ANALELE ȘTIINȚIFICE ALE UNIVERSITĂȚII „ALEXANDRU IOAN CUZA” DIN IAȘI
TOM LXVIII, SUPLIMENT 1, ȘTIINȚE JURIDICE, 2022

DOI: 10.47743/jss-2022-68-2-15

Consideraţii privind implicaţiile monedelor virtuale în sfera infracţională şi modalităţi de investigare a infracţiunilor săvârşite prin intermediul lor

Considerations on the implications of virtual currencies in the criminal sphere and ways of investigating the crimes committed through them

Marius-Cosmin Macovei[1], **Rareş-Vasile Voroneanu Popa**[2]

Rezumat: Prezenta lucrare analizează aspecte de ordin general privind implicaţiile monedelor virtuale în sfera infracţională şi modalităţi abordate de experţi criminalişti în cercetarea infracţiunilor economico – financiare săvârşite cu ajutorul acestora. Monedele virtuale sau criptomonedele reprezintă un fenomen complex şi se află într-o permanentă evoluţie de cel puţin zece ani, fapt ce coincide cu dezvoltarea ansamblului de metode, procese, operaţii făcute sau aplicate asupra materialelor şi datelor denumit tehnologie, care ocupă un loc vital în „lumea reală”. Datorită caracterului imprevizibil, speculativ şi subteran, dar şi a gradului de confidenţialitate ridicat al tranzacţiilor, au devenit un mijloc facil de efectuare de activităţi ilicite, în special din domeniul economico – financiar, pentru persoanele din sfera criminalităţii organizate. În acest context, statele se adaptează la această modalitate de comitere a infracţiunilor şi depun eforturi susţinute în adoptarea şi aplicarea de politici penale de prevenire şi combatere a acestui fenomen.

Cuvinte-cheie: criminalistică, criptomonede, investigare, criminalitate organizată, economic, financiar.

Abstract: This paper examines general issues regarding the implications of virtual currencies in the criminal sphere and ways approached by forensic experts in the investigation of economic and financial crimes committed with their help. Virtual currencies or cryptocurrencies are a complex phenomenon and have been constantly evolving for at least ten years, coinciding with the development of the set of methods, processes, operations performed or applied on materials and data called technology, which occupies a vital place in „the real world ”. Due to the unpredictable, speculative and underground nature, but also to the high degree of confidentiality of transactions, they have become an easy means of carrying out illicit activities, especially in the

[1] Consilier juridic, Asociația Profesională Colegiul Consilierilor Juridici din Iași, Master în Drept, Specializarea Criminalistică, email: mariuscosminmacovei@gmail.com.

[2] Asistent univ. dr., Universitatea de Medicină și Farmacie „Grigore T. Popa” Iași, email: raresvoroneanu95@yahoo.com.

economic-financial field, for people in the field of organized crime. In this context, States are adapting to this way of committing crimes and are making sustained efforts to adopt and implement criminal policies to prevent and combat this phenomenon.

Keywords: forensics, cryptocurrencies, investigation, organized crime, economic, financial.

1. Introducere

Internetul, mediul virtual şi tehnologiile informaţionale şi de comunicare sunt elemente foarte importante pentru prezent, care este influenţat de procesul global de informatizare al societăţii, prin creşterea complexităţii în utilizarea informaţiei şi dezvoltarea tehnologiei de profil. Întreaga societate este afectată de internet şi de progresul tehnologic aferent, devenind o societate informaţională. [3]

În acest sens, apariţia şi evoluţia internetului poate fi privită atât prin ochii unui pesimist:*„(...) odată ce noi, oamenii, ne vom pierde importanţa funcţională pentru reţea (aceasta fiind preluată de inteligenţa artificială – n.n.), vom descoperi până la urmă că nu suntem apogeul creaţiei. Etaloanele pe care noi înşine le-am păstrat cu sfinţenie ne vor condamna să ne alăturăm mamuţilor şi delfinilor chinezeşti, fiind daţi cu totul uitării. Privind în urmă, omenirea se va dovedi a fi fost doar o undă în fluxul cosmic de date*"(Y. N. Harari[4]) cât şi prin cei ai unui optimist: „*Nu mă preocupă inteligenţa maşinilor. Noi vom evolua împreună cu aceasta şi pentru o perioadă foarte lungă de timp va fi în slujba sau va deveni un aspect al Homo sapiens cybernetica. S-ar putea să evolueze dincolo de noi, dar asta nu este o problemă (...) Dacă se va întâmpla aşa, va ocupa o nişă ecologică diferită. Va opera la viteze diferite şi la scări temporale relevante. În contextul respectiv, inteligenţa artificială nu va face deosebire între oameni, roci şi procese geologice. Noi am evoluat pe lângă o mulţime de specii şi multe dintre ele se descurcă bine*"(J. Lubin[5]). În cele din urmă, adevărul se află undeva la mijloc, la cel ce priveşte realist: „*Avem o tehnologie – tehnologia blockchain – de ce să nu o folosim?*"[6].

Dezvoltarea internetului a dinamizat relaţiile sociale, economice, culturale. Planeta noastră a devenit dintr-odată prea mică pentru dorinţa oamenilor de a comunica, de a schimba impresii, cunoştinţe, produse. Astfel, lumea virtuală a devenit spaţiul unde ne facem cumpărăturile, plătim pentru diverse servicii, aplicăm pentru joburi sau facem tranzacţii.

