Marek Matulík

Technologické aspekty zaisťovania virtuálnych mien

Anotácia: Odborný článok sa zaoberá problematikou zaisťovania virtuálnych mien, pričom v rámci tejto multifaktoriálnej činnosti sa v ňom pozornosť primárne zameriava na technologické aspekty danej problematiky. Po stručnom úvode autor predkladá základné informačné penzum technologických informácií, ktorého osvojenie predstavuje nevyhnutný predpoklad pre hlbšie chápanie samotného ekosystému kryptomien. Priestor venuje technológií distribuovaného ledgeru, resp. Blockchainu, ako aj základnej charakteristike inštrumentov asymetrickej kryptografie, ktorú ďalej precizuje a dopĺňa o informácie dotýkajúce sa spôsobov uchovávania súkromného kľúča. Pred formuláciou záveru autor v rámci čiastkovej analýzy poukazuje na neaplikovateľnosť inštitútu zaistenia virtuálnej meny v konkrétnych prípadoch, v ktorých je súkromný kľúč výlučne v dispozícií osoby, ktorá nechce alebo nemôže spolupracovať s orgánmi činnými v trestnom konaní.

Kľúčové slová: virtuálne meny, blockchain, uchovávanie virtuálnych mien, peňaženka virtuálnej meny, zaisťovanie virtuálnych mien

Úvod do problematiky

Právna obec, ako aj spoločnosť a jej jednotlivé sektory dnes stoja pred jednou z najväčších výziev, ktorým doposiaľ čelili. Touto výzvou je hyperglobálny a neprebádaný fenomén s názvom „Web 3.0“ a naň nadväzujúce technológie ako umelá inteligencia, blockchain, vizualizácia a všetky jej prvky rozšírenej alebo virtuálnej reality. Dynamicky sa rozvíjajúci sektor informačných technológií v posledných rokoch priniesol (prináša a bude prinášať) nielen pre spoločnosť, ale aj pre individuálny život jednotlivcov množstvo nových trendov. Jedným z nich sú nepochybne aj kontroverzné virtuálne aktíva, resp. ich subkategória, a to „virtuálne meny“ či častejšie používané synonymum „kryptomeny“[1].

Postupná penetrácia virtuálnych mien medzi početnú heterogénnu skupinu používateľov pritiahla pozornosť regulátorov uvedomujúcich si, že medzi členov tejto skupiny nepochybne patria aj osoby s rôznymi kriminálnymi tendenciami. Tieto osoby promptne implementujú špecifické vlastnosti a potenciál virtuálnych mien do svojich kriminálnych aktivít, čoho odrazom sú aj zistenia americkej blockchainovej dátovej spoločnosti Chainalysis, ktorá odhaduje, že za rok 2022 boli zlegalizované kryptomeny v hodnote takmer 24 miliárd amerických dolárov, čo v porovnaní s rokom 2021 predstavuje nárast až o 68 %.[2]

Tento nemalý obnos nelegálne nadobudnutých finančných prostriedkov možno očami trestného zákona vnímať ako výnos z trestnej činnosti, ktorý ohrozuje a narúša integritu, stabilitu i samotnú povesť finančného sektora.

Vyššie uvedené čísla, ako aj legislatívne aktivity a na ne nadväzujúce rezultáty vo forme smerníc a nariadení európskych autorít naznačujú, že nielen Európska únia, ale aj zvyšok sveta upriamujú svoju pozornosť na jednu z najnebezpečnejších a zároveň, z pohľadu kriminálne závadových osôb, najsľubnejších kombinácií, ktorou je práve legalizácia výnosov (príjmov) z trestnej činnosti v spojení s virtuálnymi menami.

Legalizácia výnosov z trestnej činnosti, resp. používajúc terminológiu uprednostňovanú v rámci Európskej únie „pranie špinavých peňazí“, je v posledných rokoch vysoko aktuálnou témou, pričom už teraz možno konštatovať, že *pro futuro* tomu nebude inak. V tejto súvislosti slovenský zákonodarca nasledoval medzinárodné a európske štandardy, pričom transpozične reagoval na vzniknutú situáciu systematickou legislatívnou činnosťou, ktorá vyústila do rozsiahlej novelizácie trestných kódexov, a to zákonom č.

[1] V súlade s platným pozitívnym právom Slovenskej republiky v ďalšom texte preferujeme pojem „virtuálne meny“.

[2] *Chainalysis: The Crypto Crime Report,* 2023. [online]. [cit. 23. október 2023] Dostupné na internete: https://go.chainalysis.com/2023-crypto-crime-report.html

312/2020 Z. z. o výkone rozhodnutia o zaistení majetku a správe zaisteného majetku a o zmene a doplnení niektorých zákonov.

Predmetný právny akt priniesol viacero zásadných zmien, no pre potreby predkladaného článku vyzdvihneme jednu z tých najmarkantnejších, a to komplexnú a systematickú rekonštrukciu štvrtého dielu štvrtej hlavy všeobecnej časti trestného poriadku (ďalej len „TP“). Úvodné ustanovenie dotknutého dielu legálne definuje vec dôležitú pre trestné konanie, a tým *de facto* zavádza novú diferenciáciu dvoch „zaisťovacích režimov“. V rámci jedného z nich, ktorým je **zaisťovanie nástrojov a výnosov z trestnej činnosti**, katalóg zaisťovacích inštitútov obohatil aj **„inštitút zaistenia virtuálnej meny“**. Dotknutý nástroj orgánom činným v trestnom konaní (ďalej len „OČTK“) ponúka možnosť odňať z dispozície páchateľov nelegálne nadobudnuté virtuálne aktíva.

Uvedený „upgrade“ repertoáru pripraveného na zaistenia virtuálnych mien však od OČTK vyžaduje znalosť aspoň fundamentálneho „balíčka“ vedomostí, ktoré vytvárajú predpoklad pre úspešnú realizáciu zaisťovacieho úkonu. Toto informačné penzum tvoria prevažne technologické aspekty a informácie týkajúce sa principiálneho zabezpečenia virtuálnych mien, nemožno však opomenúť ani dôležité právno-teoretické a aplikačné korelácie.

S poukazom na predmet nášho záujmu nasledujúce riadky venujeme základným technologickým aspektom, ktorých osvojenie si do značnej miery determinuje i samotnú úspešnosť odhaľovania a následného vyšetrovania trestnej činnosti asociovanej s virtuálnymi menami.

Principiálne zabezpečenie virtuálnych mien

Kryptografia ako matematická disciplína zaoberajúca sa šifrovaním a ochranou informácií sa do povedomia širokej verejnosti dostala už v minulosti. Dôvodom bolo aj jej časté pertraktovanie v súvislosti s aplikáciou Threema, ktorú používal mediálne známy a právoplatne odsúdený Marián Kočner. Uvedená aplikácia totiž využíva prvky kryptografie, resp. **šifrovania end-to-end** na účel zabezpečenia vysokej miery anonymity komunikujúcich strán. Kryptografia takisto predstavuje aj „základný stavebný kameň“, na ktorom v roku 2008 neznámy developer (popr. skupina)[3] pod pseudonymom **Satoshi Nakomoto** postavil v tzv. **whitepaper (bielej knihe) „Bitcoin: A Peer-to-Peer Electronic Cash System“ –** fenomén virtuálnych mien.[4]

V rámci legálneho vymedzenia a pojmológie virtuálnych mien možno ešte aj dnes naraziť na názorovú disparitu, a to tak na úrovni európskej legislatívy, ako aj na poli medzinárodnom. Vzhľadom na charakter tohto príspevku však pri legálnom vymedzení pojmu virtuálnych mien len v krátkosti odkážeme na ustanovenie § 131 ods. 7 Trestného zákona,[5] (príp. na smernicu 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, z ktorej zákonodarca vychádzal) pričom našu pozornosť ďalej koncentrujeme na **základné technologické aspekty,** ktoré sú tým pravým dôvodom, pre ktorý pútajú na seba toľko pozornosti.

