului ori deținute în numele său de o a treia persoană sau pe care aceasta din urmă i le va datora în viitor, în temeiul unor raporturi juridice existente”*.

Având în vedere natura controversată a monedelor virtuale, la care ne-am referit anterior, rezultă că, dacă nu le recunoaștem nici măcar încadrarea în categoria largă de *bunuri*, măsurile asigurătorii ar fi excluse. În același context, trebuie făcută referire și la **finalitatea măsurilor asigurătorii,** așa cum rezultă din art. 249 alin. (1) C.pr.pen.; astfel, aceasta poate fi confiscarea specială, confiscarea extinsă, garantarea executării pedepsei

---

[76] A se vedea *A.R. Trandafir,* Comentariul art. 249 C.pr.pen., în *M. Udroiu* (coord.), Codul de procedură penală. Comentariu pe articole, ediția 4, Ed. CH Beck, București, 2022.

[77] A se vedea, de exemplu, *I. Neagu*, Tratat de procedură penală. Partea generală, Ed. Universul Juridic, Bucureşti, 2010, p. 622.

[78] A se vedea, pentru aceste aspecte, *A.R. Trandafir,* Comentariul art. 249 C.pr.pen., cit. supra, precum și *G.A. Lazăr, R. Stanciu. A.R. Trandafir, N.H. Țiț,* Poprirea - o triplă perspectivă: civilă, fiscală și penală, Ed. Hamangiu, București, 2021, p. 192 și urm.

[79] A se vedea *T.C. Briciu, A.R. Trandafir,* Incidenţa dispoziţiilor Codului de procedură civilă sau ale Codului de procedură fiscală în materia măsurilor asigurătorii luate în procesul penal. Concursul între măsurile asigurătorii luate în procesul penal şi titlurile executorii, în Revista Română de Drept Privat nr. 3/2014.

[80] A se vedea, pentru discuția privind poprirea privind bunurile corporale care pare a fi prevăzută de teza a doua a art. 781 alin. (1) C.proc.civ., *G.A. Lazăr, R. Stanciu. A.R. Trandafir, N.H. Țiț,* cit. supra, p. 37 și urm.

amenzii ori cheltuielile judiciare. Or, dacă monedele virtuale nu ar fi considerate nici măcar bunuri, acestea ar fi *de plano* excluse de la luarea măsurilor asigurătorii, dat fiind că însuși textul de lege vorbește despre evitarea ascunderii, distrugerii, înstrăinării sau a sustragerii de la urmărire a „bunurilor *care pot face obiectul confiscării speciale sau...".* O mențiune suplimentară trebuie să fie făcută în ceea ce privește cele două măsuri de siguranță, dat fiind că obiectul confiscării constă întotdeauna în niște *bunuri*.

În schimb, dacă admitem că ele sunt bunuri incorporale, măsura asigurătorie care ar putea fi, teoretic, instituită, este, în principiu, poprirea. În situația în care concepem monedele virtuale ca pe niște bunuri incorporale deținute efectiv de titularul acestora (iar nu de un terț), atunci nu ar fi exclusă înființarea sechestrului.

Prin urmare, în așteptarea calificării naturii juridice a monedelor virtuale de către legiuitor ori de către doctrina/jurisprudența de drept civil, ne mărginim să reținem că, în opinia noastră, monedele virtuale deținute pe platformele de tranzacționare centralizate (CEX) reprezintă bunuri incorporale deținute de un terț și pot fi supuse măsurii asigurătorii a **popririi**. În schimb, în cazul portofelelor non-custodiale și al platformelor de tranzacționare descentralizate (DEX), nu există un terț, monedele fiind deținute de titular, ceea ce conduce la ideea că măsura asigurătorie ce ar putea fi înființată este **sechestrul**. Prin urmare, distincția este relevantă în special pentru a putea vedea dacă terțul (platforma de tranzacționare, furnizorul de portofel digital etc.) are sau nu obligații în legătură cu respectiva măsură asigurătorie.

Menționăm totuși, că, în materie procesual penală, înființarea măsurilor asigurătorii nu este supusă unor condiții prealabile diferite, așa cum se întâmplă în cazul procedurii civile (i.e. existența somației). De asemenea, pentru moment, în materia monedelor virtuale, importanța identificării corecte a măsurii asigurătorii efectiv incidente este cu mult mai mică decât în cazul sumelor de bani din conturile bancare, având în vedere că excepțiile prevăzute de art. 729 și 781 C.pr.civ. nu sunt (cel puțin la acest moment) incidente, neputând fi acordate finanțări, salarii, alocații, indemnizații etc. sub formă de monede virtuale. Vom analiza așadar condițiile privind aducerea la îndeplinire și valorificarea măsurilor asigurătorii asupra monedelor virtuale fără a face distincție de fiecare dată în funcție de denumirea acestora, preferând să folosim termenul generic de „*măsură asigurătorie*".

