Michaela Jurisová

Virtuálne meny verzus kriminalita

Anotácia: Predkladaná práca sa zameriava na virtuálne meny, pričom predmetom skúmania sú niektoré riziká využívania virtuálnych mien a možnosti odhaľovania a objasňovania trestnej činnosti s nimi spojenej. V teoretickej rovine i aplikačnej praxi je možné sa stretnúť aj s inými synonymickými pomenovaniami virtuálnych mien, napríklad virtuálne peniaze, virtuálne platidlo, kryptomeny. V texte sú vybrané poznatky konkrétnejšie spájané aj s najprepracovanejšou, resp. najpopulárnejšou virtuálnou menou/systémom - bitcoinom. Označenie „virtuálna mena" je v texte príspevku využívané s ohľadom na zaužívanú prax, zároveň však rešpektujúc fakt, že Európska centrálna banka[1] z právneho hľadiska nepovažuje kryptomeny ani za menu ani za peniaze, a tiež ani za „úplné/plné formy peňazí" (z angl. „full forms of money"), ako môžu byť definované v ekonomickej literatúre. Kryptomeny je možné nepochybne označiť za fenomén posledných rokov (najmä vo svete financií). Virtuálne platidlá zažívajú obrovskú expanziu, sú v hľadáčiku množstva ľudí aj inštitúcií. Sú spájané s pozitívami aj negatívami. S kryptomenami (resp. s bitcoinom) je spájané obrovské množstvo prívlastkov, napríklad, že sú decentralizované, nie sú kryté (napríklad zlatom), vyznačujú sa vysokou mierou (pseudo)anonymity, celkové množstvo (bitcoinov) v obehu je fixne limitované, využívajú peer-to-peer /P2P/ komunikáciu, minimálne transakčné náklady, časová nenáročnosť transakcií, absencia právneho rámca (na národnej, európskej aj medzinárodnej úrovni), a tiež sú využívané aj na rôzne kriminálne účely (ako legalizácia príjmov z trestnej činnosti, daňové úniky, obchodovanie s ľuďmi, financovanie terorizmu). Snahou autorky je čitateľovi priblížiť predmet skúmania predovšetkým z pohľadu kriminológie, aj keď na predmetnú tému je možné nazerať multidisciplinárne. V texte je pozornosť venovaná napríklad terminológii, právnemu poňatiu, prepojeniu kryptomien a kriminality, rizikám využívania virtuálnych mien, či naznačeniu modusu operandi. Teoretické poznatky sú doplnené o reálne prípady z aplikačnej praxe (v podobe kazuistík). Spomenuté sú tiež možné poškodené objekty (obete). Z metodologického hľadiska boli využité teoretické vedecké metódy, predovšetkým analýza a syntéza faktov z odborných dokumentov a materiálov, prognostická metóda a z empirických metód rozhovor (interview) s odborníkmi na predmetnú problematiku, služobne zaradenými v rámci odboru počítačovej kriminality úradu kriminálnej polície Prezídia Policajného zboru.[2]

Kľúčové slová: virtuálna mena, kryptomena, Bitcoin, kriminalita, Slovenská republika, legislatívny rámec, oprávnené inštitúcie.

Úvod

Digitalizácia a virtuálny svet sa stali súčasťou života každého človeka. Všetci dnes viac či menej, chcene alebo nechcene, žijeme vo virtuálnom svete, sme jeho súčasťou. Postupne sa vnárame do kybernetického priestoru a tento svet sa prenáša do všetkých foriem reálneho života. Tak ako si na sociálnych sieťach vytvárame virtuálnu osobnosť, vytvorili sme si postupne v rámci obchodnej komunikácie aj virtuálne meny. Pričom tendencie k vytvoreniu digitálnych peňazí existovali už od začiatku rozširovania internetu.

Podobne ako sa v bežnom živote vyskytujú finančné trestné činy, aj vo virtuálnom svete si nachádzajú svoje miesto. Dochádza napríklad ku škodám na osobnej identite a majetku, či vytvára sa priestor na obchod so zakázaným tovarom a službami.[3] Výskumnou otázkou je, do akej miery sú virtuálne meny ako objekt predmetného skúmania zneužívané v podmienkach Slovenskej republiky. Okrem rešerše odbornej literatúry, autorka odpovede hľadala v rámci interview s odborníkmi z OPK ÚKP P PZ.

Smernica Európskeho parlamentu a Rady (EÚ) 2018/843 z 30. mája 2018, ktorou sa mení smernica (EÚ) 2015/849 o predchádzaní využívaniu finančného systému na účely prania špinavých peňazí alebo financovania terorizmu a smernice 2009/138/ES a 2013/36/EÚ (ďalej

[1] Bližšie pozri: Ecb.europa.eu. Dostupné online na: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf> [cit. 2020-07-14].
[2] Pozn. autorky: ďalej v texte aj „OPK ÚKP P PZ".
[3] Alternatívne bankové platformy, 2015, s. 6.

aj „Smernica“) predstavuje nepochybne dôležitý právny dokument. Okrajovo pojednáva aj o nástrahách virtuálnych mien[4].

Zároveň je na mieste upriamiť pozornosť na správu Európskej komisie (Správa EK Európskemu parlamentu o hodnotení rizík spojených s praním špinavých peňazí a financovaním terorizmu, Brusel, 26. 6. 2017), v ktorej bolo identifikovaných štyridsať produktov alebo služieb predstavujúcich najvyššiu zraniteľnosť.[5] Pričom najväčšie riziká prinášajú: používanie hotovosti, virtuálnych mien, crowdfundingu, financovanie neziskových organizácií alebo poskytovanie neformálnych služieb prevodu peňazí, akým je napríklad systém hawala.[6]

Vybrané vlastnosti kryptomien umožňujú ich zneužitie na trestné účely, súvisiace napríklad, s už vyššie spomenutými, ale aj s financovaním terorizmu či s praním špinavých peňazí. Teda je evidentné ich využívanie na nelegálne účely. S kryptomenami je spojených ale aj množstvo pozitív. Uvedené prepojenie virtuálnych platidiel a kriminality napĺňa účel tohto príspevku. Cieľom je snaha rozšírenia poznatkov čitateľov o možných nástrahách/rizikách kryptomien.

Virtuálne meny sú novým fenoménom, kde dochádza k neustálym inováciám. Pričom obsiahnutie niečoho, čo sa mení každý deň, nie je jednoduché.

Technológia fungovania virtuálnych mien je zložitá. Jej samotné objasnenie by niekoľkonásobne presahovalo daný príspevok. Z uvedeného dôvodu, sú „technické náležitosti“ objasnené iba okrajovo a účelne (napríklad výraz „blockchain“[7], „peer-to-peer“, „hash“).

Bitcoin - najpopulárnejšia/najrozpracovanejšia kryptomena

Určite nie jedinou, ale pravdepodobne najpopulárnejšou a laickej i odbornej verejnosti najznámejšou z kryptomien je mena bitcoin.

V novembri 2008 bol publikovaný koncept systému virtuálnej meny bitcoin. Systém bol popísaný v koncepte „Bitcoin: Decentralizovaný elektronický peňažný systém“, či „Elektronický peňažný systém postavený na princípe rovného s rovným“ (z angl. Bitcoin:

---

[4] Európska centrálna banka sa vyhýba použitiu pomenovania „virtuálna mena“ či „kryptomena“ a nahradzuje ho rigidne používaným pojmom „schéma virtuálnej meny“ (z angl. virtual currency scheme), pretože z dôvodu ustálenej ekonomickej terminológie, bitcoin nespĺňa požiadavky na finančné platidlo. Definuje ho ako digitálnu reprezentáciu určitej hodnoty, ktorá môže byť za istých okolností použitá ako alternatíva peňazí. Bližšie pozri: ŠIŠULÁK, S. a L. JAKUBÍK, 2016. *Virtuálne meny v procese legalizácie príjmov z trestnej činnosti*, s. 274.

[5] *Poznámka autorky*: Hodnotenie má štvorstupňovú škálu, počnúc nízkym rizikom, cez mierne riziko, vysoké riziko, až po veľmi významné riziko.

[6] Bližšie pozri: SABAYOVÁ, M. a M. PRESPERÍNOVÁ, 2018. *Vybrané riziká prania špinavých peňazí*, s. 124 a nasl.

[7] Databáza typu *blockchain* je využívaná väčšinou súčasných kryptomien, ale čoraz častejšie si nachádza uplatnenie aj v oblastiach bežného života, ako napríklad vládny sektor, školstvo, hlasovanie, zdravotná starostlivosť, či katastrálny register. Vyplývajúc z uvedeného Š. Zachar zameral pozornosť na otázku: Čo vlastne blockchain znamená, keď takýmto zásadným spôsobom vstupuje do života spoločnosti, organizácií, či ľudí všeobecne? Zároveň tiež približuje 19 oblastí, na ktoré bude mať (má) blockchain veľký vplyv. Nie je prekvapením, že prvou z nich je *oblasť bankovníctva a platieb*. Blockchain je tiež nazývaný technológiou budúcnosti, ktorá by v mnohých oblastiach mohla nahradiť dnešný byrokratický aparát (a to v mnohých oblastiach spoločnosti). Bližšie pozri: ZACHAR, Š., 2018. *Technológia blockchain a jej možné využitie v štátnom a verejnom sektore*, s. 186 a nasl., s. 192.