Pre virtuálne meny je príznačná ich **decentralizácia**, tzn. že na rozdiel od fiat mien, tieto neemituje žiadna centrálna inštitúcia, fyzická osoba či iná autorita, ktorá ani

[3] Či ide o konkrétnu osobu, skupinu osôb alebo určitú formu organizácie doposiaľ nie je známe.

[4] HOSP, J., 2018. *Kryptomeny Bitcoin, Ethereum, Blockchain, ICO and Co. jednoducho a zrozumiteľne*, str. 38

[5] *„Virtuálnou menou sa na účely tohto zákona rozumie digitálny nositeľ hodnoty, ktorý nie je vydaný ani garantovaný centrálnou bankou ani orgánom verejnej moci, nie je nevyhnutne naviazaný na zákonné platidlo a ktorý nemá právny status meny ani peňazí, ale je akceptovaný niektorými osobami ako nástroj výmeny, ktorý možno elektronicky prevádzať, uchovávať alebo s ním elektronicky obchodovať.“*

nespracováva transakcie, ktoré sú s virtuálnymi menami realizované. Transakciu môže uskutočniť jedine **vlastník súkromného kľúča** (pozri nižšie), pričom akonáhle sa zrealizuje určitý počet transakcií, tieto sa vo forme blokov (pri Bitcoine ide o súbor s veľkosťou 1MB) zapíšu do blockchainu. Akonáhle sú raz tieto údaje do blockchainu zapísané (k zápisu dochádza až po určitom procese, ktorý označujeme ako „ťaženie" – pozri nižšie), nie je ich možné zmeniť. Docent Šanta tento prvok označil ako **zásadu nezameniteľnosti**. V tomto kontexte je však nutné dodať, že k týmto vlastnostiam možno takisto priradiť aj ďalšie špecifiká vlastné len určitým druhom virtuálnych mien, napr. menám Bitcoin, Ether, Dogecoin a pod.[6]

V predchádzajúcej stati pracujeme s viacerými pojmami, ktoré sme doposiaľ necharakterizovali. Tie najpodstatnejšie preto v ďalšom texte postupne priblížime. Termín „**coin**" **(digitálna minca)** v slove Bitcoin, či Dogecoin pomenúva aktívum pochádzajúce z natívneho blockchainu (známym príkladom je aj Ethereum – Ether).[7]

Blockchain možno hierarchicky zaradiť pod širšie vymedzenú množinu, ktorú označujeme ako **technológie distribuovaného ledgeru** (distributed ledger technology – DLT), ktoré charakterizujeme ako *„určitú kombináciu komponentov zahŕňajúcu formu sieťového prepojenia peer-to-peer, distribuovaného úložiska údajov a kryptografie, ktorá okrem iného môže potenciálne zmeniť spôsob ukladania, vedenia záznamov a prevodu digitálnych aktív"*[8]. Inými slovami túto technológiu (označovanú aj ako **technológia distribuovanej účtovnej knihy**) možno popísať ako prostriedok slúžiaci na ukladanie informácií, resp. na vytváranie opakovaných digitálnych kópií dostupných (v rovnakom čase) na viacerých miestach.[9]

Práve pomocou týchto technológií zabezpečujeme overovanie transakcií „v účtovnej knihe" (v blockchaine) a jej následnú synchronizáciu. Absenciu určitej centrálnej autority, ktorá by nad touto knihou dohliadala, nahrádzajú konsenzuálne validačné procesy (napr. pri blockchaine najpoužívanejší Proof of Work– viď nižšie).[10]

V nadväznosti na tieto skutočnosti, vychádzajúc aj zo samotného názvu (chain – reťaz), definujeme **Blockchain** ako neustále sa rozširujúci, chronologicky vytváraný reťazec záznamov, resp. blokov (block) transakcií vzájomne prepájaných prostredníctvom kryptograficky zabezpečených peer-to-peer reťazcov.[11]

Inak povedané, blockchain sa nenachádza na jednom konkrétnom serveri, je distribuovaný medzi všetky uzly, ktoré s ním interagujú, pričom žiaden z týchto uzlov ho nevlastní, avšak má k nemu prístup.[12]

Principiálna funkčnosť blockchainu značne presahuje ciele tohto článku. Jeho fungovanie preto v nasledujúcich riadkoch opíšeme len veľmi zjednodušene. Osoba A disponuje určitou peňaženkou virtuálnych mien [tzn. disponuje súkromným, ako aj

---

[6] ŠANTA, J. a I. ŠANTA, 2022. K niektorým legislatívnym a ekonomickým aspektom virtuálnych mien v legislatíve Európskej únie a Slovenskej republiky. In: *Justičná revue, 2/2022*, str. 485-486.

[7] MAČUHOVÁ, V. a VARGA, 2022. Kryptoaktíva a dane. Legislatívne definície – obsahové vymedzenie kryptoaktív a prehľad aktivít vo virtuálnom svete. In: *Bulletin Slovenskej komory daňových poradcov*, *4/2022*, str. 8.

[8] MILLS, D. et al., 2016. *Distributed ledger technology in payments, clearing, and settlement. Finance and Economics Discussion Series 2016-095*. [online].[cit. 23. október 2023] Dostupné na internete: https://www.federalreserve.gov/econresdata/feds/2016/files/2016095pap.pdf .

[9] Bank for International Settlements, 2023. *Annual Economic Report (June 2023.* [online].[cit. 23. október 2023] Dostupné na internete: https://www.bis.org/publ/arpdf/ar2023e.pdf

[10] MAČUHOVÁ, V. a VARGA, 2022. *Kryptoaktíva a dane. Legislatívne definície – obsahové vymedzenie kryptoaktív a prehľad aktivít vo virtuálnom svete*. In: *Bulletin Slovenskej komory daňových poradcov*, *4/2022*, str. 8.