IV. ADUCEREA LA ÎNDEPLINIRE A MĂSURILOR ASIGURĂTORII

Aducerea la îndeplinire a măsurilor asigurătorii ridică mai multe probleme practice. Și de data aceasta, problema se pune distinct după cum este vorba de platforme de tranzacționare centralizate (CEX) și portofele digitale în custodie (**1**) sau despre platforme de tranzacționare descentralizate (DEX) și portofele digitale non-custodiale (**2**). Vom analiza, totodată, rolul ANABI în procesul de aducere la îndeplinire a măsurilor asigurătorii (**3**).

Facem aceste precizări întrucât o indisponibilizare veritabilă a monedelor virtuale s-ar transpune în obținerea unui control exclusiv asupra acestora, prin intermediul cheii criptografice private, urmată de tranzacționarea monedelor virtuale către o altă adresă publică[81] (e.g. aflată sub controlul ANABI). În acest sens, cu titlu preliminar, prezintă relevanță următoarele două exemple la nivel de drept comparat:

[81] A se vedea în acest sens și *A.W. Balthazor*, op. cit., pp. 1226-1227.

- În cauza *Silk Road* autoritățile americane au reușit să obțină cheia criptografică privată stocată pe laptopul suspectului, obținând astfel acces la aproximativ 175,000 bitcoin[82].
- De asemenea, Departamentul de Justiție al SUA a făcut public recent faptul că a reușit să indisponibilizeze 94,000 bitcoin în valoare de 4.5 miliarde de dolari obținuți ca urmare a atacului informatic din anul 2016, îndreptat împotriva Bitfinex (CEX). Din comunicatul de presă rezultă că moneda virtuală a putut să fie indisponibilizată prin accesarea portofelului digital al suspecților, cheia criptografică privată fiind recuperată din conturile acestora de cloud.[83]

La nivel de principiu, nu pot să fie ignorate următoarele aspecte:

i. Indisponibilizarea setului de cuvinte cheie (în eng., *seed phrase* sau *mnemonic phrase*) necesar pentru recuperarea portofelului digital nu se transpune în limitarea accesului la acesta ori la monedele virtuale. De asemenea, recuperarea unui portofel digital pe un alt dispozitiv, utilizând un *seedphrase/mnemonic* phrase, se va transpune în crearea unui nou „punct de acces" la monedele virtuale – fără a discuta însă despre o restricționare a accesului. Astfel, în măsura în care făptuitorul va avea acces la portofelul digital ori la setul de cuvinte cheie va putea exercita un control asupra monedelor virtuale, fără ca organele de urmărire penală să se poată opune.

ii. Indisponibilizarea portofelului digital non-custodial nu se va transpune *per se* în indisponibilizarea monedelor virtuale susceptibile de a fi accesate prin intermediul acestuia. Făcând o paralelă, este ca și cum s-ar indisponibiliza cheia de acces la un seif, fără a se indisponibiliza în mod efectiv și conținutul acestuia. În măsura în care făptuitorul cunoaște setul de cuvinte cheie necesar pentru recuperarea portofelului digital pe un alt dispozitiv, va putea în orice moment să creeze un nou punct de acces la monedele virtuale (a se vedea *supra*, pct. i).

1. Situația platformelor de tranzacționare centralizate și a portofelelor digitale în custodie

În cazul *platformelor de tranzacționare centralizate* (CEX), așa cum arătam, măsura asigurătorie care ar trebui înființată este poprirea, monedele virtuale fiind „deținute" de un terț (CEX-ul) în numele persoanei față de care se dispun măsuri asigurătorii. Prin urmare, organul competent să aducă la îndeplinire măsura asigurătorie potrivit art. 251 C.pr.pen. va transmite actul prin care s-a înființat măsura și cel prin care se aduce la îndeplinire respectiva măsură către deținătorul acestei platforme. De cele mai multe ori, acesta va fi o persoană juridică de naționalitate străină, însă, având în vedere obligațiile de înregistrare prevăzute de Legea nr. 129/2019, identificarea acestei persoane juridice nu este greu de

[82] Idem, p. 1234.
[83] A se vedea în acest sens *Department of Justice*, Two Arrested for Alleged Conspiracy to Launder $4.5 Billion in Stolen Cryptocurrency, 8.02.2022, comunicat de presă disponibil pe pagina https://www.justice.gov/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency.

făcut.[84] În același fel funcționează lucrurile și pentru *furnizorii de portofele digitale în custodie*[85], care de regulă vor fi tot CEX-uri.