S uvedenou problematikou ide ruka v ruke neustále sa zväčšujúci kyberpriestor. S čím narastá aj miera zločinov páchaných jeho prostredníctvom alebo priamo v jeho prostredí. Súčasťou kyberpriestoru sú aj služby založené na opisovanej technológii (blockchain), ako napríklad kryptomeny, ktoré môžu byť cieľom páchania trestnej činnosti alebo jej platidlom. Bližšie pozri: ZACHAR, Š., 2019. *Využitie znakov digitálnej stopy pri riešení problematiky blockchain*, s. 196.

A Peer-to-Peer Electronic Cash System) podľa návrhu S. Nakamota (nazývaného aj otec Bitcoinu).[8]

V odbornej literatúre je možné sa stretnúť s niekoľkými jeho charakteristikami. Pre účel daného príspevku je využitá definícia z publikácie Kybernetická kriminalita: „Bitcoin je internetová open-source peňažná mena, ktorou je možné platiť prostredníctvom úplne decentralizovanej P2P siete. Hlavnou unikátnosťou bitcoinu je práve jeho plná decentralizácia, pričom je navrhnutý tak, aby nikto, ani autor alebo iní jednotlivci, skupiny či vlády, nemohol menu akokoľvek ovplyvniť, ničiť, falšovať, zabavovať účty, kontrolovať peňažné toky alebo spôsobovať infláciu. V sieti neexistuje žiaden centrálny bod, ani nikto, kto by mohol o sieti rozhodovať. Bitcoin je deflačná mena. Celkové množstvo peňazí je konečné a vopred známe,[9] a jeho uvoľňovanie do obehu je definované iba matematickými zákonmi. V sieti prebiehajú/prebiehali platby za minimálne (alebo žiadne) poplatky.“[10]

Bitcoin je digitálna P2P[11] mena. Kryptomena. Na rozdiel od súčasných peňazí, ako sú napríklad americké doláre či české koruny, bitcoin nemá žiadnu centrálnu autoritu, ktorá by sa za neho zaručovala alebo mala možnosť „tlačiť“ nové peniaze. Okrem tejto vlastnosti ide ale o peniaze so všetkými štandardnými charakteristikami „dobrých peňazí“. A asi aj omnoho viac.[12]

Zároveň je na mieste podotknúť, že bitcoiny nie sú elektronické peniaze (nemožno ich stotožňovať)[13] – pretože nenapĺňajú definičné znaky elektronických peňazí.

Postupným vývojom je evidovaných aj veľké množstvo iných virtuálnych mien[14], napríklad Litecoin, Ethereum, Ripple, Monero.[15] Počet dostupných kryptomien je obrovský, evidované sú počty druhov v stovkách.

---

[8] ŠIŠULÁK, S. a L. JAKUBÍK, 2016. *Virtuálne meny v procese legalizácie príjmov z trestnej činnosti*, s. 269.

[9] Podľa prehlásenia autora/-ov bude celkom vygenerované konečné množstvo 20 999 999,9769 bitcoinov, pričom sa predpokladá, že tento proces sa skončí okolo roku 2140. Bližšie pozri: SMEJKAL, V., 2015. *Kybernetická kriminalita*, s. 556.
Zároveň je predpokladom, že až 99 % bitcoinov má byť v obehu do roku 2033. Ak pravda prežije všetky turbulencie, nezhody a odchody vývojárov, alebo internetové bubliny a bude mať aj stále nejakú finančnú hodnotu a zachová si dôveru účastníkov „hry“. Tiež sa predpokladá, že hodnota Bitcoinu bude časom narastať. Bližšie pozri: ŠIŠULÁK, S. a L. JAKUBÍK, 2016. *Virtuálne meny v procese legalizácie príjmov z trestnej činnosti,* s. 271, s. 277.

[10] SMEJKAL, V., 2015. *Kybernetická kriminalita*, s. 555 a nasl.

[11] P2P (peer-to-peer) je možné definovať ako zdieľanie dátových súborov medzi konkrétnymi počítačmi v sieti, a to tak, že jeden alebo viacerí dáta poskytujú a jeden alebo viacerí dáta sťahujú. Navzájom sú si počítače rovné, komunikujú na rovnakej úrovni, sieť nie je možné jednoducho vypnúť, lebo naďalej budú existovať ďalší a ďalší poskytovatelia obsahu. Rozhodujúcim faktorom zdieľania je skôr kvalita a rýchlosť pripojenia. Nevýhodou systému je okamžité zdieľanie získaných dát, čím často dochádza k porušovaniu autorských práv. Bližšie pozri: ŠIŠULÁK, S. a L. JAKUBÍK, 2016. *Virtuálne meny v procese legalizácie príjmov z trestnej činnosti*, s. 269 a nasl.

[12] STROUKAL, D. a J. SKALICKÝ, 2018. *Bitcoin a jiné kryptopeníze budoucnosti*, s. 24.

[13] Bližšie pozri: SMEJKAL, V., 2015. *Kybernetická kriminalita*, s. 560.

[14] V odbornej literatúre je možné filtrovať dve kategórie kryptomien, označovaných ako *coin* a *token*. To je jedna z možných foriem rozčlenenia kryptomien, ktorú je možné napriek týmto spektrom uplatniť: *1) coiny* sú kryptomeny s vlastným blokchainom (a sieťou uzlov) a je možné ich ďalej členiť napríklad na bitcoiny, altcoiny, atď.; *2) tokeny* – nemajú vlastný blockchain, ale sú postavené na jednej zo zmienených platforiem (v drvivej väčšine je to Ethereum) a plnia funkciu v rámci decentralizovaných aplikácií. Sú uchovávané v peňaženkách a je možné nimi platiť, čo ale nie je ich hlavným účelom. Token poskytuje prístup k systému, jeho funkciám alebo službám. Umožňuje distribúciu odmien, výhod pre držiteľov tokenu. Základné delenie je na *utility tokeny* a *security tokeny*. Bližšie pozri: KALISKÝ, B., 2018. *Bitcoin a ti druzí*, s. 67.

[15] Nie len bitcoin je spájaný s kriminalitou. Príklad s kryptomenou Monero (XMR): jej prednosťou je anonymita. Podrobnosti každej transakcie vrátane odosielateľa, prijímateľa a objemu sú zaznamenané vo verejnej knihe, ale tak, že sa nedajú odhaliť. Teoreticky neexistuje žiadna možnosť, aby sa niekto iný pripojil medzi odosielateľa a prijímateľa alebo aby videl veľkosť transakcie. Otázkou teda je: Znie to atraktívne pre zločincov? Dôkazom je príklad, kedy hackeri stojaci za globálnym útokom WannaCry, ktorý infikoval 230 000 počítačov so systémom

BTC[16] je trojmiestna skratka jednotky bitcoinovej meny (podobne ako USD pre americký dolár). Keďže konečné množstvo BTC v systéme je približne 21 miliónov a očakáva sa, že hodnota jedného BTC bude príliš vysoká pre bežné platby, existujú odvodené jednotky (bitcoin je deliteľný na osem desatinných miest) – milibitcoin (1 mBTC = 0,001 BTC), mikrobitcoin (1 μBTC = 0,001 mBTC) a satoshi (1 satoshi = 0,01 μBTC = 10^{-8} BTC).[17] Jednosymbolová skratka pre jednotku bitcoinovej meny je dvakrát preškrtnuté písmeno „B“.[18]

Hodnota bitcoinu[19], podobne ako väčšiny ostatných „zákonných“ mien, vychádza z dopytu a ponuky na trhu. Táto kryptomena teda nie je krytá zlatom alebo inými komoditami. Ale je krytá „dôverou“, že s ňou bude možné v budúcnosti zaplatiť rovnako ako dnes.[20]

Postupom času sa zmenilo naozaj veľa. Ale evolučne, nie revolučne, tvrdia autori publikácie Bitcoin a jiné kryptopeníze budoucnosti. Bitcoin sa vyvinul, zlepšil. Niektoré veľké bitky ho stále čakajú, iné už skoro vyhral. Pomaly sa vyjasňujú regulácie, graduje diskusia o tom, ako zvýšiť množstvo transakcií, ktoré je možné v sieti uskutočniť, vznikajú zaujímavejšie alternatívy. Stále viac ľudí bitcoiny prijíma a používa.[21]

Riziká využívania virtuálnych mien

Európsky bankový úrad (z angl. European Banking Authority – „EBA“) vytyčuje množstvo rizík, ktoré sa jednotlivo vyskytujú u rôznych účastníkov na trhu so systémami virtuálnej meny aj v oblastiach súvisiacich s ňou. Napríklad:

- riziká súvisiace s používateľmi virtuálnej meny (kupujúci, predávajúci);
- riziká súvisiace s ďalšími účastníkmi na trhu s virtuálnou menou (platformy zmenární);
- riziká súvisiace s trestnou činnosťou (pranie špinavých peňazí a financovanie terorizmu, finančné a iné zločiny);
- riziká súvisiace s existujúcimi platobnými systémami;
- riziká súvisiace s reguláciou a dohľadom nad trhom s virtuálnou menou.[22]

Používatelia alebo aktéri manipulujúci s virtuálnymi menami sú vystavení viacerým rizikám, napríklad:

- úverové riziko: za každých okolností sa tí, ktorí dávajú pôžičky výmenou za virtuálnu menu, môžu dostať do problémov, keďže nie je isté, či vydavateľ kryptomien dokáže splniť svoje doposiaľ nezaplatené záväzky voči veriteľovi. Zjavným príkladom môže byť bankrot platformy zmenární;
- riziko likvidity: virtuálna mena má mimoriadne nízku likviditu a jej hodnota sa zakladá na ponuke a dopyte, čo znamená vysokú nestálosť hodnoty (volatilitu);[23]
- prevádzkové riziko: je obyčajne spojené so stabilnými a bezpečnými operáciami vydavateľa virtuálnej meny a súvisí s fungovaním samotnej schémy. Hoci mnohé systémy

---

Microsoft Windows, vyžadovali platby v Monero. Bližšie pozri: KORAUŠ, A., P. KELEMEN, S. BACKA, J. POLÁK, 2019. *Alternatívne kybernetické meny v súčasnosti*, s. 61.