[11] STROUKAL, D. a J. SKALICKÝ, 2021. *Bitcoin a jiné kryptopeníze budoucnosti, 3. rozšířené vydání*, str. 28-32

[12] Napr. blockchain Bitcoinu možno sledovať na doméne: https://www.blockchain.com/explorer

verejným kľúčom (verejnou adresou)]. Tieto chce previesť na verejnú adresu (verejný kľúč) osoby B. Pri prevode virtuálnych mien ide v podstate o odoslanie určitého súboru informácií (informácie o odosielateľovi, príjemcovi, počte odosielaných jednotiek a transakčnom poplatku), ktorý sa pomocou **kryptografických hashovacích funkcií** (napr. pri procese ťažby Bitcoinu ide o jednosmernú hashovaciu funkciu SHA256) „zahashuje" a vytvorí sa tým unikátny „odtlačok" (ako napr. odtlačok prsta, tu však ide o určitý číselný reťazec), ktorý označujeme pojmom **hash.**[13] V tomto momente do procesu vstupujú aj tzv. **ťažiari** (miners), ktorých primárnou úlohou je potvrdzovanie, resp. overovanie transakcií a ich zoskupovanie do vyššie spomínaných blokov. Každý nasledujúci blok obsahuje informácie o zrealizovaných transakciách, čase kedy bol blok vytvorený a hash predchádzajúceho bloku. Ťažiar k týmto informáciám pripája ešte aj tzv. **nounce**, ktorý predstavuje náhodné číslo. Ďalej sa takýto súbor pomocou kryptografických hashovacích funkcií tiež „zahashuje, a tým pádom sa aj tento blok opatrí vlastným **hashom**. Bloky sú ďalej rozosielané každému **uzlu (full-nodes)**[14], ktorý v rámci blockchainu operuje, a ktorý overuje kompatibilitu v ňom uvedených informácií. Informácie sa teda porovnávajú a kontrolujú a v prípade, ak by sa ich niekto počas tohto procesu pokúšal zmeniť, resp. sa pokúšal zmeniť obsah bloku (napr. verejnú adresu, na ktorú má byť virtuálna mena odoslaná), dôjde aj k zmene hashu. Ako sme už skôr uvideli, každý nasledujúci blok takisto obsahuje aj **hash predchádzajúceho bloku**, na ktorý sa „pripája" (vzniká reťaz – chain). Pokusy o neoprávnené zmeny blokov eliminujeme prostredníctvom **algoritmov pre vytváranie konsenzu v blockchaine**. Medzi jeden z najpoužívanejších patrí tzv. **Proof of work**[15], pričom tento výrazne sťažuje akúkoľvek neželanú manipuláciu s blokom, keďže, ak by sa niekto pokúšal zmeniť hash niektorého z blokov, musel by zmeniť aj hash predchádzajúceho bloku a následne aj všetkých predchádzajúcich blokov. Blok je do blockchainu pridaný až potom, ako dosiahne vyššie uvedený konsenzus v blockchaine. Bloky, ktoré boli akýmkoľvek nežiadúcim spôsobom upravované, budú odmietnuté a do blockchainu sa nezapíšu. Takéto manipulácie sú však prakticky nemožné, keďže aktuálna veľkosť blockchainu je (v momente písania tohto článku) približne 508,41 GB[16]. Ak si uvedomíme, že tu neoperujeme so žiadnym grafickým prvkom, ale len s „čistými" informáciami, ide skutočne o enormné množstvo dát.[17]

Spôsoby uchovávania súkromného kľúča

Tak, ako vyplýva z vyššie uvedeného, pravdepodobnosť ohrozenia, resp. prelomenia zabezpečovacieho systému blockchainu je naozaj mizivá. Hrozbu však stále predstavuje nedostatočná miera zabezpečenia, čo ostáva v gescii buď koncového užívateľa alebo tzv. zmenárne, resp. kryptomenovej burzy. Inými slovami, ľudský faktor a ľudská vynaliezavosť operujú aj v tejto oblasti a bezpečnosť virtuálnych mien preto môže ohroziť napr. klasický phising či iné formy a spôsoby páchania kybernetickej kriminality (warez, malware a pod.). V nadväznosti na uvedené sa odporúča kombinovať prvky, ktoré v ďalšom texte opíšeme.

Virtuálne meny (resp. súkromný kľúč, ktorý zabezpečuje prístup k určitému počtu jednotiek virtuálnej meny – viď nižšie) možno zabezpečiť viacerými spôsobmi. Ešte predtým,

---

[13] STROUKAL, D.a J. SKALICKÝ, 2021. *Bitcoin a jiné kryptopeníze budoucnosti, 3. rozšířené vydání*, str. 90-93

[14] Okrem ťažiarov (miners) v decentralizovaných systémoch operujú aj ďalšie skupiny používateľov, a to používatelia (light-nodes), ktorí zväčša len realizujú transakcie a full-nodes, ktorí okrem realizácie transakcií takisto prijímajú a kontrolujú informácie od používateľov (light-nodes) a iných uzlov (full-nodes).

[15] Proof of work je len jedným z mnohých modelov, ktoré sú v rámci dosahovania konsenzu používané (napr. Proof of importance, Proof of stake...)

[16] *Blockchain: Blockchain Size (MB)* [online]. [cit. 23. október 2023] Dostupné na internete: https://www.blockchain.com/explorer/charts/blocks-size

[17] STROUKAL, D. a J.SKALICKÝ, 2021. *Bitcoin a jiné kryptopeníze budoucnosti, 3. rozšířené vydání*, str. 41-49 a 90-95.

ako si ich priblížime, charakterizujeme už viackrát použitý pojem súkromných, či verejných kľúčov a takisto si v krátkosti priblížime aj **decentralizovanú správu účtov**.

V tomto kontexte možno opätovne poukázať na decentralizáciu virtuálnych mien, odrazom ktorej je **absencia centrálnej autority zabezpečujúcej kontrolu a taktiež aj správu transakcií, účtov** a pod. Túto centrálnu inštitúciu pri decentralizovaných systémoch (akým je napr. aj blockchain) takisto zabezpečujeme prostredníctvom **inštrumentov asymetrickej kryptografie** – verejného kľúča (public key) a súkromného kľúča (private key).[18]

Súkromný kľúč (private key) je určitý reťazec znakov a číslic, ktorý predstavuje jeden z páru kľúčov vytvorených pomocou **asymetrickej kryptografie**. Uvedený reťazec je dôležité uchovať v tajnosti, keďže slúži k dešifrovaniu správči k podpisu správy, ktorá nesie informáciu o tom, komu (na akú adresu) budú pripísané odosielané jednotky určitej virtuálnej meny v rámci konkrétnej transakcie.[19]

Pri blockchaine Bitcoinu možno vytvoriť 2^{256} (v dvojkovej sústave: 101010100....) možností jeho finálnej podoby, pričom nie je vyobrazovaný v binárnej sústave, ale v hexadecimálnej, ktorá ho vyobrazí pomocou 64 znakov (v šestnástkovej sústave: D8790R897E865...).[20]

Dvojičkou súkromného kľúča je, ako už možno logicky usúdiť, **verejný kľúč (verejná adresa)**. Jeho funkcionalita je vo všeobecnosti opakom vyššie uvedeného súkromného kľúča, tzn., že prostredníctvom verejného kľúča možno zašifrovať správu pre majiteľa kľúča súkromného. V blockchaine Bitcoinu však plní úlohu verejnej adresy, na ktorú sú v rámci transakcií posielané jednotky určitej virtuálnej meny.[21]

Nielen široká verejnosť, ale aj niektoré odborné zdroje nesprávne interpretujú funkcionalitu peňaženiek (známych aj ako „crypto wallets“) a častokrát uvádzajú, že „na peňaženkách možno uchovávať svoje virtuálne meny“. Toto tvrdenie však nie je pravdivé, **peňaženky v akejkoľvek forme** (pozri nižšie) **uchovávajú len súkromný kľúč a nie samotné virtuálne meny** (resp. ich jednotlivé deriváty).[22]

Peňaženky slúžia na správu súkromných kľúčov, ktoré odkazujú na určitú adresu, kde sú jednotky virtuálnej meny uložené. Okrem „správy účtu“ peňaženka pre jej majiteľa sprostredkúva napr. informácie o tržnej hodnote jednotiek konkrétnej virtuálnej meny, evidenciu známych adries, s ktorými už v minulosti interagovala a pod.[23]

V tejto súvislosti je dôležité uvedomiť si, že ak dôjde k strate, resp. poškodeniu určitej peňaženky, táto skutočnosť ešte sama o sebe **nepredstavuje aj stratu jednotiek virtuálnej meny**. Ako sme už viackrát zdôraznili, peňaženky uchovávajú len súkromný kľúč, a nie samotné virtuálne meny. Uvedené možno vysvetliť na príklade: ak určitá osoba vlastnila hardvérovú peňaženku, ktorú stratila (alebo poškodila), no svoj súkromný kľúč (ktorý na nej uchovávala) si zapísala napr. aj na papier, môže „svoju“ virtuálnu menu opätovne získať, a to tak, že zadá **„SEED frázu“** a obnoví si tak svoj súkromný kľúč (a tým pádom aj prístup k jednotkám virtuálnej meny) v inej hardvérovej peňaženke.