Mai departe, se pune problema de a ști ce poate face în mod concret CEX-ul ori furnizorul de portofele digitale în custodie. Astfel, platforma poate restricționa accesul la contul de client al persoanei ale căror monede virtuale sunt supuse măsurilor asigurătorii, ceea ce echivalează cu restricționarea accesului la monedele respective și imposibilitatea efectuării de tranzacții cu acestea. Dacă măsura asigurătorie ar viza doar anumite monede virtuale sau doar anumite unități valorice, CEX ar putea limita inclusiv parțial accesul la fonduri.[86]

Pentru a compara cu situația conturilor bancare, în acel caz, poprirea nu antrenează o imposibilitate de a accesa contul, ci doar o indisponibilizare a sumelor existente, în limita impusă de actul prin care se înființează măsura. Desigur, dacă din punct de vedere tehnic platforma permite acest lucru - indisponibilizarea propriu-zisă a monedelor virtuale - nu ar fi necesară blocarea accesului la conturi, ci ar fi suficientă această măsură.

Și furnizorul de portofele digitale în custodie are aceleași posibilități ca platforma de tranzacționare centralizată (CEX) - restricționarea accesului la respectivul portofel ori indisponibilizarea doar a anumitor monede virtuale. De altfel, atunci când discutăm despre un portofel digital în custodie ne vom raporta îndeosebi la CEX.

O problemă importantă, într-o astfel de situație, va fi legată de evaluarea monedelor virtuale - care va fi valoarea avută în vedere de organul care aduce la îndeplinire măsura? În legătură cu acest aspect, am făcut unele mențiuni *supra*[87]. În încercarea de a tranșa această problemă, credem că valoarea unei monede virtuale este fie cea rezultată pe CEX (valoare influențată de lichiditate, cerere și ofertă), fie valoarea rezultată din agregarea unui set de date preluat de pe principalele CEX-uri. La acest moment, avem unele rezerve că valoarea unei monede virtuale ar putea să fie stabilită printr-o constatare tehnico-științifică ori a expertiză, prin raportare la o metodologie proprie a specialistului ori expertului.

2. Situația platformelor de tranzacționare descentralizate și a portofelelor digitale non-custodiale

În cazul platformelor de tranzacționare descentralizate (DEX) și al portofelelor digitale non-custodiale, nu s-ar putea impune furnizorului serviciului să restricționeze accesul la monedele virtuale, deoarece acesta nu are o asemenea posibilitate din punct de vedere tehnic. Prin urmare, o indisponibilizare efectivă a monedelor virtuale s-ar putea realiza doar în măsura în care organul judiciar ar dobândi controlul asupra cheii criptografice private și ar dispune efectuarea unei tranzacții cu monedă virtuală către o adresă publică aflată sub controlul acestuia sau a unei terțe entități (e.g. ANABI).

---

[84] Precizăm totuși faptul că, până la redactarea prezentului material, nu au fost încă adoptate normele metodologice cu privire la înregistrarea acestor entități.

[85] Legea nr. 129/2019 nu se referă în mod explicit la portofelele digitale în custodie, dar din definiția acestora rezultă că nu au fost avute în vedere și portofelele digitale non-custodiale.

[86] De altfel, au existat situații în care CEX-ul (e.g. Binance, Kraken etc.) a restricționat tranzacțiile cu anumite monede virtuale pentru a permite actualizarea ori remedierea unor probleme apărute la nivel de blockchain. Chiar dacă o astfel de restricționare a vizat toți clienții, nu este exclusă posibilitatea ca aceasta să fie implementată de o asemenea manieră încât să vizeze doar anumite conturi de utilizatori.

[87] A se vedea pct. I.5.