[16] Historicky je využívaná aj skratka XBT. Zároveň bitcoin s malým „b“ je označenie/výraz pre samotnú menu a Bitcoin s veľkým „B“ pre celý platobný systém. Bližšie pozri aj: Euroekonom.sk. Dostupné online na: https://www.euroekonom.sk/financie/kryptomeny-a-virtualne-peniaze/bitcoin-btc/ [cit. 2020-06-26].

[17] Alebo bližšie pozri: CoinExplorer.sk. Dostupné online na: <https://coinexplorer.sk/co-je-bitcoin/> : *1 BTC = 1000 mBTC = 1 000 000 bits (uBTC) = 1 000 000 000 satoshi* [cit. 2020-06-26].

[18] STROUKAL, D. a J. SKALICKÝ, 2018. *Bitcoin a jiné kryptopeníze budoucnosti*, s. 32.

[19] *Poznámka autorky*: V čase spracovania príspevku (k 3. 7. 2020) – 1 bitcoin = 8 100,62 €.

[20] SMEJKAL, V., 2015. *Kybernetická kriminalita*, s. 557.

[21] STROUKAL, D. a J. SKALICKÝ, 2018. *Bitcoin a jiné kryptopeníze budoucnosti*, s. 14.

[22] Alternatívne bankové platformy, 2015, s. 39.

[23] Nie je nezvyčajné, aby cena kryptomien narástla alebo sa znížila aj o desať a viac percent v priebehu jedného dňa. Bližšie k výhodám a nevýhodám virtuálnych mien pozri aj: KORAUŠ, A., P. KELEMEN, S. BACKA, J. POLÁK, 2019. *Alternatívne kybernetické meny v súčasnosti. Aktuálne výzvy kybernetickej bezpečnosti v podmienkach bezpečnostných zložiek*, s. 56.

kryptomien vrátane transakcií, zámeny a obchodníkov na *darknete* sú anonymné a dobre chránené, existuje tiež pravdepodobnosť, že akákoľvek šikovná a sofistikovaná osoba z IT prostredia dokáže nájsť v tomto systéme medzeru a následne vniknúť do platformy zmenární;
- právne riziká: vo všeobecnosti existuje právna neistota vo fungovaní mechanizmu platforiem kryptomien.[24]

Vyplývajúc z vyššie uvedeného, je na mieste upriamiť pozornosť na fakt, že objektom nečestného konania podvodníkov môže byť ktokoľvek. Obzvlášť vo virtuálnom prostredí. O konkrétnom prípade sme diskutovali s odborníkmi zaradenými v rámci odboru počítačovej kriminality úradu kriminálnej polície Prezídia Policajného zboru.

Objektom konania podvodníkov sa v analyzovanom prípade stal aj známy politický predstaviteľ. Webový portál Živé.sk o tom čitateľov informuje v príspevku s názvom „Falošný Matovič hovorí, ako zbohatnúť. V napodobenine Nového Času.“[25]

V uvedenom prípade sa stal objektom on-line podvodu aktuálny premiér Slovenskej republiky Igor Matovič. Podľa podvodného článku sa mal premiér objaviť v relácii („Neskoro večer“) známeho slovenského moderátora Petra Marcina. Nešlo však iba o tento jeden prípad, ale o sériu prakticky totožných fiktívnych článkov lákajúcich na investovanie cez internet. Podvodníci v článkoch zneužili aj mená iných známych tvárí. Napríklad meno úspešného slovenského športovca Petra Sagana, rappera Rytmusa či podnikateľa Jaroslava Haščáka, prostredníctvom ktorých takúto možnosť rýchleho zárobku „vychvaľovali“.

V predmetnom článku mal premiér „vychvaľovať“ investovanie do kryptomien. A aby toho nebolo málo, išlo o sporadickejší prípad o niečo sofistikovanejšieho podvodu. Zatiaľ čo drvivá väčšina takýchto falošných článkov využíva vlastný vizuál tváriaci sa ako spravodajský web, tento konkrétny článok verne skopíroval vzhľad webstránky bulvárneho slovenského denníka Nový Čas.

Povedomý vizuál môže mnohých ľudí presvedčiť, že sa nachádzajú na legitímnom webe. Napriek niektorým nezrovnalostiam v samotnom texte tak môže návštevník vďaka strate ostražitosti fiktívnemu článku uveriť.

Podvodný článok návštevníkov láka na zapojenie sa do platformy Bitcoin Era (u iných verzii článku môže ísť o inak nazvané platformy, napríklad Bitcoin Revolution). Záujemcovia, ktorí sa cez odkazy v článku zaregistrujú, sú kontaktovaní telefonicky osobami, ktoré ich prevedú procesom prvého vkladu. Zväčša v minimálnej hodnote 250 €.

Podľa informácií portálu Živé.sk, v prípade článku s I. Matovičom, nakoniec záujemca skončí na on-line investičnej platforme Askobid.fm. Ide o pochybnú offshore brokerskú stránku, na mnohých weboch označovanú za podvod.

Je na mieste zdôrazniť, že podobným platformám, sľubujúcim rýchly zisk, je dobré sa vyhnúť. Uvedené podčiarkuje, že je možné sa z týchto prípadov poučiť a byť v budúcnosti preventívne ostražitejší.

Virtuálne meny verzus kriminalita

Odborníci často predikujú virtuálnym menám problémy existenčného, finančného, ale aj legislatívneho charakteru. V tejto súvislosti je na mieste si zodpovedať niektoré otázky, a to kto virtuálnu menu emituje, od čoho sa odvíja jej cena, kto ju vôbec uznal a ako sa s ňou nakladá, ako by sa mala používať, ale aj to, ako býva zneužívaná, či aká trestná činnosť s ňou môže súvisieť.

---

[24] Alternatívne bankové platformy, 2015, s. 40 a nasl.

[25] Bližšie pozri: Zive.sk. Dostupné online na: https://zive.aktuality.sk/clanok/146193/falosny-matovic-hovori-ako-zbohatnut-v-napodobenine-noveho-casu/ [cit. 2020-07-22].

S kriminalitou môžu byť spojené takzvané „obidva veľké svety virtuálnych mien“ – virtuálne herné meny, aj virtuálne kryptomeny a z pomedzi nich hlavne bitcoin.[26]

Existencia Bitcoinu dala napríklad možnosť vzniknúť novému druhu malvéru. Škodlivé programy sa nemusia zapodievať iba krádežami dát, ale objavujú sa aj také, ktoré „kradnú výpočtový výkon“ napadnutého počítača tým, že na ňom ťažia kryptomeny. V neposlednom rade nevystopovateľné bitcoiny uľahčujú páchanie takzvanej „klasickej“ kriminality, ako napríklad vydieranie alebo únos.[27]

Pri páchaní trestnej činnosti sa stále častejšie stretávame so sofistikovanejšími spôsobmi realizácie, nevynímajúc prevody finančných prostriedkov – a to prostredníctvom alternatívnych bankových platforiem, ktoré možno chápať ako virtuálne bankové účty, ktoré fungujú mimo regulovaného globálneho finančného sektora. Práve alternatívne bankové platformy sa stávajú prostriedkom na prevody malých alebo aj veľkých objemov peňazí, legalizáciu finančných prostriedkov či anonymný nákup prostriedkov na páchanie trestnej činnosti, softvéru, falošných dokladov, kreditných kariet a i., ktoré sa do veľkej miery používajú na páchanie ďalšej trestnej činnosti (ako napríklad ekonomické a finančné podvody či organizovaná teroristická činnosť). S použitím takto získaných prostriedkov sa dnes u páchateľov stretávame bežne.

Hoci sa zdá, že virtuálne meny sú budúcim trendom platobných systémov, riziko spojené s ich používaním a legalizáciou vo svete obchodu je na mieste sledovať. Kryptomeny dnes poskytujú nový, výkonný nástroj – aj pre zločincov, pomocou ktorého je možný presun a uchovávanie peňazí pochádzajúcich z trestnej činnosti. Okrem toho predstavujú významné prostriedky na financovanie terorizmu mimo dosahu orgánov činných v trestnom konaní (ďalej aj „OČTK“) a ďalších orgánov regulujúcich finančné trhy a bankové systémy.

Na rozdiel od „skutočných peňazí“ (*fiat money*) možno virtuálne meny použiť na rýchle investovanie, nákup a predaj iba „jediným kliknutím“. Hoci sú virtuálne meny lákavým platobným prostriedkom pre akékoľvek investície, platobné produkty a služby využívajúce kryptomeny otvárajú dvere neobmedzeným možnostiam legalizovania príjmov pochádzajúcich z trestnej činnosti a financovania terorizmu. Virtuálne platidlo však nie je jediným prostriedkom, ktorý je využívaný/používaný pri páchaní trestnej činnosti. Páchatelia majú k dispozícii množstvo rôznych aplikácií a nástrojov, prostredníctvom ktorých môžu napríklad zatajiť svoju identitu, transakcie a komunikačné kanály, údaje uložené na pevných diskoch, ako aj kolotoč uskutočňovaných platieb.