Typy peňaženiek

V kontexte vyššie uvedených informácií diferencujeme medzi týmito **spôsobmi uchovávania súkromného kľúča**:

---

[18] HOSP, J., 2018. *Kryptomeny Bitcoin, Ethereum, Blockchain, ICO and Co. jednoducho a zrozumiteľne*, str. 43-44.
[19] STROUKAL, D. a J. SKALICKÝ, 2021. *Bitcoin a jiné kryptopeníze budoucnosti, 3. rozšířené vydání*, str. 98.
[20] HOSP, J. 2018. *Kryptomeny Bitcoin, Ethereum, Blockchain, ICO and Co. jednoducho a zrozumiteľne*, str.44-45.
[21] STROUKAL, D. a J. SKALICKÝ,2021. *Bitcoin a jiné kryptopeníze budoucnosti, 3. rozšířené vydání*, str. 100.
[22] HOSP, J. 2018. *Kryptomeny Bitcoin, Ethereum, Blockchain, ICO and Co. jednoducho a zrozumiteľne*, str. 83.
[23] STROUKAL, D. a J. SKALICKÝ, 2021. *Bitcoin a jiné kryptopeníze budoucnosti, 3. rozšířené vydání*, str. 47.

Cold storage predstavuje súhrnné označenie pre rozdielne typy peňaženiek, ktorých spoločným menovateľom je offline prostredie. Inými slovami ide o riešenie, ktoré **uchováva súkromný kľúč prostredníctvom offline médií**, resp. rôznych periférií vyrábaných súkromnou sférou.[24] Do tejto kategórie zaraďujeme papierové, pamäťové a hardvérové peňaženky.

Papierová peňaženka (paper wallet) – tieto peňaženky sa používali ako jedny z prvých, no používajú sa dodnes. Z názvu možno usúdiť, že médiom uchovávajúcim súkromný kľúč je papier, na ktorý sa kľúč vygenerovaný prostredníctvom rôznych generátorov[25] zapíše. Neodporúča sa použiť guľôčkové pero, keďže atrament môže pôsobením času vyblednúť aj bez pôsobenia vonkajších vplyvov. Na účel zvýšenia miery zabezpečenia možno súkromný kľúč zapísať na viacero papierov a tie následne uložiť na rôznych (v ideálnom prípade zabezpečených) miestach.[26] Pre úplnosť dodávame, že v teoretickej rovine možno uvažovať o rôznych druhoch médií, na ktoré je možné poznačiť si súkromný či verejný kľúč (v médiách už boli prezentované aj prípady osôb, ktoré si verejnú adresu dali vytetovať priamo na svoje telo).

Pamäťová peňaženka (mind wallet) – v záujme komplexnosti tejto diverzifikácie uvádzame aj kontroverzný koncept pamäťovej peňaženky, ktorý sa však často nevyužíva. V teoretickej rovine by toto riešenie pripadalo do úvahy pre jedincov s dobrou, resp. (doposiaľ experimentálne neoverenou) eidetickou pamäťou. Súkromný kľúč človek uchováva v materiálnom prostredí mozgu ako pamäťovú stopu. Takto uchovávaný súkromný kľúč síce nie je možné napadnúť žiadnym z kybernetických útokov, môže však dôjsť k jeho zániku pri poškodení pamäťovej stopy, napr. pri rôznych ochoreniach postihujúcich mozog, resp. pri komócii mozgu a pod.[27]

Hardvérová peňaženka (hard wallet) – kategóriu **cold storage** nám uzatvárajú peňaženky pripomínajúce USB kľúče. Tieto zariadenia však v žiadnom prípade nemožno stotožňovať (aj keď sú už registrované prípady, kedy páchatelia predávali USB kľúče, ktoré prezentovali ako hardvérové peňaženky). V tomto prípade ide o periférium, ktorá komunikuje s operačným systémom zariadenia po zadaní (vopred nastaveného) **PIN kódu**. Súkromný kľúč je uchovávaný priamo na tejto perifériі (tzn. offline), to však **neznamená**, že ho (znakovo-číselný reťazec) na zaistenie virtuálnych mien postačuje preniesť, resp. skopírovať na iné zariadenie. Spracovávanie transakcií prostredníctvom hardvérových peňaženiek prebieha týmto spôsobom:

- peňaženka cez USB rozhranie príjme transakciu od počítača, ktorý túto získal zo siete (blockchain),
- peňaženka následne podpíše transakciu (pomocou súkromného kľúča),
- peňaženka cez USB rozhranie prenáša informácie o vykonaných úkonoch späť do počítača, ktorý následne odosiela dáta do siete (blockchainu). [28]

Aktuálny trh ponúka množstvo druhov hardvérových peňaženiek. Medzi ich najznámejších poskytovateľov radíme českú spoločnosť SatoshiLabs (napr. **TREZOR T**) a Ledger (napr. **Ledger Nano**).

---

[24] PERPER, R, 2022. *Hot vs. Cold Crypto Storage: What Are the Differences?* Dátum aktualizácie: 17. mája 2023 [online].[cit. 24. októbra 2023]. Dostupné na internete: https://www.coindesk.com/learn/hot-vs-cold-crypto-storage-what-are-the-differences/

[25]Napr. pre Bitcoin možno použiť generátor dostupný na doméne: https://bitcoinpaperwallet.com/bitcoinpaperwallet/generate-wallet.html

[26] *Metodika postupu pri zaisťovaní virtuálnych mien pre útvary Policajného zboru*, str. 15.

[27] HOSP, J. 2018. *Kryptomeny Bitcoin, Ethereum, Blockchain, ICO and Co. jednoducho a zrozumiteľne,* str. 83-86.

[28] *Metodika postupu pri zaisťovaní virtuálnych mien pre útvary Policajného zboru*, str. 13-15.

Termín **hot storage** reprezentuje riešenie, ktoré uchováva virtuálnu menu v rozhraní aplikácie alebo platformy, ktorá je **pripojená na internet**, tzn. pracuje v **online režime**.[29] Toto riešenie je často spájané s **KYC procedúrami**[30], pričom práve táto skutočnosť je z hľadiska zaisťovania, trasovania a samotného vyšetrovania trestnej činnosti spojenej s virtuálnymi menami kruciálnym kritériom, pre ktoré väčšina páchateľov v rámci svojich kriminálnych aktivít uprednostňuje **hardvérové peňaženky** (ako **cold storage** s absenciou KYC procedúr). Kategóriu hot storage reprezentujú softvérové peňaženky a online (depozitné) peňaženky.