Așa cum am precizat deja *supra*, simpla indisponibilizare a unui portofel digital non-custodial de tip hardware (e.g. Nano Ledger) nu se transpune în indisponibilizarea monedelor virtuale așa cum indisponibilizarea unei chei de la o casă de valori nu se transpune în indisponibilizarea banilor sau valorilor conținute de aceasta. Suspectul sau inculpatul va avea posibilitatea teoretică de a utiliza în continuare monedele virtuale prin utilizarea setului de cuvinte (*mnemonic phrase* sau *seed phrase*) ce permite importarea portofelului digital non-custodial pe un alt dispozitiv.

În acest context, se pune problema în ce măsură organele judiciare ar putea apela la instituția percheziției informatice (**2.1**) ori a accesului la un sistem informatic (**2.2)** în scopul dobândirii accesului la portofelul digital non-custodial și efectuarea unei tranzacții cu monedă virtuală la o altă adresă publică.

2.1. Limitele percheziției informatice

Având în vedere că un portofel digital non-custodial poate să fie atât un tip dispozitiv (e.g. Nano Ledger), cât și un program informatic (aplicație) instalat pe un sistem informatic (laptop, PC sau telefon mobil inteligent), ne putem întreba, mai întâi, în ce măsură s-ar putea dispune efectuarea unei percheziții informatice potrivit art. 168 C.pr.pen.

În ceea ce ne privește, răspunsul este unul pozitiv, având în vederea că percheziția informatică poate fi efectuată asupra oricărui sistem informatic ori mijloc de stocare a datelor informatice. Cu toate acestea, apreciem că prin intermediul percheziției informatice nu se poate accesa portofelul digital. De asemenea, este exclusă posibilitatea efectuării unei tranzacții cu monedă virtuală, la o altă adresă aflată sub controlul organului de urmărire penală ori a unei terțe entități (e.g. ANABI).

În primul rând, din interpretarea art. 168 alin. (1) C.pr.pen. rezultă că toate activitățile specifice percheziției informatice au ca scop strângerea de probe (digitale). Or, un asemenea demers este incompatibil *de plano* cu scopul luării măsurilor asigurătorii. De asemenea, accesarea portofelului digital excedează sferei percheziției informatice, luând forma unui veritabil acces la un sistem informatic.

Nu în ultimul rând, strângerea de probe nu poate echivala cu efectuarea unei tranzacții cu monedă virtuală. Această activitate specifică percheziției informatice echivalează cu crearea unei copii după datele informatice identificate într-o sursă terță aflată sub controlul organului de urmărire penală. Or, în cazul unei tranzacții cu monedă virtuală nu discutăm despre un „transfer" propriu-zis, lipsind o copiere ori a relocarea a datelor informatice. Din punct de vedere tehnic, o tranzacție cu monedă virtuală ia forma unei introduceri de date informatice în următorul bloc de date din blockchain, fiind generat așadar un set de date noi ce nu corespunde cu setul de date precedent.

În ceea ce ne privește, percheziția informatică ar putea fi folosită doar în scopul obținerii setului de cuvinte cheie (*seed phrase* sau *mnemonic phrase*) necesar pentru recuperarea portofelului digital, în măsura în care acte date informatice sunt stocate pe entitatea percheziționată.

2.2. Limitele accesului la un sistem informatic

La prima vedere, nu ar exista un impediment pentru utilizarea măsurii de supraveghere tehnică, constând în accesarea unui sistem informatic [art. 138 alin. (1) lit. b)

C.pr.pen.], în scopul accesării unui portofel digital și efectuarea unei tranzacții cu monedă virtuală. Totuși, la o analiză atentă, rezultă că un astfel de acces ar putea fi calificat ca fiind unul transfrontalier. Astfel, accesarea portofelului digital și efectuarea unei tranzacții cu monedă virtuală se transpune într-o interacțiune la nivel logic cu rețeaua blockchain, care operează prin intermediul nodurilor (sisteme informatice) situate din punct de vedere geografic în multiple jurisdicții[88]. Sub acest aspect, apreciem că se poate face o paralelă cu accesarea datelor în *cloud*.

Chiar dacă art. 32 din Convenția privind criminalitatea informatică face vorbire despre accesarea datelor disponibile (în eng., *open source*), indiferent de locația geografică în care acestea sunt stocate, apreciem că ipoteza accesării unui portofel digital și efectuarea unor tranzacții cu monedă virtuală diferă în mod semnificativ. Astfel, analiza datelor din blockchain prin intermediul unui *blockchain explorer* (a se vedea *supra*) echivalează cu citirea datelor disponibile într-o sursă deschisă (e.g. o pagină web accesibilă publicului). În schimb, accesarea unui portofel digital și efectuarea de tranzacții cu monedă virtuală se transpune într-o interacțiune logică cu rețeaua blockchain ce este condiționată de folosirea unui set de chei criptografice private. Discutăm așadar despre un acces condiționat și nu despre accesarea unei surse deschise, în ciuda faptului că în cazul unui blockchain discutăm despre un registru public descentralizat.