Naznačený, relatívne nový, fenomén zločinu si vyžaduje, aby OČTK a súvisiace finančné či bankové inštitúcie a regulačné orgány kráčali o krok vpred alebo aby prinajmenšom udržali krok s inovatívnymi nezákonnými praktikami.[28]

Virtuálna mena nemá status zákonného platidla, čo znamená, že ju nevydáva ani negarantuje žiadna jurisdikcia. Legalizácia statusu platidla je predmetom dohody v komunite používateľov virtuálnej meny.

Pri konvertibilných virtuálnych menách, z nich práve konvertibilita robí nekrytý (*fiat*) cieľ alebo prostriedok na uskutočňovanie nezákonných finančných operácií a pranie špinavých peňazí.

Pre lepšie pochopenie konania páchateľov je na mieste oboznámiť sa s mechanizmami, ktoré im prinášajú väčšie príležitosti, t. j. či sa virtuálne meny riadia centralizovaným systémom alebo nie.

---

[26] ŠIŠULÁK, S. a L. JAKUBÍK, 2016. *Virtuálne meny v procese legalizácie príjmov z trestnej činnosti*, s. 267.; a k virtuálnym herným menám bližšie pozri s. 268.

[27] SMEJKAL, V., 2015. *Kybernetická kriminalita*, s. 562.

[28] Alternatívne bankové platformy, 2015, s. 7 a nasl.

OČTK sa pri hodnotení rizík a vyšetrovaní väčšinou zameriavajú na decentralizované virtuálne meny známe ako kryptomeny, pretože ide o virtuálne meny typu open-source, ktoré sú založené na princípe decentralizovaného elektronického platobného systému.[29]

Pre zvýšenie úspešnosti objasňovania nelegálnej činnosti súvisiacej s kryptomenami je pre OČTK vhodné poznať významných účastníkov procesu realizácie. K účastníkom, ktorých možno do procesu začleniť alebo zneužiť na uľahčenie nezákonných činností patrí napríklad „správca“[30], „používateľ“[31] či „poskytovateľ peňaženiek“.[3233]

Anonymita platieb je lákavou prednosťou, ktorá poskytuje priestor pre prevody finančných prostriedkov pochádzajúcich z trestnej činnosti a z nelegálnych činností (pranie špinavých peňazí, teroristické aktivity, daňové úniky a pod.). Aj keď rovnaké možnosti v súčasnosti poskytujú hotovostné platby (*cash*), kryptomenové prenosy navyše prinášajú výhodu v podobe verejnej databázy všetkých platobných transakcií (*blockchain*). Osoby zapísané v tejto databáze sú síce anonymné, no existuje možnosť analytického spracovania údajov na účely získavania informácií o ich totožnosti.[34]

V praktickej rovine je dôležité uvedomiť si fakt (potvrdený aj expertmi z OPK ÚKP P PZ), že odhaľovanie trestných činov, pri ktorých sú virtuálne meny zneužívané na páchanie trestnej činnosti (napr. financovanie terorizmu) alebo sú zneužívané na zakrytie pôvodu/výnosu z trestnej činnosti (t. j. legalizácia príjmov z trestnej činnosti) prebieha na základe toho, ako sa o danej skutočnosti (ilegálnej aktivite) dozvedia OČTK. Existuje množstvo spôsobov, na základe ktorých môžu OČTK začať odhaľovanie trestnej činnosti spojenej so zneužívaním kryptomien. Napríklad vlastná „operatívno-pátracia činnosť“ policajných útvarov; oznámenie o podozrivej finančnej transakcii konkrétnou finančnou inštitúciou; preverovanie informácií, na ktoré poukázali investigatívni novinári v médiách; podanie trestného oznámenia o tom, že došlo k spáchaniu trestného činu konkrétnou osobou; výmena informácií od medzinárodných partnerov či vyšetrovanie predikatívnych trestných činov.[35]

---

[29] Alternatívne bankové platformy, 2015, s. 8 a nasl.

[30] „Správca“ dáva do obehu centralizovanú menu a obyčajne ide o fyzickú alebo právnickú osobu, ktorú možno v reálnom svete sledovať ako zaregistrovaný právny subjekt. Správca tiež hrá dôležitú úlohu v prípadoch skupovania virtuálnej meny alebo jej sťahovania z trhu. Fyzické alebo právnické osoby, samozrejme, vymieňajú skutočné peniaze za virtuálnu menu a fungujú ako zmenárne. Bližšie pozri: Alternatívne bankové platformy, 2015, s. 10 a nasl.

[31] „Používateľ“ je klient, ktorý môže byť naozaj zapojený do akýchkoľvek nezákonných činností, keďže ide o skutočnú osobu alebo právny subjekt predstavujúci iného skrytého činiteľa. Používateľ nadobúda virtuálne peniaze na účely nákupu skutočných alebo virtuálnych tovarov a služieb, pričom prenosy uskutočňuje vo vlastnej kompetencii alebo v mene inej osoby či subjektu. Používateľ tiež môže použiť virtuálne meny na akékoľvek investičné účely. Bližšie pozri: Alternatívne bankové platformy, 2015, s. 11.

[32] „Poskytovatelia peňaženiek“, t. j. subjekty poskytujúce virtuálne peňaženky, konkrétne softvérové aplikácie alebo ďalšie mechanizmy na držanie, ukladanie a prenos virtuálnej meny, dopĺňajú skupinu účastníkov v transakciách zahŕňajúcich virtuálne meny. Poskytovateľ peňaženky dokáže na zamaskovanie transakcií a majiteľov peňaženiek ponúknuť rôzne nástroje, ako napríklad šifrovanie, viacnásobný kľúč, ochranu podpisu, zálohovanie „studených úložísk“ a „zmiešavače“. Bližšie pozri: Alternatívne bankové platformy, 2015, s. 11.

[33] Systém virtuálnej meny je tiež spojený s nezávislými zmenárnikmi, správcami, poskytovateľmi služieb webovej správy, odosielateľmi platieb tretej strany, vývojármi softvéru a poskytovateľmi aplikácií, ktorí ponúkajú aplikácie a softvér na legitímne, ale aj nezákonné účely. Dobré je tiež vedieť, že tzv. „zmiešavači“, vývojári alebo operátori môžu osloviť čiernych používateľov prostredníctvom produktov navrhnutých s cieľom vyhnúť sa dohľadu regulačných orgánov aj OČTK. Bližšie pozri: Alternatívne bankové platformy, 2015, s. 10 a nasl.

[34] Alternatívne bankové platformy, 2015, s. 14 a nasl.

[35] Rozhovor realizovaný s odborníkmi na predmetnú problematiku zaradenými v rámci OPK ÚKP P PZ.

Využitie nástroja Chainanalysis

Spoločnosť Chainanalysis sa pred niekoľkými rokmi rozhodla vybudovať nástroj, ktorý by bol schopný sledovať bitcoinové operácie a bol by nápomocný OČTK.

Je potrebné nezabúdať na fakt, že bitcoiny nie sú úplne anonymné, ale pseudoanonymné. To znamená, že bitcoinová adresa je taký druh informácie, ktorý môže preukázať ďalšie vykonané transakcie. Na základe toho je možné vytvoriť určitú schému a následne identifikovať subjekty, ktoré za transakciami stoja.

Na rozdiel od bežných analytických produktov BTC, ktoré získavajú údaje z IP adries, analytický nástroj Chainanalysis dokáže takto zoskupovať viaceré bitcoinové adresy z jednotlivých transakcií a priradiť ich k jednotlivým kryptoburzám.[36]

Pre vyšetrovanie trestnej činnosti spojenej s kryptomenami je podstatné, že stlačením tlačidla Send (Odoslať) sa transakcia okamžite zobrazí na internete. Tri adresy na každú jednu transakciu sa zobrazia v bitcoinovej peňaženke a tie isté informácie sa zobrazia aj na internete. Pomocou databázy blockchain[37] dokážeme identifikovať IP adresu odosielateľa aj prijímateľa, sumu a čas uskutočnenia transakcie. Nedokážeme však určiť totožnosť osôb, ktoré sú majiteľmi adries.

Cez blockchain možno bitcoin sledovať. Entity uložené v tejto databáze sú síce anonymné, no existuje možnosť analytického spracovania údajov na účely získavania informácií, napríklad pomocou IP adries, ktoré možno takto sledovať. Monitoring síce vyzerá ľahko, no trvá nejaký čas. V zásade však ide o riešenie, ako bitcoiny sledovať.

V prostredí internetu existujú aj voľne prístupné stránky, v rámci ktorých sú dohľadateľné informácie o bitcoinových adresách. V optimálnom prípade dostatočných informácií, je eventuálne zistiteľné prostredníctvom ktorej stránky a adresy je peňaženka spravovaná. Môže napríklad ísť o nelegálny trh či zmenáreň. Brožúra (Alternatívne bankové platformy) tiež uvádza, že niekoľko pokusov a kontrol na internete môže vyšetrovateľovi pomôcť identifikovať správcu daných adries/transakcií.

Zmenárne sú kľúčovým partnerom OČTK pri zbere digitálnych dôkazov súvisiacich s platbami realizovanými prostredníctvom kryptomien. Zo strany zmenární by mali byť monitorované a hlásené podozrivé aktivity kompetentným dozorným orgánom.

V prípade zaznamenania adresy v zmenárni, môžu OČTK získať priamy prístup k zaznamenaným údajom a overiť ich. Za optimálnych podmienok by zmenárne mohli OČTK poskytnúť maximálnu súčinnosť aj prostredníctvom právnej pomoci. Vyplývajúc z množstva poskytnutých údajov môžu OČTK eventuálne bližšie identifikovať majiteľa peňaženky.