Softvérová peňaženka (soft wallet) – výhodou tohto typu peňaženiek je, že na rozdiel od offline hardvérových peňaženiek sú (vo väčšine prípadov) dostupné bezplatne, poskytujú príjemné používateľské rozhranie, ktoré môže byť priamo prepojené na konkrétnu platformu, kde s nimi možno aj obchodovať, vykonávať transakcie, prípadne ich použiť na kúpu rôznych virtuálnych či iných predmetov. V záujme korektnosti je však dôležité zdôrazniť, že softvérové peňaženky je možné používať i vo forme **cold storage**, a to napr. v prípade peňaženiek Electrum, ktoré možno stiahnuť a nainštalovať na zariadenie, ktoré bude permanentne v offline režime. V tomto prípade možno hovoriť o rovnakej miere ochrany, akú ponúka aj hardvérová peňaženka. Vo všeobecnosti však softvérové peňaženky (využívané ako **hot storage**) **neposkytujú takú mieru bezpečnosti ako hardvérové peňaženky.** Tieto peňaženky (resp. databázy a servery, na ktorých sú spustené) sú častokrát terčom rôznych hackerských útokov. Medzi najznámejšie softvérové peňaženky možno zaradiť napr. **Electrum**, **Metamask**, **Exodus** ap.[31]

Zmenárne alebo aj **online (depozitné) peňaženky** (exchanges alebo aj custodial wallets či hosted wallets) – najväčšie pohodlie pre používateľa, zároveň však (z technologického pohľadu) s najvyšším bezpečnostným rizikom, ponúkajú tzv. depozitné peňaženky, resp. burzy, napr. **Binance**, **Coinbase** a pod. Ako najviac rizikové ich opisujeme z toho dôvodu, že používatelia, ktorí sa ich rozhodnú využiť, **odovzdávajú celkovú správu nad svojimi súkromnými kľúčmi** do rúk danej spoločnosti. Tento typ peňaženiek poskytuje používateľom možnosť rýchlej výmeny a prevodov virtuálnej meny, a to aj bez nutnosti poznať technologické aspekty, ktoré sú späté s ich úschovou. Rovnako ako aj v predchádzajúcom prípade, aj tu hrozbu predstavujú rôzne druhy kybernetických útokov (napr. malware, hacking a pod.).[32]

Ak vychádzame z vyššie uvedeného, peňaženky spadajúce do kategórie cold storage, sú z technologického pohľadu pri dodržaní základných bezpečnostných zásad (napr. v prípade paper wallet sa neodporúča vyhotoviť digitálnu kópiu uvedeného kľúča – odfotografovaním a pod.) bezpečnejšie ako peňaženky využívané ako hot storage. Na druhej strane pre OČTK je vzhľadom na absenciu KYC procedúr oveľa náročnejšie trasovanie transakcií prevádzaných z/do cold storage peňaženiek. Hot storage peňaženky poskytujú svojim používateľom oveľa pohodlnejšie používateľské rozhranie, vo väčšine prípadov sú dostupné zadarmo a umožňujú

---

[29] PERPER, R., 2022. *Hot vs. Cold Crypto Storage: What Are the Differences?* Dátum aktualizácie: 17. mája 2023 [online]. [cit. 24. októbra 2023]. Dostupné na internete: https://www.coindesk.com/learn/hot-vs-cold-crypto-storage-what-are-the-differences/

[30] Z ang. **know your customer** (poznaj svojho zákazníka) **procedúry**, ktoré možno vnímať ako súbor štandardných procedúr používaných rôznymi finančnými inštitúciami pri nadväzovaní obchodných vzťahov s klientmi. Primárne sa zameriavajú na overenie identity zákazníka a identifikáciu potenciálnych rizík, ktoré vyplývajú z tohto ich obchodného vzťahu, pozornosť takisto sústreďujú na zdroje finančných príjmov a peňažné toky konkrétneho zákazníka.

[31] HOSP, J., 2018. *Kryptomeny Bitcoin, Ethereum, Blockchain, ICO and Co. jednoducho a zrozumiteľne*, str. 86-87.

[32] BEDNÁR, J., 2020. *Kryptomenová peňaženka vs burza – aký je rozdiel?* Dátum publikovania 2. marca 2020. [online]. [cit. 24. októbra 2023]. Dostupné na internete: https://paralelnapolis.sk/kryptomenova-penazenka-vs-burza-aky-je-rozdiel/

rýchlu a pohodlnú výmenu, resp. prevod virtuálnych mien. Naproti tomu najfrekventovanejšie využívaný typ cold storage peňaženiek – hardvérové peňaženky je potrebné zakúpiť (suma hardvérovej peňaženky TREZOR T je v čase písania článku približne 225 eur) a obchodovanie virtuálnych mien je s ich použitím komplikovanejšie, ale (za predpokladu dodržania bezpečnostných záruk) aj bezpečnejšie.

Trasovanie transakcií virtuálnych mien pomocou nástrojov spoločnosti Chainalysis

Ako sme už vyššie uviedli, vzhľadom na decentralizáciu virtuálnych mien nevyhnutnou súčasťou „ekosystému kryptomien" je technológia distribuovaného ledgera, a teda blockchain, ktorý poskytuje základný rámec informácií o transakciách s virtuálnymi menami. Páchatelia však disponujú bohatou plejádou rozmanitých metód a techník, ktorými sa pokúšajú maskovať toky zrealizovaných transakcií. Vzhľadom k tomu je mimoriadne náročné, ba priam nemožné tieto transakcie sledovať len pomocou záznamov validovaných transakcií, ktoré sú voľne dostupné v blockchaine. V zahraničí sa preto problému chopili **súkromné analytické spoločnosti**, ktoré OČTK ponúkli svoje komerčné softvérové riešenia v podobe rôznych analytických nástrojov. Spomedzi najznámejších spoločností ponúkajúcich tieto riešenia možno uviesť napr. **CipherBlade**, **Elliptic**, **Blockchain Intelligence Group** a v neposlednom rade aj už viackrát spomínanú spoločnosť **Chainalysis**, ktorej produkty si v krátkosti priblížime v nasledujúcej stati.[33]

Prvý z produktov nesie názov **Businness Data**. Tento produkt umožňuje sledovať adresy klientov a identifikovať transakcie realizované pred i po odoslaní na určitú platformu. Uvedená funkcionalita môže byť užitočná najmä v nadväznosti na hojne využívanú metódu tzv. **chain hoppingu** (preskakovanie medzi blockchainami) spočívajúcu v konverzii virtuálnych mien, ktoré využívajú odlišné blockchainy (napr. prevod Bitcoinu na Ether). Popisovaný softvérový nástroj ponúka aj možnosť sledovať transakcie smerujúce na adresy, ktorých majitelia sú v databáze Chainalysis označení za osoby v minulosti sa podieľajúce na procese legalizácie výnosov z trestnej činnosti alebo ako obchodníci s nelegálnym tovarom napr. na „darknete".[34]

Ďalším softvérovým nástrojom, ktorý spoločnosť ponúka, je produkt **KYT (Know Your Transaction –** poznaj svoju transakciu**)**, ktorého názov je odvodený od KYC procedúr. Uvedený softvérový nástroj umožňuje monitorovať jednotlivé adresy, ktoré boli priradené ku konkrétnym fyzickým či právnickým osobám alebo iným subjektom. Jednou z jeho funkcií je aj detekcia využitia **tumblerov**[35] alebo informovanie o prijatí virtuálnych mien adresou disponujúcou už odcudzenými virtuálnymi menami.[36]

Ako posledný z komerčných nástrojov spomenieme **Reactor**, ktorý dátová spoločnosť prezentuje ako vyšetrovací softvér umožňujúci vizualizovať tok jednotlivých transakcií medzi zúčastnenými stranami. Produkt identifikuje pokusy o maskovanie toku týchto transakcií a v neposlednom rade s využitím umelej inteligencie spätne vyhľadáva a následne vyhodnocuje pre konkrétny prípad relevantné a z trestnoprávneho hľadiska rizikové transakcie.[37]

---

[33] ŠANTA, J. a I. ŠANTA, 2022. Procesnoprávne aspekty trestnej činnosti spojenej s virtuálnymi menami. In: *Justičná revue 10/2022*, s. 1156.