---

[3] C. Simulescu, *Bitcoin – moneda viitorului sau un pariu eșuat?*, Editura Printech, București, 2015, p. 6.

[4] Y. N. Harari (https://www.ynharari.com/), istoric israelian, filosof, profesor titular la Departamentul de Istorie al Universității Ebraice din Ierusalim, autor al cărților de succes internațional *Sapiens: Scurtă istorie a omenirii* și *Homo Deus: Scurtă istorie a viitorului.*

[5] J. Lubin, antreprenor canadiano-american, fondator ConsenSys, un studio de producție de software din Brooklyn și confondator al Ethereum, platformă descentralizată de criptomonede.

[6] M. A. Hotca, [Online] la https://htcp. eu/blockchainul-criptomonedele-si-evaziunea-fiscala/ , accesat la 28.05.2021.

Mai mult, acestea se pot realiza nu numai cu bani reali (cash sau card), ci şi cu criptomonede sau bani virtuali.[7] Tehnologia ce stă la baza acestora – blockchain – reprezintă o inovaţie ce ar revoluţiona în sens pozitiv domeniul economico – financiar, cum ar fi, de exemplu, stimularea incluziunii financiare prin a crearea şi oferirea unor modalităţi de plată mai facile, la costuri mai reduse celor ce nu deţin conturi în bănci, precum cei din statele cu venituri mai mici[8].

După puţin peste un deceniu de la apariţia lor, criptomonedele au crescut atât ca număr, cât şi ca valoarea pe piaţă, fiind o realitate a zilelor noastre. Dar, cu toate acestea, ele reprezintă în continuare un mister.

Prima criptomonedă lansată a fost bitcoin, fapt ce pentru anumite categorii de persoane a reprezentat o revoluţie a sistemului de plăţi, dar şi a investiţiilor cu caractere speculative. În acelaşi timp, autorităţile au trecut de la sentimente de indiferenţă şi prudenţă faţă de investitori şi publicul nevăzut la unele de interdicţii, care au devenit mult mai frecvente odată cu dinamica fenomenului. Pe lângă bitcoin, au mai apărut şi alte criptomonede, precum Ethereum (ETH), Ripple (XRP), Stellar (XLM), Dogecoin (DOGE), Elrond (EGLD), etc.[9]

2. Noţiuni generale

Criptomonedele constituie rezultatul unei imixtiuni de realizări din diferite ştiinţe, precum reţea, peer-to-peer, criptografie (funcţii hash, semnături digitale) şi economie (teoria jocurilor), astfel devenind un instrument / bun în format digital, existent într-un sistem criptografic specific, ce constă, în general, dintr-o reţea – peer-to-peer (P2P), un mecanism de încredere şi un public şi o infrastructură de tip cheie publică şi privată.

Reprezintă o formă de monedă digitală descentralizată, pentru care nu este nevoie o autoritate centrală, precum o unitate bancară, care să aprobe tranzacţiile.

Începuturile criptomonedelor datează încă din anul 2008, anul apariţiei primei şi devenită cea mai cunoscută dintre toate – Bitcoin (BTC, termen folosit pe piaţa de trading). Aceasta a fost inventată de către Satoshi Nakamoto, persoană sau grup de persoane încă necunoscute. Ulterior, în anul 2010, i-a predat Gavin Andersen controlul asupra depozitului şi cheii de alertă de reţea.

În anii 2011 – 2012, după o perioadă lungă de a face cunoscut conceptul, criptomonedele şi-au făcut apariţia şi au devenit utile şi pe piaţa neagră, când au apărut primii mari utilizatori ai acestei criptomonede, precum Silk Road.

Drept urmare, se poate deduce faptul că monedele virtuale au ca şi caracteristici: 1)natura descentralizată; 2)confidenţialitate; 3) anonimitate; 4) accesibilitate; 5) libertate. Pe lângă acestea, datorită globalizării, criptomonedele au

---

[7] [Online] la https://www.investopedia.com/terms/s/silk-road.asp , accesat la 28.05.2021.

[8] [Online] la https://blogs.imf.org/2018/03/13/addressing-the-dark-side-of-the-crypto-world/?cid=sm-com-FB , accesat la 28.05.2021.

[9] M. Gust, *Cryptocurrencies. Technical and functional aspects*, The Journal Contemporary Economy, Vol. 3, Issue 3/2018.

şi o trăsătură transfrontalieră – privită atât ca un avantaj, fiind uşor de tranzacţionat între orice locuri de pe glob, cât şi ca un dezavantaj, din perspectivă penală, din cauza existenţei paradisurilor fiscale sau a lipsei reglementărilor în privinţa infracţiunilor de spălare de bani sau finanţarea terorismului.[10]

3. Repere legislative

Moneda virtuală a fost definită de Banca Centrală Europeană în 2012, într-un raport al acesteia, ca fiind un tip de monedă digitală încă nereglementată, care este emisă li controlată de către dezvoltatorii acesteia şi care este acceptată de către membrii comunităţii virtuale specifice. În raport se identifică existenţa a trei tipuri de monede virtuale, după criteriul posibilitatea de interacţiune a monedei virtuale cu lumea reală şi monedele reale, respectiv: 1)scheme închise de monedă virtuală, ce sunt folosite în jocurile online şi nu au aproape nicio legătură cu lumea reală; 2) scheme cu flux unidirecţional de monedă virtuală, unde aceasta poate fi achiziţionată la schimb cu bani reali, la un anumit curs de schimb, însă moneda virtuală nu se poate schimba înapoi cu bani reali; 3) scheme de flux bidirecţional de monedă virtuală, în cadrul cărora aceasta poate fi cumpărată şi vândută la un anumit curs. Monedele virtuale create şi dezvoltate până în prezent, anterior menţionate, se încadrează în această ultimă categorie, acestea putând fi folosite ca monede de schimb atât pentru monede naţionale, cât şi pentru bunuri şi servicii, în lumea reală şi lumea virtuală, unde se permite şi se acceptă.[11]