Za optimálnych podmienok je tu stále možnosť, že majiteľ bitcoinovej peňaženky udelí OČTK prístupové práva (v podobe digitálneho kľúča), za pomoci ktorého budú zobrazené všetky transakcie.[38]

---

[36] Alternatívne bankové platformy, 2015, s. 30 a nasl.

[37] Blockchain – akási „účtovná kniha“, ktorá je verejná a zdieľaná všetkými užívateľmi Bitcoinu. Tí potvrdzujú transakcie rovnako ako je to pri centrálnej autorite, avšak v prípade Bitcoinu decentralizovane. Všetci užívatelia môžu vidieť záznamy o všetkých transakciách v celej histórii. Bližšie pozri: STROUKAL, D. a J. SKALICKÝ, 2018. *Bitcoin a jiné kryptopeníze budoucnosti*, s. 27.
Blockchain možno definovať aj ako povedzme zreťazenie do bloku, teda previazanie transakcií z jedného času navzájom a vznik akéhosi jednoznačného časového sledu o tom, ktoré transakcie sa už realizovali a z toho dôvodu nemôžu byť zopakované – bitcoiny nemôžu byť vďaka tomu dvakrát použité alebo predané. Bližšie pozri: ŠIŠULÁK, S. a L. JAKUBÍK, 2016. *Virtuálne meny v procese legalizácie príjmov z trestnej činnosti*, s. 270.

[38] Alternatívne bankové platformy, 2015, s. 19 a nasl.; UJVÁRY, K. a J. KUCHTOVÁ, 2019. *Špecifiká objasňovania finančných transakcií v súvislosti s bitcoinom*, s. 186.

Keď sa uskutočňuje transakcia určitej sumy v bitcoinoch, eventuálny výdavok musí byť zaslaný na bitcoin adresu, keďže na rozdiel od platieb v klasických štátmi riadených (*fiat*) peniazoch, neexistuje okrem prevodu iný spôsob na rozdelenie bitcoinu. Z toho vyplýva, že každý prevod časti bitcoinu predpokladá existenciu adresy odosielateľa, adresy prijímateľa a adresy, na ktorú bude zaslaný výdavok pre odosielateľa. Používateľ zašle dohodnutú sumu príjemcovi a tiež adresu pre zaslanie výdavku. Adresa výdavku na strane odosielateľa je jedným z najdôležitejších zdrojov informácií pre OČTK. Často je prvým krokom pri výkone vyšetrovacích úkonov na blockchaine.

Z uvedeného vyplýva, že výhodou blockchainu je aj jeho odolnosť voči zmene údajov v ňom. Keďže ide o otvorenú technológiu, ktorá dokáže efektívne a overiteľným a trvalým spôsobom zaznamenávať transakcie medzi dvoma stranami. Pre úspešné sledovanie platieb políciou je nevyhnutné disponovať aspoň základnými kryptografickými znalosťami (porozumenie reťazeniu binárnych hashov).[39] Bez týchto znalostí je aj napriek možnosti použitia sofistikovaných analytických nástrojov pravdepodobnosť identifikácie platby a prepojenia medzi bitcoin adresami ako aj ich majiteľmi minimálna.[40]

Zachar zároveň dodáva, že pokiaľ teda predpokladáme, že skúmaný blockchain obsahuje potenciálne digitálne stopy, no nemáme mechanizmy na jeho dešifrovanie, nemá pre nás žiadnu informačnú hodnotu.[41]

Naznačené úvahy nemusia byť generálne uplatňovanými. Objasňovanie prípadov môže byť individuálne a odvíjajúce sa od heterogénnych podmienok (geografických, personálnych, časových a pod.).

Virtuálne meny a „darknet“

Darknet prešiel veľkým vývojom. Pred niekoľkými rokmi sa v rámci skrytých trhov predávali najmä kradnuté kreditné karty a transakcie sa odohrávali osobne. Dnes darknet funguje ako pohodlný tajný nákupný portál, na ktorom si do košíka môžete vložiť zbrane, drogy či falošné doklady. Rozšíreným obchodom na darknete je napríklad aj predaj odcudzených osobných údajov alebo falošných bankoviek (ktoré sa predávajú rovno s radami ako ich zaviesť do obehu). V zásade sa dá povedať, že nákupný košík napokon jednoducho vyprázdnite tak, že uhradíte platbu bitcoinovými jednotkami. Tento relatívne nenáročný model má na darknete za následok postupný mnohonásobný nárast obchodov ponúkajúcich „nezákonné dary“. Ceny tovarov sú uvádzané v bitcoinoch, pričom pre lepšiu orientáciu zákazníka môžu byť zobrazované aj v amerických dolároch.[42]

Pojem *darknet* môže znieť tajuplne. Obvykle je opisovaný ako - špecifické skryté siete, ktoré sú dostupné len prostredníctvom špeciálne navrhnutého softvéru, pričom existujú mimo bežných komunikačných protokolov a internetových aplikácií a služieb. Darknet je teda súhrnné označenie, podobne ako internet, pričom v rámci neho existujú jednotlivé prvky a služby tak, ako v rámci bežného internetu existujú sociálne siete, diskusné fóra, e-maily či e-shopy. Pričom tieto regulárne služby môžu a obvykle aj majú svoje *darknetové ekvivalenty*.

---

[39] *Hash algoritmus* je vlastne jednosmerná (jednocestná) funkcia, ktorá za presne definovaných podmienok vytvorí zo zdrojových dát ľubovoľnej veľkosti jedinečný reťazec (nazývaný aj odtlačok, fingerprint, miniatúra), ktorý je závislý na všetkých bitoch zdrojového reťazca. Hash funkcie v blockchaine nám teda umožňujú efektívnym spôsobom overovať, či sa niekto pokúšal manipulovať s dátami alebo nie. Bližšie pozri: ZACHAR, Š., 2018. *Technológia blockchain a jej možné využitie v štátnom a verejnom sektore*, s. 188 a nasl.

[40] UJVÁRY, K. a J. KUCHTOVÁ, 2019. *Špecifiká objasňovania finančných transakcií v súvislosti s bitcoinom*, s. 190 a nasl.

[41] Bližšie pozri: ZACHAR, Š., 2019. *Využitie znakov digitálnej stopy pri riešení problematiky blockchain*, s. 198.

[42] Alternatívne bankové platformy, 2015, s. 21 a nasl.

Aj keď sa o darknete zvyčajne hovorí ako o samostatnej entite, v skutočnosti je to logická alebo v trochu násilnom preklade „prekryvná“ sieť (z angl. overlay network), fungujúca v rámci internetovej infraštruktúry. Obvykle pritom využíva princípy P2P.

Dominantným prvkom darknetu je šifrovanie a anonymita. Ochrániť identitu účastníka je v zásade hlavným cieľom akýchkoľvek internetových sietí tohto typu. Vzhľadom na tieto princípy nie je prekvapujúce, že ich využívajú ľudia, ktorí svoju činnosť chcú skryť, a to najmä z dôvodu, že je nelegálna. Ide napríklad o predaj narkotík, falošných dokladov, zbraní, aj o obchod s ľuďmi či ľudskými orgánmi. Môže predstavovať útočisko i pre distribútorov detskej pornografie, členov nenávistných skupín, ktoré zastávajú idey rasizmu či neonacizmu. V neposlednom rade môže slúži ako komunikačný nástroj teroristických skupín či náboženských extrémistov. V zásade, podobne ako darknet je možné vnímať aj kryptomeny, ktorých princíp a výhody nevyhnutne prilákajú aj „horšie živly“.[43]

Právna úprava, formálny rámec a vybrané činnosti kompetentných orgánov

Smernica Európskeho parlamentu a Rady (EÚ) 2015/849 z 20. mája 2015 o predchádzaní využívaniu finančného systému na účely prania špinavých peňazí alebo financovania terorizmu, problematiku virtuálnych mien neopomína.

V zmysle čl. 4 smernice, predchádzanie praniu špinavých peňazí a financovaniu terorizmu môže byť účinné len v prostredí, ktoré nevyhovuje páchateľom hľadajúcim úkryt pre svoje financie za pomoci netransparentných štruktúr. Cieľom smernice je nielen odhaľovať a vyšetrovať pranie špinavých peňazí, ale aj brániť jeho vzniku. Zvyšovanie transparentnosti by mohlo byť silným odstrašujúcim prostriedkom.[44]

Stieranka a kol. vo všeobecnosti legalizáciu príjmov z trestnej činnosti (resp. pranie špinavých peňazí) definujú ako proces premeny príjmov získaných trestnou činnosťou na legálne majetkové hodnoty prostredníctvom využitia legálneho finančného systému. Legislatívne poňatie problematiky je obsiahnuté v medzinárodných aj slovenských právnych dokumentoch.[45]

V podmienkach Slovenskej republiky je to predovšetkým Zákon č. 297/2008 Z. z. o ochrane pred legalizáciou príjmov z trestnej činnosti a o ochrane pred financovaním terorizmu a o zmene a doplnení niektorých zákonov (ďalej aj „AML“[46] zákon). V zmysle trestno-právnej úpravy je legalizácia príjmov z trestnej činnosti vymedzená v § 233 zákona č. 300/2005 Z. z. Trestný zákon.