[34] Chainalysis. *Blockchain Customer Intelligence. Chainalysis Business Data*. [online].[cit. 24. októbra 2023]. Dostupné na internete: https://www.chainalysis.com/chainalysis-business-data/ a ŠANTA, J. a I. ŠANTA, 2022. Procesnoprávne aspekty trestnej činnosti spojenej s virtuálnymi menami. In: *Justičná revue 10/2022*, s. 1157.

[35] Ide o nástroj, resp. službu, ktorá umožňuje spájať či rozdeľovať transakcie s virtuálnymi menami s cieľom sťaženia ich sledovania a nájdenia pôvodného zdroja.

[36] ŠANTA, J.a I. ŠANTA, 2022. Procesnoprávne aspekty trestnej činnosti spojenej s virtuálnymi menami. In: *Justičná revue 10/2022*, s. 1159.

[37] Chainalysis. *Cryptocurrency Forensics. Chainalysis Reactor*. [online]. [cit. 24. októbra 2023]. Dostupné na internete: https://www.chainalysis.com/chainalysis-reactor/

Ako sme už uviedli, spoločnosť Chainalysis nie je na trhu jediná, ktorá poskytuje tento druh služieb. Jej produkty sa však aktuálne považujú za najefektívnejšie svojho druhu. Samozrejme, aj konkurenčné spoločnosti ponúkajú mnoho podobných analytických softvérových aplikácií, spomedzi ktorých za zmienku stojí aj **Qualitative Law Enforcement Unified Edge** (Kvalitatívna výhoda v zjednotenom vymáhaní práva), ktorú na trh uviedla vyššie spomínaná spoločnosť **Blockchain Intelligence Group**. Tento nástroj pridáva k službám na analyzovanie transakcií aj možnosť **vrátenia virtuálnych mien** naspäť ich oprávneným držiteľom v prípade, že sa ich OČTK podarilo vypátrať.[38]

Zaisťovanie virtuálnych mien

Vzhľadom na prezentované informácie možno bez ďalšej polemiky uviesť, že rozhodujúca je v tomto kontexte práve kvalitná a proaktívna spolupráca OČTK a súkromného sektora zastúpeného poskytovateľmi služieb peňaženky, resp. zmenárne virtuálnej meny[39] a analytickými spoločnosťami, ktorých nástroje predstavujú nielen jeden z kľúčových determinantov úspešnosti odhaľovania, ale aj samotného vyšetrovania trestnej činnosti asociovanej s virtuálnymi menami.

Poukázaním na takpovediac okamžitú negociabilitu virtuálnych mien v online priestore je viac ako žiadúci prvotný operatívny postup s poskytovateľmi služieb peňaženky, resp. zmenárne virtuálnej meny, ktorý bude ex post „sprocesnený“. V aplikačnej praxi sa, bohužiaľ, stretávame aj s prípadmi, keď aj tieto sú subjekty zaangažované v legalizačných schémach, prípadne nie sú ochotné spolupracovať či dokonca upozorňujú podozrivé osoby na to, že boli požiadané o poskytnutie súčinnosti v zmysle § 3 ods. 1 TP. V tomto kontexte nemožno opomenúť ani ďalšie významné subjekty, ktoré v danom procese vystupujú, a to **finančnú spravodajskú jednotku Prezídia Policajného zboru,** ktorá *„plní úlohy centrálnej národnej jednotky v oblasti predchádzania a odhaľovania legalizácie a financovania terorizmu“*[40], ako aj **Úrad pre správu zaisteného majetku**, s ktorým OČTK kooperujú už pri samotnej realizácií zaisťovacieho úkonu.[41]

S cieľom zaistiť virtuálne meny je dôležité, aby OČTK disponovali už vyššie popísaným fundamentálnym súborom znalostí o technologických aspektoch virtuálnych mien, najmä o **spôsoboch uchovávania súkromných kľúčov** a takisto i o iných pojmoch, s ktorými TP operuje v ustanovení **§ 96d** s názvom **„Zaistenie virtuálnej meny“**. V nasledujúcich riadkoch preto vykonáme čiastkovú analýzu tohto ustanovenia v jeho vzájomnej korelácií s inými, naň nadväzujúcimi technologickými aspektmi.

Predpokladom vydania príkazu na zaistenie virtuálnej meny je prítomnosť dôvodného podozrenia o tom, že virtuálna mena je **nástrojom trestnej činnosti** alebo **výnosom pochádzajúcim z trestnej činnosti**. Príkaz na zaistenie však takisto možno vydať aj v tom prípade, ak zistené informácie nasvedčujú tomu, že virtuálna mena je potrebná k **zabezpečeniu nároku poškodeného na náhradu škody** alebo aj v prípade potreby zaistenia výkonu trestu prepadnutia majetku podľa § 425 TP.[42] Opierajúc sa o ustanovenie § 89 TP, označujeme oba vyššie uvedené pojmy za **vec dôležitú pre trestné konanie**, pričom ods. 1 písm. b) predmetného ustanovenia explicitne konkretizuje **nástroj trestnej činnosti** ako vec, ktorá **bola použitá** na spáchanie trestného činu alebo **bola určená** na jeho spáchanie.

---

[38] ŠANTA, J.a I. ŠANTA, 2022. Procesnoprávne aspekty trestnej činnosti spojenej s virtuálnymi menami. In: *Justičná revue 10/2022,* s. 1160.

[39] *§ 5 ods. 1 písm. o) a písm. p) zákona 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.*

[40] *§ 26 ods. 1 zákona 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*

[41] MARR, S. a B. SUCHOVSKÝ, 2023. Právno-aplikačné problémy zaisťovania kryptomien. In: *Bulletin Slovenskej advokácie, 5/2023,* str. 5-6.

[42] IVOR, J.; POLÁK, P a J. ZÁHORA, 2021. *Tresté právo procesné I. Všeobecná časť,* str. 410.