Conform art. 1 pct. 1 lit. d) din Directiva (UE) 2018/843 a Parlamentului European şi a Consiliului din 30 mai 2018 de modificare a Directivei 2015/849 privind prevenirea utilizării sistemului financiar în scopul spălării banilor sau finanţării terorismului, precum şi de modificare a Directivelor 2009/138/CE şi 2013/36/UE[12], ”*moneda virtuală*” este definită ca fiind ”*o reprezentare digitală a valorii care nu este emisă sau garantată de o bancă centrală sau o autoritate publică, nu este în mod obligatoriu legată de o monedă instituită legal şi nu deţine statutul legal de monedă sau de bani, dar este acceptată de către persoane fizice sau juridice ca mijloc de schimb şi care poate fi transferată, stocată şi tranzacţionată în mod electronic;”.*

În legislaţia din România, moneda virtuală a fost menţionată prima dată în Legea 30 din 2019 pentru aprobarea Ordonanţei de Urgenţă a Guvernului nr. 25 din 2018[13] privind modificarea şi completarea unor acte normative, precum şi pentru

---

[10] R. Houben, A. Snyers, *Cryptocurrencies and blockchain. Legal context and implications fir financial crime, money laundering and tax evasion*, European Parliament, Directorate - General for Internal Policies, Policy Department for Economic, Scientific and Quality of Life Policies, PE 619.024 – July, 2018, Study requested by TAX3 committee.

[11] D.-M. Ilucă, *De la sare la Libra coin: scurt istoric al formelor monetare și aspectul lor juridic,* în Analele Științifice ale Universității „Alexandru Ioan Cuza” din Iași, Tomul LXV/Supliment, Științe Juridice, 2019, p. 225.

[12] Publicat în Official Journal of the European Union, L 156 din 19.06.2018.

[13] Publicată în M. Of. nr. 291 din 30 martie 2018.

aprobarea unor măsuri fiscal – bugetare[14], prin care se definesc veniturile impozabile ce provin din alte surse şi declararea, stabilirea şi plata impozitului pentru acestea: *„17. La articolul I, după punctul 16 se introduc şase noi puncte, punctele 16^1 – 16^6, cu următorul cuprins: „16^1. La articolul 114 alineatul (2), după litera (l) se introduce o nouă literă, litera m), cu următorul cuprins: «m) venituri din transferul de monedă virtual.»” (...) 16^5. La articolul 116 alineatul (2), după litera b) se introduce o nouă literă, litera c), cu următorul cuprins: «câştigului din transferul de monedă virtuală în cazul veniturilor prevăzute la art. 114 alin. (2) lit. m), determinat ca diferenţă pozitivă între preţul de vânzare şi preţul de achiziţie, inclusiv costurile directe aferente tranzacţiei. Câştigul sub nivelul a 200 lei/tranzacţie nu se impozitează cu condiţia ca totalul câştigurilor într-un an fiscal să nu depăşească nivelul de 600 lei.»”.*

Ulterior, în anul 2020, ţinând cont de continua dezvoltare a criptomonedelor, de posibilitatea acestora de putea fi utilizate în mod abuziv în săvârşirea de infracţiuni, precum spălarea banilor, finanţarea terorismului, şi România nu dispune de o legislaţie specifică care să reglementeze moneda virtuală, spre deosebire de majoritatea statelor membre ale Uniunii Europene care dispun, a fost adoptată *Ordonanţa de Urgenţă a Guvernului nr. 111 din 2020*[15] privind modificarea şi completarea *Legii 129 din 2019* pentru prevenirea şi combaterea spălării banilor şi finanţării terorismului[16], precum şi (...), conform căreia, se introduc două noi litere astfel: *„Articolul I pct. 11 La articolul 2, după litera t) se introduc două noi litere, literele t^1) şi t^2), cu următorul cuprins: t^1)monede virtuale 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 şi nu deţine statutul legal de monedă sau de bani, dar este acceptată de către persoane fizice sau juridice ca mijloc de schimb şi poate fi transferată, stocată şi tranzacţionată electronic; t^2) furnizor de portofel digital înseamnă o entitate care oferă servicii de păstrare în siguranţă a unor chei criptografice private în numele clienţilor săi, pentru deţinerea, stocarea şi transferul de monedă virtuală;”.*

4. Aspecte de drept penal special

În contextul apariţiei fenomenului de globalizare, al schimburilor din ce în ce mai accentuate de ordin economic, al concurenţei în maximizarea câştigurilor, asistăm în mod evident şi la o creştere a criminalităţii, a celei transfrontaliere organizate, în mod particular.