Dincolo de caracterul transfrontalier al accesului, se pune problema în ce măsură efectuarea unei tranzacții cu monedă virtuală este o activitate prevăzută de lege. Din definiția accesului [art. 138 alin. (3) C.pr.pen.] rezultă fără echivoc că legiuitorul a avut în vedere în mod limitativ „pătrunderea" într-un sistem informatic ori mijloc de stocare a datelor informatice. Prin urmare, singura posibilitate este aceea de a ne raporta la activitățile conexe accesului, prevăzute la art. 141 alin. (5) C.pr.pen. – realizarea și conservarea unei copii după datele informatice; suprimarea accesării datelor informatice; îndepărtarea datelor informatice din sistemul informatic accesat.

În ceea ce privește realizarea și conservarea unei copii după datele informatice identificate, apreciem ca fiind evident că această activitate conexă nu acoperă o tranzacție cu monedă virtuală. Concluzia rămâne valabilă și în ceea ce privește îndepărtarea datelor informatice din sistemul informatic accesat. O asemenea activitate ar putea avea la bază o ștergere de date informatice, urmare inexistentă în contextul efectuării unei tranzacții cu monedă virtuală. În schimb, s-ar putea susține că suprimarea accesării datelor informatice ar putea echivala cu efectuarea unei tranzacții cu monedă virtuală, acestea nemaifiind accesibile la adresa publică aflată sub controlul făptuitorului.

3. Rolul ANABI în aducerea la îndeplinire a măsurilor asigurătorii privind monedele virtuale

În acest context, trebuie menționat și că, potrivit art. 28 alin. (1) din Legea nr. 318/2015 pentru înfiinţarea, organizarea şi funcţionarea Agenţiei Naţionale de Administrare a Bunurilor Indisponibilizate şi pentru modificarea şi completarea unor acte normative[89], solicitarea procurorului sau a instanţei de judecată, Agenţia (ANABI) depozitează temporar şi

[88] Nu este exclusă *de plano* posibilitatea ca toate nodurile din rețeaua blockchain să fie situate geografic în aceeași jurisdicție. Totuși, în ceea ce privește Bitcoin sau alte rețele blockchain consacrate (e.g. Ethereum, Cardano, Elrond etc.), această posibilitate este totuși exclusă.
[89] M.Of. nr. 861 din 24 decembrie 2015.

administrează bunurile mobile indisponibilizate a căror valoare individuală depăşeşte, la momentul dispunerii măsurii asigurătorii, echivalentul în lei al sumei de 15.000 euro; în acest scop, Agenţia este numită custode, în sensul art. 252 alin. (9) din Legea nr. 135/2010, cu modificările şi completările ulterioare.

De exemplu, ANABI a anunțat că, în cadrul unui dosar unde au fost dispuse măsuri asigurătorii privind trei monede virtuale (bitcoin, Tether - USDT, ether), *„din dispoziţia procurorului, pe parcursul lunii decembrie 2021, au fost preluate în administrare de către ANABI”*[90]. În mod evident, o asemenea „preluare în administrare” se putea realiza doar în urma unei tranzacții cu monedă virtuală de la adresa publică a persoanei care a făcut obiectul măsurii asigurătorii, la adresa publică aflată sub controlul ANABI.

V. VALORIFICAREA MONEDELOR VIRTUALE SUPUSE MĂSURILOR ASIGURĂTORII

Depășind problema măsurii asigurătorii instituite efectiv asupra monedelor virtuale și cea a aducerii la îndeplinire a respectivelor măsuri, se pune problema ce se întâmplă mai departe, în situația în care se dorește valorificarea bunurilor astfel indisponibilizate. O astfel de valorificare ar putea fi realizată în cursul procesului penal, în procedura prevăzută de art. 252^1 și urm. C.pr.pen. ori ulterior, în faza de executare silită.

Astfel, art. 252^1 alin. (2) C.pr.pen. prevede *cazurile speciale de valorificare a bunurilor mobile sechestrate* la cererea proprietarului sau cu acordul acestuia. Aceleași situații sunt incidente în faza urmăririi penale și în ipoteza în care nu există acordul proprietarului, potrivit art. 252^2 C.pr.pen.; pentru valorificarea bunurilor în faza judecății, sunt relevante dispozițiile art. 252^3 C.pr.pen.