Diferenciačným prvkom je v tomto prípade **časové hľadisko**. Vec, ktorá **bola použitá** na spáchanie trestného činu, je vec, o ktorej možno dôvodne predpokladať, že ju páchateľ pri páchaní trestného činu **už použil**. Z uvedeného možno konštatovať, že v čase zaistenia tejto veci bol už trestný čin dokonaný a takúto vec z kriminalistického hľadiska možno označiť ako **nositeľa stôp** a z pohľadu trestného práva ako **prameň dôkazu**. V prípade virtuálnych mien možno toto ustanovenie aplikovať napr. pri zaisťovaní hardvérovej peňaženky, a to na účel preukázania napr. manipulácie s touto peňaženkou konkrétnou osobou (napr. obvineným). Na druhej strane vec, ktorá **bola** na spáchanie trestného činu (iba) **určená,** je vec, o ktorej sa možno odôvodnene domnievať, že **má byť v budúcnosti použitá** na spáchanie trestného činu (napr. hardvérová peňaženka, na ktorej sú vyčlenené prostriedky k financovaniu terorizmu).[43]

TP stanovuje pre príkaz na zaistenie virtuálnej meny **písomnú formu** a taktiež jeho náležité **odôvodnenie**. V príkaze sa **zakáže akákoľvek dispozícia s virtuálnou menou**, pričom neuposlúchnutie tohto zákazu sankcionuje TP **absolútnou neplatnosťou právnych úkonov**, a to ***ex tunc***. V tomto individuálnom právnom akte sa ďalej prikáže **vydanie virtuálnej meny,** a to vrátane **hesiel** či **prístupových kódov** alebo **iných údajov** (napr. SEED frázu), ktoré umožnia s virtuálnou menou nakladať. Osobitosť virtuálnych mien sa odráža aj v ďalších obligatórnych náležitostiach, ktorými je **adresa úložiska virtuálnej meny orgánu, ktorý spravuje virtuálnu menu**, **označenie virtuálnej meny** (Bitcoin, Ether ap.) a napokon **určenie počtu jednotiek** konkrétnej virtuálnej meny.[44] Uvedené náležitosti však prinášajú hneď niekoľko aplikačných a takisto aj teoreticko-právnych otázok, resp. problémov. Vzhľadom na predmet nášho záujmu však odhliadneme od teoreticko-právnej dilemy[45] a priestor vyčleníme pre zásadný aplikačný problém dotknutého ustanovenia.

Problémom, ktorý v tomto smere identifikujeme, je situácia, ktorá môže nastať pri zaisťovaní virtuálnych mien (resp. pri zaisťovaní súkromného kľúča, keďže ten je pre nakladanie s virtuálnymi menami „kľúčový“) v prípadoch, keď páchateľ je **jedinou osobou, ktorá disponuje so súkromným kľúčom**. Ako sme už predtým uviedli, pre OČTK je podstatne priaznivejšia situácia, keď má páchateľ zriadený účet na niektorej z búrz (napr. Coinbase, Binance a pod.), keďže v týchto prípadoch so súkromným kľúčom disponuje práve táto spoločnosť. Páchateľ má síce prístup a prihlasovacie údaje k účtu zriadenému na určitej platforme, avšak, **ak sa OČTK podarí nadviazať spoluprácu** so spomínanou burzou, páchateľ už nemá k dispozícii žiadne prostriedky, ktorými by dokázal zaisteniu virtuálnych mien zabrániť.

Čo však v prípade, ktorým sme uviedli tento problém? Odpoveďou je bohužiaľ „nič“. Tak, ako uvádza aj Jochman *„hlavnou výhodou bitcoinu nie je jeho rýchlosť, avšak jeho necenzurovateľnosť a **nekonfiškovateľnosť**“*.[46] Inými slovami, len ten, v koho dispozícií sa nachádza súkromný kľúč rozhoduje, ako sa s jednotkami virtuálnej meny naloží. S cieľom úspešne zaistiť virtuálne meny, resp. k tomu, aby sme mohli úspešne realizovať zaisťovací úkon podľa ustanovenia § 96d TP, je nevyhnutné zabezpečiť údaje (PIN kód, heslo, SEED fráza), ktoré nám umožnia s virtuálnou menou nakladať. K nájdeniu týchto údajov možno použiť aj iné zaisťovacie inštitúty, a to napr. domovú prehliadku alebo prehliadku iných priestorov a pozemkov. V tomto kontexte nie je vylúčená ani realizácia výsluchu. Ak však páchateľ nemá v úmysle s OČTK spolupracovať, tieto s najväčšou pravdepodobnosťou **nenájdu žiadny spôsob, ktorým by bolo možné tento súkromný kľúč získať** (samozrejme,

[43] ČENTÉŠ, J; KURILOVSKÁ, L; ŠIMOVČEK, I a E. BURDA et. al., 2021. *Trestný poriadok. Komentár. I. zväzok,* str. 466-468.
[44] ČENTÉŠ, J; KURILOVSKÁ, L.; ŠIMOVČEK, I. a E. BURDA. et. al. 2021. *Trestný poriadok. Komentár. I. zväzok.* str. 502-503.
[45] Porušenie špeciálnej zásady dokazovania – zásady nemo tenetur se ipsum accusare (zákaz donucovania k sebaobviňovaniu).
[46] SMEJKAL, V., 2022. *Kybernetická kriminalita,* str. 979.

za predpokladu, že páchateľ tento kľúč skryl). V „slepej uličke“ sa možno ocitnúť aj v tom prípade, keď obvinený síce chce spolupracovať, no svoj súkromný kľúč skutočne stratil, prípadne zabudol. Jediným riešením je **obnovovacia (SEED) fráza**, ktorá zväčša pozostáva z 12 až 24 slov, ktorých zadanie sa vyžaduje v tom prípade, ak by majiteľ peňaženky (či už softvérovej alebo hardvérovej) nemal prístup k PIN kódu alebo heslu. Tieto SEED frázy sa takisto uchovávajú na rôznych, napr. aj ohňovzdorných médiách (CRYPTOTAG).

Vychádzajúc z vyššie uvedených skutočností nám neostáva nič iné, len s poľutovaním konštatovať, že v prípadoch, keď súkromným kľúčom disponuje výlučne nespolupracujúci páchateľ, resp. páchateľ, ktorý zabudol alebo stratil súkromný kľúč, je predmetný zaisťovací inštitút **neaplikovateľný**.

V nadväznosti na už skôr prezentované informácie si dovoľujeme opätovne zdôrazniť, že na úspešné zaistenie virtuálnych mien **nepostačuje skopírovať, resp. inak rozmnožiť znakovo-číselný reťazec nachádzajúci sa v internej pamäti hardvérovej peňaženky**. Samotný zaisťovací úkon sa realizuje zaistením súkromného kľúča, a to za súčinnosti špecializovaných policajných zložiek, ktoré v tomto smere kooperujú s **Úradom pre správu zaisteného majetku**, ktorý disponuje virtuálnymi peňaženkami, na ktoré sú potom zaistené virtuálne meny odosielané.[47]