Dezvoltarea internetului nu are efecte asupra societăţii doar din perspectivă pozitivă, ci şi din perspectivă negativă, respectiv şi asupra mediului infracţional, infractorii fiind la curent cu noutăţile tehnologice, cunoscând cele mai avansate instrumente digitale. Astfel, internetul a devenit un mediu favorabil datorită faptului că oferă multe avantaje şi oportunităţi acestora (*s.n.,* infractorilor), şi,

[14] Publicată în M. Of. nr. 44 din 17 ianuarie 2019.

[15] Publicată în M. Of. nr. 620 din 15 iulie 2020.

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

totodată, prezintă şi vulnerabilităţi pe care le descoperă. Acest fapt se datorează şi unei serii de caracteristici de care beneficiază, şi anume[17]: *a) Scara* – comunicarea este mult mai eficientă, timpul şi costurile fiind mult reduse comparativ cu mediul off-line, infracţiunile săvârşindu-se la un nivel global; *b) Accesibilitatea* – evoluţia tehnologică a determinat trecerea de la dispozitive de mari dimensiuni, care erau utilizate doar de anumite categorii de persoane şi instituţii, poate chiar doar cei care aveau o calificare, la unele care sunt disponibile pentru oricine (în acest caz, facem distincţie doar între infractori şi victime) şi pentru orice (informare, socializare, divertisment, sarcini de muncă, etc.); *c) Anonimitatea* – infractorii au posibilitatea de a utiliza internetul, implicit aplicaţiile oferite sub o identitate falsă, pentru unele nefiind necesară o verificare prealabilă a identităţii (de exemplu, deschiderea unui cont de e-mail). Totodată, sunt folosite instrumente de criptare sau de îndepărtare a istoricului electronic; *d) Portabilitatea şi transferabilitatea* – datele pot fi stocate pe dispozitive de mici dimensiuni şi cu o capacitate mare de stocare, fără a fi diminuate sau alterate, cu costuri reduse, uşor transmisibile către mulţi destinatari; *e) Acoperirea globală* - existenţa multiplelor legături teritoriale, respectiv activitatea infractorului se poate desfăşura pe teritoriul unui singur stat, iar acţiunile să aibă ca ţintă victime de pe teritoriul mai multor state; *f) Lipsa eficienţei anumitor organe sau autorităţi de punere în aplicare a legii* – caracteristicile anterior enunţate ridică dificultăţi în sarcina organelor de a descoperi şi pedepsi faptele din cauza legislaţiilor diferite ale statelor aplicabile competenţelor şi atribuţiilor, procedurilor de investigare, termenelor, dar şi a obligaţiei de respectare a vieţii private a persoanelor.

În privinţa temei abordate, a criptomonedelor, modalităţile de săvârşire a faptelor penale sunt multiple, de la utilizarea de către organizaţiile de crimă organizată sau reţele teroriste până la acţiuni care au drept consecinţă creşterea instabilităţii pe pieţele financiare, precum încurajarea speculaţiilor şi a instrumentelor financiare.

”Datorită” faptului că sunt instrumente de natură descentralizată – nu este nevoie de un terţ pentru autorizarea tranzacţiilor, oferă un nivel ridicat de confidenţialitate, nu e nevoie de un cont bancar şi de legitimare cu un act de identitate, criptomonedele oferă un grad mare de atracţie organizaţiilor criminale pentru a le utiliza în activităţile lor ilicite, precum spălare de bani, finanţare terorism. Totodată, sunt folosite şi site-urile de schimb de criptomonede, infracţiunile devenind mai complexe şi mai dificil de descoperit şi pedepsit.[18]

Rolul criptomonedelor în cadrul activităţilor infracţionale este în creştere, atât datorită utilizării lor pentru facilitarea multiplelor aspecte ale criminalităţii informatice, ci şi datorită adoptării lor pe scară mai largă ca mijloc de plată. Prin urmare, utilizatorii cinstiţi de criptomonede şi exchange-urile devin ţinta atacurilor

[17] A.C. Moise, E. Stancu, *Criminalistica: elemente de tehnică și de tactică a investigării penale,* ed. a III-a, rev. și ad., Editura Universul Juridic, București, 2020, pp. 185 – 186.

[18] M. Constantinescu, *Criptomonedele. Aspecte tehnologice, economice și implicații asupra securității naționale,* Editura Pro Universitaria, București, 2020, p. 237

care erau până acum orientate doar spre utilizatorii instrumentelor financiare tradiţionale.

Utilizarea criptomonedelor de către grupările de crimă organizată generează întrebarea dacă şi în ce măsură acestea pot fi utilizate şi de către organizaţiile teroriste. Până în prezent, nu au fost cazuri cunoscute de utilizare în scară importantă a criptomonedelor pentru finanţarea terorismului, dar asta nu înseamnă că lucrurile vor rămâne la fel şi în viitor.

Cerinţele de finanţare a terorismului variază în funcţie de organizaţie. În general, acestea constă în finanţarea unor operaţiuni specifice şi/sau acoperirea costurilor mai largi necesare pentru menţinerea viabilităţii organizaţiei teroriste şi promovarea ideologiei şi a obiectivelor acesteia.

În acest sens, un prim exemplu era Silk Road[19], printre cele mai mari pieţe negre online. Silk Road (Drumul Mătăsii) era cunoscută drept o reţea comercială care leagă Orientul, începând din China, cu Occidentul, nume ce provine de la comerţul intens cu mătase, dar şi alte bunuri, în perioada secolul al II-a î. Hr. până în secolul al XVIII-lea d. Hr.. De asemenea, a avut un rol deosebit în dezvoltarea civilizaţiilor, prin schimburile de religii, filosofii, ştiinţe şi tehnologii, cum ar fi, de exemplu, hârtia sau praful de puşcă. A avut, din păcate, şi un rol negativ, cel de răspândire a diferitelor boli, mai ales a ciumei.