Jeden zo zahraničných príkladov snahy o reguláciu bitcoinov pochádza z Nemecka. Nemecko neuznalo bitcoiny ako menu, označilo ich len za „súkromné peniaze“ („*privates Geld*“) a vytvorilo predpoklad na ich ďalšiu reguláciu. Hlavným motívom bolo zabránenie daňovým únikom, keďže obchod s bitcoinmi v tejto krajine sa značne rozrastá, a z dôvodu značného posilnenia jeho kurzu (v čase uverejnenia tejto informácie) oproti doláru bolo možné získať jeho predajom pomerne veľký príjem, ktorý nebol zdaňovaný.[47]

Aby bolo možné čeliť hrozbám (napríklad v súvislosti s voľným pohybom zločincov, teroristov, príjmami z trestnej činnosti a finančnými zdrojmi pre terorizmus) aj na európskej úrovni, finančné spravodajské jednotky Francúzska, Talianska, Luxemburgu a Spojeného

[43] Touchit.sk. Dostupné online na: https://touchit.sk/darknet-a-deepweb-temne-zakutia-siete-o-ktorych-sa-nehovori/37785 [cit. 2020-07-14].
[44] Smernica európskeho parlamentu a rady (EÚ) 2018/843 z 30. mája 2018.
[45] STIERANKA, J. a kol., 2018. *Legalizácia príjmov z trestnej činnosti a financovanie terorizmu*, s. 14 a nasl.
[46] *Poznámka autorky*: Z angl. *Anti-money laundering*; a zároveň využívané skratky *ML – money loundering* – pranie špinavých peňazí a *FT – financing of terrorism* – financovanie terorizmu.
[47] NBS.sk. Dostupné online na: https://www.nbs.sk/_img/Documents/_PUBLIK_NBS_FSR/Biatec/Rok2013/08-2013/06_biatec13-8_nadasky.pdf [cit. 2020-07-03].

kráľovstva sa v roku 2002 pripojili k vízii holandskej finančnej spravodajskej jednotky vytvoriť Informačnú sieť finančných spravodajských jednotiek. Vytvorením väčšej synergie medzi finančnou a kriminálnou spravodajskou službou (FIU.net) sa v konečnom dôsledku zvyšuje úsilie v boji s najzávažnejšou kriminalitou.

Nezastupiteľné miesto pri koordinácii opatrení na boj proti legalizácii a financovaniu terorizmu má aj organizácia Financial Action Task Force (FATF). Bola založená s cieľom stanoviť normy a podporiť účinné vykonávanie regulačných a právnych opatrení zameraných na boj proti legalizácii príjmov z trestnej činnosti a financovaniu terorizmu a ďalším ohrozeniam integrity medzinárodného finančného systému.

Z iniciatívy skupiny Egmont[48], Interpolu, Europolu sa organizujú stretnutia pracovnej skupiny kryptomien, kde si zástupcovia finančných spravodajských jednotiek, OČTK a súkromného sektora vymieňajú technické zručnosti a skúsenosti v spojitosti s kryptomenami. Sú pripravované návrhy regulácie[49] digitálnych zmenární a poskytovateľov digitálnych peňaženiek, ako aj definície konceptov kryptomien, zmenární kryptomien a i., za účelom zahrnutia do právneho rámca európskej legislatívy.

Pozornosť tejto téme je venovaná aj v USA. Príkladom je Sieť na vyšetrovanie finančnej kriminality (z angl. Financial Crimes Enforcement Network FinCEN, Dept. of Treasury), ktorá je kompetentným orgánom pre zločiny spojené s kryptomenami v USA.[50]

Ak chceme úspešne bojovať a efektívne zabezpečiť elimináciu legalizácie príjmov z trestnej činnosti a financovania terorizmu, je potrebné vytvoriť ucelený kompaktný systém inštitúcií na rôznych vertikálnych úrovniach, ktoré budú môcť využívať rôzne nástroje, prostriedky a postupy. Ide o tieto roviny: povinné osoby (prvá vertikálna rovina), finančná spravodajská jednotka (druhá vertikálna rovina), OČTK (tretia vertikálna rovina).[51]

V podmienkach Slovenskej republiky, ohľadom predmetnej problematiky v systéme inštitúcií, zohráva dôležitú úlohu Finančná spravodajská jednotka (ďalej aj „FSJ“). Najpodstatnejšia časť činnosti FSJ je zameraná na prijímanie, analyzovanie, vyhodnocovanie a spracovanie hlásení o neobvyklých obchodných operáciách (ďalej aj „NOO“) – na základe zákonom stanovenej ohlasovacej povinnosti vyplývajúcej z AML zákona, a to od povinných osôb, definovaných v tomto zákone (najmä bánk, ostatných finančných inštitúcií či nefinančných inštitúcií).

FSJ vo svojej výročnej správe uvádza prognózu legalizácie príjmov z trestnej činnosti a financovania terorizmu. Pričom na základe analýzy získaných informácií a aktuálnych udalostí v Slovenskej republike, možno predpokladať nasledovné aktivity a vývoj trendov v ML/FT, ktoré by mali generovať príjem, napríklad (okrem iných) aj zo zneužívania nákupu kryptomeny, elektronických peňaženiek a elektronických platobných brán.[52]

FSJ v roku 2019 pripravila návrh novely AML zákona, ktorého hlavným cieľom bola transpozícia smernice Európskeho parlamentu a Rady EÚ 2018/843 a akceptácia odporúčaní

---

[48] Egmont Group: Organizácia združujúca 159 finančných spravodajských jednotiek na celom svete. Poskytuje platformu na zabezpečenú výmenu znalostí a spravodajských informácií v boji proti legalizácii príjmu z trestnej činnosti a financovaniu terorizmu. Bližšie pozri: Minv.sk. Dostupné online na: https://www.minv.sk/?Egmont_Group-1 [cit. 2020-06-30].

[49] K potrebe a podpore regulácie sa prikláňajú mnohí autori venujúci pozornosť predmetnej problematike. Bližšie pozri napr. aj DAUDRIKH, Y., 2018. *Kryptomena ako novodobý právny inštitút*, s. 107 a nasl.

[50] UJVÁRY, K. a J. KUCHTOVÁ, 2019. *Špecifiká objasňovania finančných transakcií v súvislosti s bitcoinom*, s. 186 a nasl.

[51] STIERANKA, J. a kol., 2018. *Legalizácia príjmov z trestnej činnosti a financovanie terorizmu*, s. 118 a nasl.

[52] *Poznámka autorky*: Od 1. augusta 2019 je FSJ v priamej podriadenosti prezidenta Policajného zboru, bez zmien v jej vnútornej štruktúre. Bližšie pozri: Výročná správa, 2019, Finančná spravodajská jednotka, s. 4 a s. 15.

výboru Moneyval a FATF, v snahe účinne reagovať na neustály vývoj v oblasti boja proti ML/FT. Cieľom predloženého návrhu bolo vo všeobecnosti zlepšiť prístup k registru konečných užívateľov výhod, posilniť a harmonizovať pravidlá zvýšenej starostlivosti vo vzťahu ku klientovi, prijať prísnejšie opatrenia na zníženie rizík ML/FT spojených s anonymnými predplatenými nástrojmi, aj monitorovať NOO vykonávané prostredníctvom virtuálnej kryptomeny, rozšíriť okruh politicky exponovaných osôb a sprecizovať postup FSJ pri výmene informácií s príslušnými orgánmi členských štátov potrebných pri predchádzaní a odhaľovaní ML/FT.[53]

Nemenej dôležitou inštitúciou súvisiacou, s touto problematikou, je odbor počítačovej kriminality úradu kriminálnej polície Prezídia Policajného zboru. Bez ohľadu na vývoj situácie súvisiacej s právnym stavom a povahou kryptomien či ochranou ich vlastníctva, už teraz je nevyhnutné pre OČTK vedieť reagovať na túto problematiku. Tak v súvislosti s vnútroštátnym trestným konaním (v ktorom je potrebné zabezpečiť zodpovedajúcu reakciu a v prípade potreby zaistiť kryptomeny, t. j. zrušiť možnosť dispozície vlastníka, resp. držiteľa s touto kryptomenou), ako aj v kontexte medzinárodnej justičnej spolupráce.

Bitcoin je potrebné vnímať ako počítačový údaj (vec), ktorý je nositeľom majetkovej hodnoty, vždy z hľadiska kvantitatívneho, v reálnom čase. Posúdenie Bitcoinu/kryptomeny ako počítačového údaja, ktorý je nositeľom majetkovej hodnoty v reálnom čase, je nevyhnutné z dôvodu zabezpečenia ochrany práv a záujmov fyzických, právnických osôb a štátu prostriedkami práva, ako aj pre efektívnu medzinárodnú spoluprácu v trestných veciach a plnenie medzinárodných záväzkov vyplývajúcich pre Slovenskú republiku v tejto oblasti. Uvedené vyplýva zo slovenskej policajnej praxe.

V zmysle interných právnych aktov (z roku 2019) OPK ÚKP P PZ vykonáva odhaľovanie a dokumentovanie prípadov na úseku počítačovej kriminality, ak si to vyžaduje povaha veci vzhľadom na spôsob páchania trestného činu, procesné strany alebo iný dôležitý záujem, zabezpečuje prevádzkovanie elektronických peňaženiek pre účel zaisťovania digitálnych kryptomien. OPK ÚKP P PZ tiež riadi činnosť zaisťovania kryptomien a organizuje špecializované vzdelávanie v tejto oblasti.

Analýza a pochopenie pravidiel fungovania digitálnych trhov a predovšetkým virtuálnych mien je predpokladom účinného uplatňovania kontroly kriminality tak v podobe prevencie, ako aj represie.