Záver

In fine si dovolíme konštatovať, že virtuálne meny a ich regulačné, no hlavne implementačné procesy sú stále na začiatku svojej neistej cesty. Rovnako chceme i v závere zdôrazniť, že problematika virtuálnych mien je vzhľadom na jej multi-dimenzionálny charakter obsahovo oveľa širšia. Naším zámerom bolo sprostredkovať čitateľovi fundamentálny „balíček“ informácií technologického charakteru, ktoré z pohľadu autora môžu napomôcť nielen študentom Akadémie Policajného zboru v Bratislave, ale aj príslušníkom Policajného zboru, ktorí si v predmetnej oblasti rozšíria svoje vedomosti. Vzhľadom na to, že ide o širokospektrálny a dynamicky sa rozvíjajúci hyperglobálny fenomén, je dôležité uvedomiť si, že i *pro futuro* bude potrebné informácie neustále dopĺňať a obohacovať o nové zistenia reflektujúce vývoj informačno-technologickej sféry. Už dnes však možno v tejto oblasti pozorovať napr. aj odklon páchateľov od Bitcoinu a uchyľovanie sa k virtuálnym menám so zvýšenou anonymitou (napr. Zcash, Monero a pod.). V nadväznosti na čiastkovú analýzu, ktorú sme predostreli, je potrebné poukázať na zásadný problém, ktorým je samotné ustanovenie § 96d TP, jeho problematická aplikácia a nesúlad so špeciálnou zásadou dokazovania v trestnom práve, a to so zásadou *nemo tenetur se ipsum accusare*, ktorá obvinenému zaručuje, že zo strany OČTK či súdu nebude nútený k tomu, aby aktívne participoval na svojom usvedčení. Vzhľadom na to, že v príkaze na zaistenie virtuálnej meny sa ako obligatórna náležitosť uvádza príkaz vydať virtuálne meny, a to spolu s heslom, prístupovým kódom a ďalšími podobnými údajmi, ktoré umožnia s jednotkami virtuálnej meny nakladať, je možné konštatovať, že týmto konaním by páchateľ výrazne napomáhal OČTK pri jeho usvedčení. Ďalším závažným problémom, ktorý so sebou toto ustanovenie prinieslo, je i jeho neaplikovateľnosť v prípadoch, keď páchateľ vystupuje ako jediný a výlučný vlastník súkromného kľúča, ktorý ho nechce alebo nemôže (ak napr. aj on sám zabudol SEED frázu alebo prístupové heslo či samotný súkromný kľúč) odovzdať zo svojej dispozície. V týchto prípadoch OČTK pravdepodobne nenájdu žiadny spôsob, akým by mohli tieto virtuálne meny zaistiť. Z článku je však možné vyabstrahovať aj čiastkové postrehy, napr. uvedomenie si toho, že i pri samotných domových prehliadkach, resp. prehliadkach iných priestorov a pozemkov je potrebné (samozrejme v nadväznosti na operatívne informácie) zamerať svoju pozornosť na konkrétne aspekty uchovávania

[47] ŠANTA, J.a I. ŠANTA, 2022. Procesnoprávne aspekty trestnej činnosti spojenej s virtuálnymi menami. In: *Justičná revue 10/2022*, s. 1158.

virtuálnych mien, ktoré OČTK následne využijú pri určovaní predmetu, ktorý príslušný policajt uvedie v príkaze, ako aj pri inštruktáži jednotlivých policajtov.

Literatúra

BEDNÁR, J., 2020. *Kryptomenová peňaženka vs burza – aký je rozdiel*. [online]. [cit. 24. októbra 2023]. Dostupné na internete: https://paralelnapolis.sk/kryptomenova-penazenka-vs-burza-aky-je-rozdiel/

Blockchain: Blockchain Size (MB). [online]. [cit. 23. október 2023]. Dostupné na internete: https://www.blockchain.com/explorer/charts/blocks-size

ČENTÉŠ, J; KURILOVSKÁ, L.; ŠIMOVČEK, I. a E.BURDA et. al., 2021. *Trestný poriadok. Komentár. I. zväzok.* Praha: C. H. Beck. 1267 s. ISBN 978-80-89603-88-6.

HOSP, J., 2018. *Kryptomeny Bitcoin, Ethereum, Blockchain, ICO and Co. jednoducho a zrozumiteľne*. Vydavateľstvo TATRAN. 172 s. ISBN 978-80-222-0945-8.

Chainalysis. *Blockchain Customer Intelligence. Chainalysis Business Data*. [online]. [cit. 24. októbra 2023]. Dostupné na internete: https://www.chainalysis.com/chainalysis-business-data/

Chainalysis: The Crypto Crime Report 2023. [online]. [cit. 23. október 2023] Dostupné na internete: https://go.chainalysis.com/2023-crypto-crime-report.html

Chainalysis. *Cryptocurrency Forensics. Chainalysis Reactor*. [online]. [cit. 24. októbra 2023]. Dostupné na internete: https://www.chainalysis.com/chainalysis-reactor/

IVOR, J.; POLÁK, P. a J. ZÁJORA, 2021. *Trestné právo procesné I. Všeobecná časť*. 2. vydanie. Bratislava: Wolters Kluwer, 596 s. ISBN 978-80-571-0332-5.

MAČUHOVÁ, V. a P. VARGA, 2022. Kryptoaktíva a dane. Legislatívne definície – obsahové vymedzenie kryptoaktív a prehľad aktivít vo virtuálnom svete. In: *Bulletin Slovenskej komory daňových poradcov, 4/2022*, s.4 – 10 ISSN 2644-688X.

MARR, S.a B. SUCHOVSKÝ, 2023. Právno-aplikačné problémy zaisťovania kryptomien. In: *Bulletin Slovenskej advokácie, 5/2023.* ISSN 1335-1079.

Metodika postupu pri zaisťovaní virtuálnych mien pre útvary Policajného zboru.

MILLS, DAVID et al., 2023. *Distributed ledger technology in payments, clearing, and settlement. Finance and Economics Discussion Series 2016-095*. Washington: Board of Governors of the Federal, 5. decembra 2016. [online]. [cit. 23. október 2023] Dostupné na internete: https://www.federalreserve.gov/econresdata/feds/2016/files/2016095pap.pdf

PERPER, R.. 2022. *Hot vs. Cold Crypto Storage: What Are the Differences?* Dátum aktualizácie: 17. máj 2023. [online]. [cit. 24. októbra 2023] Dostupné na internete: https://www.coindesk.com/learn/hot-vs-cold-crypto-storage-what-are-the-differences/

SMEJKAL, V., 2022. *Kybernetická kriminalita.* 3. vyd. Plzeň: Aleš Čeněk. 1166 s. ISBN 978-80-7380-849-5.

STROUKAL, D.a J. SKALICKÝ, 2021. *Bitcoin a jiné kryptopeníze budoucnosti. Historie, ekonomie a technologie kryptoměn*. Grada Publishing. 294 s. ISBN 978-80-271-1043-8.

ŠANTA, J. a I. ŠANTA, 2022. K niektorým legislatívnym a ekonomickým aspektom virtuálnych mien v legislatíve Európskej únie a slovenskej republiky. In: *Justičná revue, 2/2022*, s. 164 – 179. ISSN 1335-6461. č. 2.

ŠANTA, J. a I. ŠANTA, 2022. Procesnoprávne aspekty trestnej činnosti spojenej s virtuálnymi menami. In: *Justičná revue 10/2022*, s. 1146 – 1164. ISSN 1335-6461.

Zákon Národnej rady Slovenskej republiky 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.

Keywords: virtual currencies, blockchain, storage of virtual currencies, virtual currency wallets, seizure of virtual currencies

Summary

The article discusses the issue of seizure of virtual currencies, with a primary focus on the technological aspects of this complex activity. After a brief introduction, the author presents fundamental technological information that is essential for a deeper understanding of the crypto ecosystem. The author covers distributed ledger and blockchain technologies, as well as the key characteristics of asymmetric cryptography tools, which are further explained, along with insights into methods of private key storage. Towards the conclusion, within a sub-analysis the author highlights the challenges of applying the seizure of virtual currency in cases where the private key is exclusively controlled by an individual who is unwilling or unable to co-operate with law enforcement authorities.

Mgr. Marek Matulík
Oddelenie vedy a vedeckých projektov
Akadémia Policajného zboru v Bratislave
Sklabinská 1
835 17 Bratislava
e-mail: marek.matulik@akademiapz.sk

Recenzent: Mgr. Štefan Zachar, PhD.