În vremurile actuale, Silk Road era una dintre cele mai cunoscute platforme de vânzare a produselor ilegale, fiind prima piaţă modernă de tip darknet, care a luat naştere din „nevoia" traficanţilor de droguri de a lua legătura cu persoanele interesate de a cumpăra droguri, în condiţii stricte de confidenţialitate, chiar anonimitate. Aceasta era cunoscută în special pentru activităţi precum spălare de bani şi trafic de droguri cu ajutorul tranzacţionării Bitcoin. Site-ul era accesibil numai prin reţeaua cunoscută sub numele de *Tor*, preferată de infractori pentru anonimizarea datelor şi activităţilor utilizatorilor. Astfel, datele utilizatorilor erau ascunse faţă de cei care doreau să supravegheze tranzacţiile.

Pe această piaţă s-au tranzacţionat, în tot timpul existenţei ei – în jur de 30 de luni, anii 2011 – 2013 -, aproximativ 9.9 milioane în bitcoin, echivalentul a 214 milioane de dolari la acea vreme.

Platforma a fost destructurată de agenţii FBI, infiltraţi ca investigatori sub acoperire, în colaborare cu cei ai DEA, IRS şi agenţi vamali, în anul 2013, în urma căruia s-au confiscat 144.000 monede bitcoin (echivalentul a 34 de milioane de dolari la acea vreme).

Un alt exemplu, mai recent, este cazul AlphaBay[20], care, după destructurarea Silk Road din 2013, a devenit cea mai mare piaţă criminală online. Aceasta a fost închisă în anul 2017, de către autorităţile din Statele Unite ale Americii, în urma unei operaţiuni internaţionale. Criptomonedele au avut un rol esenţial înainte de

[19] [Online] la https://www.fbi.gov/contact-us/field-offices/newyork/news/press-releases/ross-ulbricht-the-creator-and-owner-of-the-silk-road-website-found-guilty-in-manhattan-federal-court-on-all-counts , accesat la 31.05.2021.

[20] [Online] la https://www.fbi.gov/news/stories/alphabay-takedown , accesat la 31.05.2021.

închiderea pieţei. Astfel, pe parcursul a doi ani, pe AlphaBay s-au efectuat vânzări de droguri, arme de foc, instrumente de piratare, substanţe chimice toxice, iar banii, aproximativ 1 miliard de dolari, au fost schimbaţi în criptomonede, în acest mod pierzându-se urma lor[21].

O alt mod de spălare a banilor este prin intermediul brokerilor „over the counter" (OTC) terţi. Cu ajutorul lor, infractorii convertesc criptomonedele achiziţionate în numerar întrucât acest sistem le permite să evite tranzacţionarea printre-un schimb reglementat. Situaţia este cu atât mai favorabilă infractorilor deoarece aceşti brokeri deţin afaceri legitime şi, totodată, sunt specializaţi în domeniu, oferind servicii de spălare a banilor.

Printre altele, criptomonedele sunt utilizate şi în activităţile de criminalitate cibernetică în privinţa căreia au un rol esenţial pentru a fi iniţiate, executate şi plata activităţilor.

O primă activitate din această sferă este *activitatea de ransomware*[22] (atacuri care urmăresc obţinerea unei răscumpărări din partea victimei), deoarece aceasta a cunoscut o răspândire importantă în ultima vreme, devenind un fel de „marcă" a atacatorilor cibernetici. Anul 2019 a fost un an prolific pentru acest tip de activităţi, conform unui raport fiind anul cu cele mai costisitoare atacuri de ransomware din SUA, depăşind 75 de miliarde de dolari. Tendinţa crescătoare a activităţii de ransomware nu este preconizată să încetinească în viitor, mai ales dacă ne uităm la perioada anterioară. Astfel, numai în primele 9 luni ale anului 2016, rata atacurilor de răscumpărare asupra firmelor a crescut de la un atac odată la două minute la un atac odată la 40 de secunde, apărând astfel 62 de variante noi de malware.

Criptomonedele reprezintă o variantă eficientă din punctul de vedere al infractorilor, care cer răscumpărarea într-o monedă virtuală datorită faptului că acestea sunt mai greu de urmărit decât bancnotele sau transferurile bancare. Spre exemplu, criptomonedele pot fi utilizate ca monedă de plată a răscumpărătorilor în urma atacurilor de spear phising, malware sau SIM swapping. Atacul de SIM swapping presupune ca odată ce atacatorul a primit numărul telefonului compromis al victimei, îl va utiliza pentru a reseta parole şi a intra în conturile victimelor, inclusiv în conturile de pe exchange – urile de criptomonede.

Bitcoin este cea mai des utilizată criptomonedă în atacurile de răscumpărare (ransomware). De exemplu, în februarie 2016, un hacker a preluat controlul asupra tuturor sistemelor computerizate ale Centrului Medical de la Hollywood Presbyterian, iar în schimb spitalul a fost nevoit să plătească o răscumpărare în cuantum de 17.000 de dolari pentru a recâştiga controlul.[23]

---

[21] [Online] la https://blogs.imf.org/2018/03/13/addressing-the-dark-side-of-the-crypto-world/?cid=sm-com-FB , accesat la 28.05.2021.