Príklady z praxe

„Podvodná stránka zneužíva Aktuality.sk, Slovenskú sporiteľňu a meno známeho podnikateľa“ (február 2020, SR)

Podvodná stránka sa navonok tvári, že ide o spravodajský portál Aktuality.sk, spomína Slovenskú sporiteľňu a do popredia dáva logá ďalších známych slovenských médií, len aby pritiahla pozornosť ľudí na svoj podvodný biznis. Podvodná stránka láka potenciálne obete cez sponzorované odkazy na facebooku. Ak naň návštevník klikne, ocitne sa na falošnej stránke pripomínajúcej web Aktuality.sk. Prekliky z týchto stránok následne smerujú k projektu Bitcoin Era, kde ľudí nabádajú založiť si účet. Existuje v slovenskom aj anglickom jazyku. Platforma Bitcoin Era nepravdivo informovala, že s ňou Slovenská sporiteľňa spustila spoluprácu. Slovenská sporiteľňa sa od aktivít dištancovala a klientov upozornila, aby boli obozretní a nenechali sa oklamať.[54]

[53] Výročná správa, 2019, Finančná spravodajská jednotka, s. 22.

[54] O mediach.com. Dostupné online na: https://www.omediach.com/hoaxy/17210-podvodna-stranka-zneuziva-aktuality-sk-slovensku-sporitelnu-a-meno-znameho-podnikatela [cit. 2020-07-02].

„Ťažba kryptomeny“(august 2018, SR - Obvodné oddelenie Humenné)

V auguste 2018 neznámy páchateľ na sociálnej sieti vylákal pod zámienkou predaja hardvéru na ťažbu kryptomien od 34-ročného Jána sumu 2 300 €. Ján po vzájomnej dohode uhradil túto sumu prostredníctvom internetbankingu zo svojho bankového účtu na účet „predajcu,“. Dohoda znela, že predajca po prijatí finančných prostriedkov zašle predmetný hardvér. Uvedené nebolo zrealizované.[55]

„Slovák vydieral holandskú spoločnosť“ (február 2018, SR – okres Dolný Kubín/Holandsko)

Slovenská polícia spolupracovala s holandskou, aby tak spoločne našli Slováka, ktorý údajne vydieral zahraničnú spoločnosť. Od Holanďanov požadoval, aby mu poslali bitcoiny. V opačnom prípade plánoval vo vydieraní pokračovať. Za úspešnou akciou stoja policajti zo Žiliny, pričom tá prebehla na území okresu Dolný Kubín.

Takú príležitosť tak skoro mať nebude. Tridsaťdva ročný muž skončil v rukách zákona. V Holandsku pokračuje vyšetrovanie vydierania. Stratégia Oravčana spočívala v tom, že ak mu dotknutá holandská spoločnosť neposkytne to, čo od nej chce, tak zverejní citlivé údaje, ktoré mal mať k dispozícii.[56]

Poznatky nadobudnuté z interview

Príslušníci zaradení v rámci OPK ÚKP P PZ sa doposiaľ stretli iba s takou trestnou činnosťou, pri ktorej došlo k zneužitiu prípadne odcudzeniu kryptomeny bitcoin (BTC) a ripple (XRP).

Vo všeobecnej rovine (bez poukázania na konkrétny prípad) ide napríklad o takýto modus operandi:

- vydieranie (páchateľ kontaktuje vybranú obeť prostredníctvom sociálnej siete, vytvára si ľúbostný vzťah s obeťou a neskôr požiada obeť o financie v kryptomene bitcoin na základe rôznych emocionálnych príbehov – tzv. „romance scam“);
- podvod - kúpa tovaru za kryptomenu bitcoin (väčšinou mobilný telefón prostredníctvom internetového inzertného portálu/e-shopu – podvod – tovar nedodaný);
- ransomvér (páchateľ infikuje počítač obete škodlivým softvérom a zašifruje dátové súbory nachádzajúce sa na pamäťovom zariadení, následne žiada výkupné vo forme kryptomeny bitcoin za dešifrovanie súborov);
- platby za falošné pôžičky (platba poplatku za poskytnutie pôžičky formou bežného peňažného vkladu na účet bieleho koňa a následne majiteľ účtu (biely kôň) peniaze vybral a vložil na bitcoinovú adresu prostredníctvom bitcoinového automatu);
- nákup a predaj ilegálneho tovaru prostredníctvom darknetových trhov (zbrane, drogy, detská pornografia, falošné doklady, falošné bankovky, ...).[57]

Záver

V určitých oblastiach zločinu dochádza k zmenám veľmi rýchlo (nevynímajúc protiprávnu činnosť spojenú s kryptomenami) a kompetentné orgány niekedy ešte stále reagujú na tieto nelegálne činnosti s oneskorením.

Do veľkej miery aj globalizácia internetu mala za následok vznik novej „cezhraničnej“ povahy digitálneho zločinu, ako napríklad podvody súvisiace s elektronickým obchodom (online prevádzky, či platby), virtuálne meny používané ako finančné vyrovnanie v rámci

[55] Minv.sk. Dostupné online na: http://www.minv.sk/?aktuality-presov&sprava=tazba-kryptomeny [cit. 2020-07-02].
[56] Techbyte.sk. Dostupné online na: https://www.techbyte.sk/2018/02/slovak-kryptomeny-kryptomena-bitcoin-vydieranie-holandsko/ [cit. 2020-07-02].
[57] Rozhovor realizovaný s odborníkmi na predmetnú problematiku zaradenými v rámci OPK ÚKP P PZ.

trestných činností (nelegálne obchodovanie s drogami, zbraňami, ukradnutým tovarom, ľuďmi, ukradnutými a falošnými dokumentmi, detská pornografia) a pranie peňazí.

Existujú určité výhody virtuálnych mien (napríklad rýchlejšie a lacnejšie transakcie, ako aj finančná inklúzia), ale riziká z nich vyplývajúce prevažujú nad výhodami. Táto skutočnosť sa však v Európskej únii spomína menej často.

V prípade virtuálnych kryptomien sa stal rýchly a nepozorovateľný presun takýchto prostriedkov kamkoľvek na svete a celková anonymita systému živnou pôdou pre to, aby sa virtuálne meny stali jediným reálnym platidlom na elektronickom čiernom trhu.

Tak ako na jednej strane technológie uľahčujú trestnú činnosť, na strane druhej aj pomáhajú pri jej odhaľovaní. Pokrok v možnostiach analýzy údajov naznačuje, že technologické riešenia hrajú obrovskú úlohu v boji proti tejto kriminalite. Technológie umožňujú OČTK napríklad nastaviť upozornenia, monitorovať podozrivé transakcie a začať hlbšie vyšetrovanie.

Rastúce využívanie nových technológií pri páchaní kriminality predstavuje väčšiu výzvu pre OČTK v členských štátoch Európskej únie. Finančné zločiny sú nadnárodné a zložité a čoraz častejšie sú páchané pomocou nástrojov obchodovania s virtuálnymi kryptomenami na burze.

Na účinný boj proti závažnej a organizovanej trestnej činnosti je potrebné neustále rozširovať vedomosti, informovanosť a spôsobilosť OČTK na účely odhaľovania rozličných finančných zločinov, ale takisto aj ich prepojenosť v rámci globalizovaného finančného prostredia.

Organizovaní páchatelia týchto zločinov budú aj naďalej rozvíjať svoje schopnosti vrátane osvojovania inovatívnych foriem informačných a komunikačných technológií na podporu trestnej činnosti vo finančnej oblasti. Ale vďaka pokročilým formám investigatívnej analýzy môžu OČTK zvýšiť svoju schopnosť identifikovať jednotlivcov a organizácie, a tým posilniť boj proti týmto trestným činom.

Na základe analýzy a štúdia odbornej literatúry je evidentné, že každý štát zatiaľ pristupuje k problematike Bitcoinov inak. Nie je ešte jasné, či sa celosvetovo náhľad na Bitcoin zjednotí, alebo si s právnou úpravou poradí každá krajina po svojom.[58]

Experti z OPK ÚKP P PZ sa prognosticky pozerajú na problematiku virtuálnych mien takto: *„Zaoberať sa témou kryptomien a vyšetrovaním trestnej činnosti spojenej s kryptomenami je v súčasnosti nepochybne nesmierne potrebné, nakoľko sú z viacerých dôvodov čoraz viac zneužívané pri páchaní rôznych druhov trestnej činnosti (ransomvér, financovanie terorizmu, legalizácia príjmov z trestnej činnosti, podvody a pod.). Dôvodom je mnohokrát vyšší pocit anonymity páchateľov, pretože sú presvedčení, že pre políciu je extrémne zložité sledovať tok transakcií (napríklad pri zneužití kryptomeny bitcoin na páchanie trestnej činnosti), a to z dôvodu náročnosti sledovania transakcií v blockchain databáze - bez konkrétneho softvéru vyvinutého na trasovanie bitcoinových transakcií, či z dôvodu využívania služieb ako sú takzvaný mixér, či transformácie kryptomien na online burzách (predaj jednej kryptomeny a nákup inej kryptomeny). Navyše, páchatelia sú čoraz viac zdatnejší v oblasti využívania anonymizačných sietí, anonymizačných služieb VPN, anonymných remailer serverov, kryptomien, čo podstatne sťažuje vyšetrovanie tejto trestnej činnosti.*

V súčasnej praxi možno navyše konštatovať rýchlu adaptáciu páchateľov tejto trestnej činnosti na využívanie úplne anonymných kryptomien, akou je napríklad kryptomena Monero.

[58] Alternatívne bankové platformy, 2015, s. 38, s. 43 a nasl.; SMEJKAL, V., 2015. *Kybernetická kriminalita*, s. 562; ŠIŠULÁK, S. a L. JAKUBÍK, 2016. *Virtuálne meny v procese legalizácie príjmov z trestnej činnosti*, s. 277.