Dintre aceste situații, în ceea ce privește monedele virtuale ar putea fi incident cazul prevăzut la lit. a) - atunci când, în termen de un an de la data instituirii sechestrului, valoarea bunurilor sechestrate s-a diminuat în mod semnificativ, respectiv cu cel puţin 40% în raport cu cea de la momentul dispunerii măsurii asigurătorii. În special pentru monedele virtuale a căror evoluție poate fi ușor urmărită, organul de urmărire penală ori instanța ar putea să constate destul de ușor respectiva diminuare a valorii monedelor, în vederea demarării procedurii de valorificare.

Se ridică problema în ce măsură poate deveni aplicabilă inclusiv lit. d) a textului de lege - atunci când sechestrul asigurător s-a aplicat asupra unor bunuri a căror depozitare sau întreţinere necesită cheltuieli disproporționate în raport cu valoarea bunului. Apreciem totuși că această teză nu poate fi incidentă, deoarece deținerea de monedă virtuală prin intermediul unui portofelul digital non-custodial nu implică alte costuri decât cele necesare pentru achiziționarea portofelului digital – în măsura în care se utilizează în acest sens un portofel digital tip dispozitiv (e.g. Nano Ledger). Ulterior, singurul cost vizează costul de tranzacționare cu privire la o anumită monedă virtuală.

Valorificarea efectivă a bunurilor mobile sechestrate se realizează de Agenția Națională de Administrare a Bunurilor Indisponibilizate (ANABI), potrivit art. 29 din Legea nr. 318/2015. Conform alin. (5) al acestui text de lege, valorificarea bunurilor prevăzute la alin. (1) se realizează: de către Agenţie, prin licitaţie publică; de către entităţi sau societăţi specializate, selectate cu respectarea prevederilor legale privind achiziţiile publice; prin

[90] A se vedea știrea disponibilă la această adresă.

intermediul executorilor judecătoreşti, potrivit procedurilor proprii; de către organele fiscale, potrivit procedurilor proprii de valorificare.

În acest sens, ANABI a anunțat încă din luna octombrie 2020 organizarea a două licitații publice pentru moneda virtuală bitcoin și ether[91]. Anunțurile menționau că *„având în vedere natura bunului mobil scos la licitație, la finalizarea procedurii, adjudecatarul va trebui să comunice Agenției, în vederea efectuării transferului, adresele publice de BTC, respectiv ETH, asociate unei platforme de tranzacționare de monedă virtuală. Platforma trebuie să aparțină unei entități juridice care se supune normelor legislative privind funcționarea şi operarea de instrumente financiare ale statului unde este înregistrată ca entitate juridică. Totodată, respectiva platformă trebuie sa aibă un proces de înregistrare a utilizatorilor de tip "cunoaștere a clientelei" (KYC - know your customer) și să respecte procedurile și standardele interne și internaționale privind prevenirea şi combaterea spălării banilor".* Finalitatea acestei proceduri este efectuarea unei tranzacții cu monedă virtuală, la adresa publică indicată de către adjudecatar. În mod evident, discutăm aici despre efectuarea unei tranzacții de la adresa publică controlată de ANABI la adresa publică furnizată de către adjudecatar. Necesită însă precizat faptul că ANABI solicită ca adresa publică să fie asociată unui CEX care are implementat un proces de cunoaștere a clientelei, fiind așadar exclusă posibilitatea indicării unei adrese publice accesibile prin intermediul unui portofel digital non-custodial. Menționăm totodată că monedele virtuale respective au fost vândute la licitație[92]. În concret, adjudecatarul a achiziționat de la ANABI monedă virtuală, plătind în schimbul acesteia monedă fiduciară.

În ceea ce privește valorificarea, *ulterior obținerii titlului executoriu*, a monedelor virtuale indisponibilizate, aceasta se face potrivit dispozițiilor aplicabile executării silite. De pildă, dacă este vorba de monede virtuale confiscate, valorificarea acestora se va face în conformitate cu prevederile O.G. nr. 14/2007 pentru reglementarea modului şi condiţiilor de valorificare a bunurilor intrate, potrivit legii, în proprietatea privată a statului[93].

[91] A se vedea știrea disponibilă la această adresă.
[92] A se vedea știrile disponibile aici și aici.
[93] M.Of. 694 din 23 septembrie 2014.