[22] M. Constantinescu, *op. cit.*, pp. 249 – 250.

[23] R. Winton, *Hollywood Hospital Pays $17000 in Bitcoin to Hackers; FBI Investigating*, Los Angeles Times, 2016, [Online] lahttp://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html, accesat la data de 30.05.2021

Atacurile de ransomware sunt atât de strâns legate de criptomonede „datorită" caracterul anonim necesar pentru lansarea de atacuri rapide de succes, oferit relativ uşor de criptomonede, de obicei bitcoin, iar propunerile de a găsi modalităţi pentru a împiedica ireversibilitatea, rapiditatea sau descentralizarea bitcoin au fost respinse, deoarece sunt percepute ca o compromitere a naturii esenţiale a monedelor virtuale.

Cripto – jacking[24] este definit ca fiind deturnarea computerelor minerilor de criptomonede. Fenomenul se referă la orice proces prin care un atacator utilizează puterea de calcul sau lăţimea de bandă a unui echipament hardware pentru a extrage criptomonede fără permisiunea proprietarului acestuia. De cele mai mult ori, aceasta se face printr-un script care rulează pe un website. Prin intermediul browserului vizitatorului, scriptul permite website-ului să utilizeze puterea de calcul a vizitatorului pentru a extrage criptomonede, pe durata cât acesta rămâne pe site. De obicei, aceşti atacatori utilizează puterea de calcul astfel deturnată pentru a extrage Monero, deoarece nu necesită o putere de calcul la fel de mare pentru a fi extras comparativ cu bitcoin.

Premisele pentru efectuarea unui atac de cryptojacking prin intermediul browserului sunt prin urmare următoarele: a) Un utilizator în necunoştinţă de cauză accesează o pagină web compromisă; b) Pagina web respectivă conţine un JavaScript care include codul de cryptojacking; c) Codul de cryptojacking deturnează procesorul calculatorului şi îl utilizează pentru a extrage criptomonede; d) În unele cazuri, JavaScript deschide o fereastră minimizată, ascunsă, în fereastra browserului. Când utilizatorul părăseşte site-ul, extragerea ilicită de criptomonede continuă; e) Extragerea se încheie în momentul în care tab-ul site-ului compromis se închide.

În afară de cryptojacking, se mai utilizează şi atacuri de cryptomining prin malware clasice, în care malware–ul infectează calculatorul prin modalităţile uzuale cu scopul de a utiliza calculatorul infectat pentru extragerea de criptomonede. Impactul acestui tip de activităţi este mai uşor de detectat dar nu mai puţin nociv. Astfel, conform raportului McAffee[25] din 2018 s-a constatat o creştere a malware utilizate pentru extragerea de cripromonede cu 629% faţă de anul anterior.

Fraudele sunt o categorie de infracţiuni în care criptomonedele pot reprezenta un mijloc sau obiectul lor, precum[26]: a) Infracţiuni financiare: tranzacţiile instantanee ale criptomonedelor, portabilitatea şi acoperirea internaţională înseamnă că pot fi folosite ca instrumente pentru promovarea evaziunii fiscale, spălării banilor şi mitei; b) Ofertă iniţială de monede înşelătorie: prima ofertă a unei anumite criptomonede de vânzare, numită Ofertă iniţială de monede sau ICO, poate fi un mijloc de a profita de cei nepăsători. Multe ICO-uri sunt fabricate complet, cu

[24] M. Constantinescu, *op. cit.,* pp. 250 – 252.

[25] Companie globală de naționalitate americană în domeniul software-ului de securitate.

[26] [Online] la https://constantinecannon.com/practice/whistleblower/ whistleblower-types/financial-investment-fraud/cryptocurrency-fraud/, accesat la 28.05.2021.

biografii false ale membrilor echipei inexistente şi cărţi tehnice copiate din alte criptomonede legitime; c) Scheme de pompare şi descărcare: moneda virtuală poate oferi o nouă variantă a schemei clasice de pompare şi descărcare, în care proprietarii de acţiuni încearcă să crească preţul înainte de a-şi vinde deţinerile la un vârf artificial. În lumea criptografică, acest lucru este obişnuit în stadiul ICO, sau chiar dincolo, ori de câte ori reclamaţiile false pot susţine cererea şi permit iniţiatorilor sau deţinătorilor dominanţi ai criptomonedei să câştige profituri enorme false; d) Manipularea pieţei: fraudatorii pot încerca să manipuleze pieţele în care sunt tranzacţionate criptomonede sau produse derivate conexe. Manipularea necorespunzătoare a pieţei poate include spoofing, front-running, churning şi alte scheme; e) Scheme Ponzi: investiţiile criptografice pot fi folosite şi ca vehicul pentru o schemă tradiţională Ponzi , în care sunt necesari noi adoptatori pentru a oferi profituri artificiale primilor adoptatori. Investiţiile presupuse pe pieţele emergente de criptare pot servi şi ca obiectiv presupus pentru schemele Ponzi. Având în vedere că cripto-ul este pe larg înţeles, poate fi acoperirea perfectă pentru o schemă falsă; f) Furt tradiţional: criptomonedele oferă, de asemenea, infractorilor noi oportunităţi de furt. Ei pot pirata portofelele criptografice ale investitorilor şi le pot fura moneda; pot configura portofele false pentru a-şi împărţi omologii; şi pot stabili schimburi de criptografie false pentru a fura banii clienţilor.