Príkladom môže byť platba za objednaný tovar kryptomenou Monero na darknetových trhoch Empire, Berlusconi, Cryptonia. Ďalej evidujeme veľký nárast podvodných internetových stránok sľubujúcich zbohatnutie na obchodovaní s kryptomenami ako sú Bitcoin Revolution, Bitcoin Era, Bitcoin Bilionare a podobne.“

Výzvy súvisiace s finančným vyšetrovaním, ktoré sa týka kryptomien pomenúvajú experti z mnohých krajín. V podmienkach Slovenskej republiky odborníci z OPK ÚKP P PZ zdôrazňujú najmä tieto:

- problémy spojené so samotným dokazovaním, že kryptomeny predstavujú výnos z trestnej činnosti;
- analýza kryptomenových transakcií je náročná a zároveň musí byť odôvodniteľná, vysvetliteľná a následne uznávaná aj pred súdom;
- otázky spojené s využívaním úplne anonymných druhov kryptomien, akou je napríklad kryptomena Monero;
- problém so zahraničnými kryptoburzami – žiadosti o poskytnutie informácií ako aj príkazu na vydanie a uchovanie počítačových údajov je potrebné adresovať cestou medzinárodnej právnej pomoci;
- fakty spojené s anonymitou v rámci internetu a sveta kryptomien – anonymná registrácia na kryptoburze (napríklad VPN/TOR/falošné doklady), využívanie bitcoinových bankomatov, ktoré sú samy osebe pomerne anonymné, nedostatočná implementácia bezpečnostnej politiky „Know Your Customer“ („KYC“) na online-kryptomenových burzách a celkovo nedostatočná legislatíva v oblasti kryptomien v niektorých štátoch (regulácia podmienok ktoré musia spĺňať spoločnosti ponúkajúce služby v tejto oblasti);
- výzvou do budúcna je aj samotná potreba zvyšovania vzdelanostnej úrovne týkajúcej sa danej problematiky u príslušníkov Policajného zboru, prokurátorov či sudcov.[59]

Literatúra

CoinExplorer.sk. Dostupné online na: https://coinexplorer.sk/co-je-bitcoin/ [cit. 2020-06-26].

DAUDRIKH, Y., 2018. *Kryptomena ako novodobý právny inštitút*. In Právní rozpravy 2018, mezinárodní vědecká konference oblasti práva a právních věd – s podtitulem “nové jevy a právo“, Sborník, Hradec Králové: Magnanimitas, s. 107 – 111. ISBN 978-80-87952-23-8.

Ecb.europa.eu. Dostupné online na: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf> [cit. 2020-07-14].

Euroekonom.sk. Dostupné online na: https://www.euroekonom.sk/financie/kryptomeny-a-virtualne-peniaze/bitcoin-btc/ [cit. 2020-06-26].

KALISKÝ, B., 2018. *Bitcoin a ti druzí. Nepostratelný průvodce světem kryptoměn*. Praha: IFP Publishing, s. r. o., 133 s. ISBN 978-80-87383-71-1.

KOLEKTÍV AUTOROV. 2015. *Alternatívne bankové platformy*. Brožúra. Vydané ako súčasť projektu KNOWLEDGE ENHANCEMENT AND OPERATIONAL CAPACITY PEINFORCEMENT ON MTIC FRAUDS.

KORAUŠ, A., P. KELEMEN, S. BACKA, J. POLÁK, 2019. *Alternatívne kybernetické meny v súčasnosti*, In Aktuálne výzvy kybernetickej bezpečnosti v podmienkach bezpečnostných zložiek, Zborník príspevkov z vedeckej konferencie s medzinárodnou

[59] Rozhovor realizovaný s odborníkmi na predmetnú problematiku zaradenými v rámci OPK ÚKP P PZ.

účasťou konanej dňa 4.6.2019, Bratislava: Akadémia Policajného zboru v Bratislave, s. 54 – 64. ISBN 978-80-8054-820-9.

Minv.sk. Dostupné online na: http://www.minv.sk/?aktuality-presov&sprava=tazba-kryptomeny [cit. 2020-07-02].

Minv.sk. Dostupné online na: https://www.minv.sk/?Egmont_Group-1 [cit. 2020-06-30].

NBS.sk. Dostupné online na: https://www.nbs.sk/_img/Documents/_PUBLIK_NBS_FSR/Biatec/Rok2013/08-2013/06_biatec13-8_nadasky.pdf [cit. 2020-07-03].

O mediach.com. Dostupné online na: https://www.omediach.com/hoaxy/17210-podvodna-stranka-zneuziva-aktuality-sk-slovensku-sporitelnu-a-meno-znameho-podnikatela [cit. 2020-07-02].

Rozhovor (interview) realizovaný s odborníkmi na predmetnú problematiku zaradenými v rámci OPK ÚKP P PZ.

SABAYOVÁ, M. a M. PRESPERÍNOVÁ, 2018. *Vybrané riziká prania špinavých peňazí a financovania terorizmu*, In Policajná teória a prax, roč. XXVI, č. 1. Bratislava: Akadémia Policajného zboru v Bratislave, s. 124 – 132. ISSN 1335-1370.

SMEJKAL, V., 2015. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s. r. o. 636 s. ISBN 978-80-7380-501-2.

Smernica európskeho parlamentu a rady (EÚ) 2018/843 z 30. mája 2018, ktorou sa mení smernica (EÚ) 2015/849 o predchádzaní využívaniu finančného systému na účely prania špinavých peňazí alebo financovania terorizmu a smernice 2009/138/ES a 2013/36/EÚ.

STIERANKA, J. a kol., 2018. *Legalizácia príjmov z trestnej činnosti a financovanie terorizmu, právna a inštitucionálna ochrana v Slovenskej republike*. Bratislava: Wolters Kluwer SR, s. r. o., 193 s. ISBN 978-80-8168-912-3.

STROUKAL, D. a J. SKALICKÝ, 2018. *Bitcoin a jiné kryptopeníze budoucnosti*. 2. rozšírené vyd. Praha: Grada Publishing, a. s., 200 s. ISBN 978-80-271-0742-1.

ŠIŠULÁK, S. a L. JAKUBÍK, 2016. *Virtuálne meny v procese legalizácie príjmov z trestnej činnosti*, In Aktuálne otázky trestného práva v teórii a praxi, 4. ročník interdisciplinárnej celoštátnej vedeckej konferencie s medzinárodnou účasťou (Zborník príspevkov). Bratislava: Akadémia Policajného zboru v Bratislave, s. 267 – 279, ISBN 978-80-8054-682-3.

Techbyte.sk. Dostupné online na: https://www.techbyte.sk/2018/02/slovak-kryptomeny-kryptomena-bitcoin-vydieranie-holandsko/ [cit. 2020-07-02].

Touchit.sk. Dostupné online na: https://touchit.sk/darknet-a-deepweb-temne-zakutia-siete-o-ktorych-sa-nehovori/37785 [cit. 2020-07-14].

UJVÁRY, K. a J. KUCHTOVÁ, 2019. *Špecifiká objasňovania finančných transakcií v súvislosti s bitcoinom*, In Zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou konanej dňa 4. 6. 2019, Bratislava: Akadémia Policajného zboru v Bratislave, s. 185 – 195. ISBN 978-80-8054-820-9.

Výročná správa, 2019, Finančná spravodajská jednotka.

ZACHAR, Š., 2018. *Technológia blockchain a jej možné využitie v štátnom a verejnom sektore*, In Tradície a dynamika vývoja manažmentu a informatiky z pohľadu univerzít s bezpečnostným zameraním, Zborník príspevkov zo 7. virtuálnej konferencie s medzinárodnou účasťou konanej dňa 18. 12. 2017, Bratislava: Akadémia Policajného zboru v Bratislave, s. 186 – 195. ISBN 978-80-8054-768-4.

ZACHAR, Š., 2019. *Využitie znakov digitálnej stopy pri riešení problematiky blockchain*, In Aktuálne výzvy kybernetickej bezpečnosti v podmienkach bezpečnostných zložiek,

Zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou konanej dňa 4.6.2019, Bratislava: Akadémia Policajného zboru v Bratislave, s. 196 – 204. ISBN 978-80-8054-820-9.

Zakony pre ludi.sk. Dostupné online na: https://www.zakonypreludi.sk/zz/2008-297 [cit. 2020-06-28].

Zive.sk. Dostupné online na: https://zive.aktuality.sk/clanok/146193/falosny-matovic-hovori-ako-zbohatnut-v-napodobenine-noveho-casu/ [cit. 2020-07-22].

Key words: virtual currency, cryptocurrency, Bitcoin, crime, The Slovak Republic, legislation, authorized institutions.

Summary

The topic of the article are cryptocurrencies – especially their traps and possibility of police investigation. Many crimes are related to virtual currency, for example money laundering, terrorist financing, human trafficking or tax evasion. Therefore; the article is linked with research: Detection of tax evasion and tax crime, Detecting and proving crimes in the economy (researches were carried out at The Academy of the Police Force in Bratislava). Attention is focused on the most famous virtual currency – bitcoin. Many attributes are relevant to virtual currency, for example: decentralization, (pseudo) anonymity, they are not covered with gold, their quantity is limited (valid for bitcoin), using P2P communication, transactions are time-saving, there is no legal (law) framework (international, european, slovak). Practical examples (from the Slovak republic) are stated in this paper.

mjr. JUDr. Michaela Jurisová, PhD.
Katedra kriminológie
Akadémia Policajného zboru v Bratislave
Tel.: 0961057113
e-mail: michaela.jurisova@minv.sk

Recenzenti: prof. Ing. Jozef Stieranka, PhD., mjr. Ing. Mária Sabayová, PhD.