5. Investigarea infracţiunilor

Aşa cum am precizat şi în prima parte referitor la caracterele criptomonedelor, cele de a fi descentralizate, conferă anonimitate aparţinătorului, confidenţialitate, libertate, accesibilitate, astfel ajungând şi la imprevizibilitate, în privinţa investigării infracţiunilor săvârşite cu acestea, organele de cercetare întâmpină dificultăţi în activitatea lor.

Activitatea de investigare a infracţiunilor trebuie să lămurească următoarele probleme:

1. Activitatea ilicită săvârşită de natură să producă statului un prejudiciu cu caracter patrimonial.

2. Identificarea făptuitorilor şi stabilirea contribuţiei fiecăruia la săvârşirea faptelor.

3. Stabilirea existenţei şi întinderii prejudiciului.

4. Existenţa concursului de infracţiuni.

5. Depistarea cauzelor, a condiţiilor şi împrejurărilor care au favorizat săvârşirea activităţii ilicite şi stabilirea măsurilor de prevenţie.

Principalele metode de cercetare utilizate în descoperirea acestui tip de infracţiuni sunt: a) Obţinerea datelor privind tranzacţiile financiare ale unei persoane din care reies identitatea conturilor, tranzacţiile efectuate, rulajele din conturi, declaraţii privind sursa fondurilor, adresele IP de unde au fost efectuate tranzacţiile, raportările privind tranzacţiile suspecte, metodele sau instrumentele de plată utilizate; b) Obţinerea datelor privind situaţia financiară a persoanelor suspecte; c) Conservarea datelor informatice; d) Percheziţia; e) Ridicarea de obiecte şi înscrisuri; f) Comisii rogatorii şi delegări, atât la nivel naţional, cât şi

internaţional, în baza protocoalelor de cooperare judiciară – EUROJUST, EUROPOL, INTERPOL, EUROFISC. [27]

Specific acestei categorii de infracţiuni pentru descoperirea lor sunt probele digitale, informaţii ce sunt stocate, prelucrate sau transmise cu ajutorul unui sistem informatic, cu valoare probantă atât pentru organele de urmărire penală, cât şi instanţele judecătoreşti. Ce este posibil, însă esenţial să găsească investigatorii pe sistemele informatice sunt următoarele tipuri de fişiere: a) fişiere create de utilizator: agende, fişiere audio-video, fişiere de bază de date, fişiere text, fişiere e-mail, fişiere imagine; b) fişiere protejate de utilizator: fişiere criptate, fişiere comprimate, fişiere protejate prin parolă, fişiere ascunse prin metoda stenografiei, fişiere ascunse; c) fişiere create de computer: cookies, fişiere back-up, fişiere log, fişiere swap, fişiere de configurare, fişiere history, fişiere temporare, fişiere de sistem, fişiere ascunse; d) alte zone în care se găsesc fişiere: spaţiu inactiv, spaţiu nealocat, partiţii ascunse, spaţiul liber, zone rezervate.[28]

La nivel internaţional, cel puţin în sistemul de drept anglo-saxon sau common law, specifice Marii Britanii şi Statelor Unite ale Americii, sunt utilizate aplicaţii sau platforme create cu scopul de a descoperi infracţiunile unde predomină anonimitatea şi confidenţialitatea, precum:

O primă metodă este *dezanonimizarea*, denumită şi re-identificare, este o tehnică ce se utilizează în exploatarea datelor care încearcă să re-identifice informaţiile criptate sau ascunse. Ca mod de realizare, dezanonimizarea constă în efectuarea de operaţiuni de încrucişare a datelor anonimizate cu alte date, care sunt disponibile, pentru identificarea persoanelor, grupurilor sau tranzacţiilor. În această procedură, se folosesc şi aplicaţii, precum CipherTrace Crypto, ce facilitează realizarea rapidă a unei investigaţii, permiţând aflarea identităţii şi a adreselor legate de tranzacţiile cu criptomonede.

Autopsy[29] este o platformă digitală de criminalistică folosită pentru investigaţiile cazurilor ce au implicat folosirea computerului, cu module ce oferă: analiza cronologiei, filtrarea fişierelor, marcându-le pe cele rele şi ignorându-le pe cele bune, căutarea de cuvinte cheie, indexate, extragerea istoricului, a cookie-urilor şi a marcajelor, recuperarea fişierelor şterse din spaţiul liber, extragerea formatului imaginilor şi clipurilor video.

Disk imaging – procesul de realizarea a unei arhive, a unui duplicat sau a unei copii de rezervă a întregului conţinut de pe hard-ul unui terminal (calculator, laptop). În cadrul analizei duplicatului (niciodată originalul), se vor putea identifica atât datele existente pe acesta, cât şi cele care au fost şterse.

---

[27] C. Bogdan, E. Hoch, *Ghid pentru combaterea spălării banilor destinat judecătorilor și procurorilor*, Consiliul Superior al Magistraturii, București, 2015, [Online] la http://inm-lex.ro/fisiere/d_1443/Ghid%20combatere%20spalare%20bani_judecatori%20si%20procurori.pdf , accesat la 31.05.2021, p. 62.

[28] A. C. Moise, E. Stancu, *op. cit.,* pp. 186 – 190.

[29] [Online] la https://www.sleuthkit.org/autopsy/ , accesat la 31.05.2021

6. Concluzii

Criptomonedele, la momentul actual, au doar o mică influenţă în mediul fiscal, fiind foarte puţin reglementate din acest punct de vedere, astfel încât să fie folosite precum banii reali, precum leul, euro sau dolarul. Autorităţile competente încearcă pas cu pas să reglementeze şi să se adapteze la noile tendinţe în această materie.

Christine Lagarde, directorul general al Fondului Monetar Internaţional, afirma în anul 2018, în legătură cu beneficiile criptomonedelor şi posibilitatea băncilor centrale de a le emite: *„Înainte de a ajunge acolo, totuşi, trebuie să facem un pas în spate şi să înţelegem pericolul care vine alături de promisiuni. Aceste oferte digitale sunt în mod tipic construite într-un mod descentralizat şi nu sunt supervizate de o bancă centrală. Tranzacţiile cu criptomonede sunt anonime, aşa cum sunt tranzacţiile cu numerar, ceea ce ar putea avea ca rezultat un nou vehicul pentru spălarea de bani şi finanţarea terorismului."*[30]

Din păcate însă, cei care doresc să îşi maximizeze profiturile, să deţină putere şi care o pot face doar prin activitatea infracţională, au profitat de apariţia criptomonedelor şi au văzut oportunităţi foarte bune în atingerea scopurilor, săvârşind spălare de bani, finanţarea terorismului, furturi, şantaj ş.a.

Cu toate că există multe provocări legate de aceasta, o soluţie o reprezintă reglementarea tehnologiei blockchain, o platformă care foloseşte registre electronice pentru a permite efectuarea tranzacţiilor cu criptomonede în mod transparent şi în siguranţă. Tehnic vorbind, tehnologia blockchain este un registru în format electronic, cu caracter descentralizat (spre deosebire de bancă, care este unul centralizat) *peer-to-peer*[31] care face transcrieri şi menţine în mod precis evidenţa tranzacţiilor, putând fi modificat doar cu acordul tuturor membrilor din lanţ[32]. Prin această tehnologie, „banii" vor fi urmăriţi mult mai uşor, în acest fel reuşindu-se diminuarea fenomenului infracţional.

Referinţe

Arusoaie A., *Blockchain: tehnologie, criptomonede, aplicaţii,* Universitatea „Alexandru Ioan Cuza" din Iaşi

Bogdan C., E. Hach E., *Ghid pentru combaterea spălării banilor destinat judecătorilor şi procurorilor,* Consiliul Superior al Magistraturii, Bucureşti, 2015

Constantinescu M., *Criptomonedele. Aspecte tehnologice, economice şi implicaţii asupra securităţii naţionale,* Editura ProUniversitaria, Bucureşti, 2020

Danţiş D., *Cryptocurrencies, a new reality for econonomy and security,* Strategies XXI International Scientific Conference, The Complex and Dynamic Nature of the

[30] [Online] la https://blogs.imf.org/2018/03/13/addressing-the-dark-side-of-the-crypto-world/?cid=sm-com-FB – 28.05.2021.

[31] În limbaj informatic, *peer-to-peer înseamnă* conexiunea directă dintre două computere din aceeaşi reţea, capabile să-şi distribuie reciproc informaţii fără să fie necesară existenţa unui al treilea care sa deţină rolul de server

[32] D. Ștețiu, *Ofertele inițiale de monede (ICO) bazate pe tehnologia blockchain*, [Online] la *www.juridice.ro* , accesat la 31.05.2021.

Security Environment, Centre for Defence and Security Strategic Studies/"Carol I" National Defence University, Nov. 27-28, 2018, Bucharest, Romania

Franţ A.E., *Criminalistică. Curs universitar*, Editura Universul Juridic, Bucureşti, 2018

Gust M., *Cryptocurrencies. Technical and functional aspects,* The Journal Contemporary Economy, Vol. 3, Issue 3/2018

Houben R., Snyers A., *Cryptocurrencies and blockchain. Legal context and implications fir financial crime, money laundering and tax evasion",* European Parliament, Directorate - General for Internal Policies, Policy Department for Economic, Scientific and Quality of Life Policies, PE 619.024 – July, 2018, Study requested by TAX3 committee

Ilucă D.-M., *Reglementare bitcoin. Aspecte juridice privind utilizarea de bitcoin.,* Analele Ştiinţifice ale Universităţii „Alexandru Ioan Cuza" din Iaşi, Tomul LXIII, Seria Ştiinţe Juridice, 2017, nr. II

Ilucă D.-M., *De la sare la Libra coin,* Analele Ştiinţifice ale Universităţii „Alexandru Ioan Cuza" din Iaşi, Tomul LXV/Supliment, Ştiinţe Juridice, 2019

Moise A. C., Stancu E., *Criminalistica. Elemente de tehnică şi de tactică a investigării penale,* ed. a III-a, rev. şi ad., Editura Universul Juridic, Bucureşti, 2020

Olănescu A., *Criptomonedele faţă în faţă cu evaziunea fiscală,* prezentare Litigators 2021, Conferinţa Nicolae Volonciu, Probleme dificile de drept penal şi procedură penală (ed. a VI-a), *„Capra cu trei iezi: evaziunea fiscală, corupţia şi fraudarea fondurilor europene"*, 21 aprilie 2021

Şteţiu D, *Ofertele iniţiale de monede (ICO) bazate pe tehnologia blockchain,* www.juridice.ro, 2017