

# Kryptoaktiva optikou trestného práva Českej republiky, Slovenskej republiky a práva Európskej únie

## Cryptoassets from the Perspective of Criminal Law of the Czech Republic, the Slovak Republic and the Law of the European Union

Adrián Jalč<sup>\*</sup>, Karin Vrtíková<sup>\*\*</sup>

### Abstrakt

Príspevok sa zaoberá fenoménom súčasnej doby, a to kryptomenami, ktoré sa stávajú súčasťou nie len nášho každodenného života, ale aj života organizovaného zločinu. Na otázky vynárajúce sa v oblasti kryptoaktív neexistujú jednoznačné a už vôbec nie jednoduché odpovede. S ohľadom na to, sa autori budú snažiť priniesť nový pohľad na trestnoprávne aspekty previazané s kryptoaktívami, a to poukázaním na zavedený slovenský inštitút zaistenia kryptoaktíva v zmysle § 96d Trestného poriadku. Zároveň tiež prinášajú aj analýzu právnej úpravy Českej republiky a práva Európskej únie. V tomto kontexte rovnako upriamia pozornosť na možné návrhy de lege ferenda, ktoré do skúmanej problematiky prinesú viac jednoznačnosti a právnej istoty.

### Kľúčová slova

Kryptoaktíva; digitálne euro; zaistenie; trestné konanie.

### Abstract

The article deals with a contemporary phenomenon, namely cryptocurrencies, which are becoming a part not only of our everyday life, but also of organized crime. There are no clear and easy answers to the questions arising in the field of crypto-assets. With this in mind, the authors will try to bring a new perspective on the criminal law aspects associated with crypto-assets, by pointing to the established Slovak institute of seizure of crypto-assets under Section 96d of the Criminal Procedure Code. At the same time, they also provide an analysis of the legal regulation of the Czech Republic and European Union law. In this context, they will also draw attention to possible de lege ferenda proposals that will bring more clarity and legal certainty to the issue under review.

### Keywords

Cryptoassets; Digital Euro; Securing; Criminal Procedure.

\* Prof. JUDr. Ing. Adrián Jalč, PhD., Katedra trestného práva a kriminológie, Právnická fakulta, Trnavská univerzita v Trnave, Slovenská republika / Department of Criminal Law and Criminology, Faculty of Law, Trnava University, Trnava, Slovak Republic / E-mail: [adrian.jalc@truni.sk](mailto:adrian.jalc@truni.sk) / ORCID: 0000-0002-3772-9263

\*\* JUDr. Karin Vrtíková, PhD., Katedra trestného práva a kriminológie, Právnická fakulta, Trnavská univerzita v Trnave, Slovenská republika / Department of Criminal Law and Criminology, Faculty of Law, Trnava University, Trnava, Slovak Republic / E-mail: [kvrtikova@gmail.com](mailto:kvrtikova@gmail.com) / ORCID: 0000-0001-9951-6426 / Scopus ID: 57998161400

## Úvod

**Kryptoaktíva** vo všeobecnosti môžeme definovať ako digitálne aktíva založené na kryptografii (šifrovaní), ktoré sú decentralizované (t. j. nie sú vydávané alebo riadené jednou entitou, napr. centrálnou bankou) a väčšinou fungujú na tzv. blockchainovej technológii. Ide zároveň o súhrnné označenie pre elektronické „mince“, resp. „tokeny“. Ako známe príklady kryptoaktív (ďalej „kryptomeny“) možno uviesť Bitcoin, Ether, Litecoin a Ripple<sup>1</sup>.

Kryptoaktíva sú charakterizované vysokou volatilitou, inovačným potenciálom a absenciou centralizovaného riadiaceho orgánu, čo z nich robí predmet záujmu regulačných orgánov, najmä v kontexte ochrany spotrebiteľov, prevencie prania špinavých peňazí a finančnej stability. V súčasnosti preto vstúpilo do účinnosti **nariadenie Európskeho parlamentu a Rady (EÚ) č. 2023/1114 o trhoch s kryptoaktívami (MiCA), ktoré stanovuje právny rámec pre trh s kryptoaktívami v rámci trhu EÚ**. Cieľom MiCA je zabezpečiť právnu istotu, podporiť inovácie, chrániť spotrebiteľov a investorov a zaistiť finančnú stabilitu tým, že reguluje vydávanie a obchodovanie kryptoaktív, ktoré nespádajú pod súčasné finančné regulácie. Nariadenie tak zavádza takisto požiadavky na poskytovateľov služieb kryptoaktív, vrátane povinností týkajúcich sa transparentnosti, správy a dohľadu a zavádza nové pravidlá pre stablecoiny. MiCA je súčasťou širšieho balíka legislatívnych opatrení EÚ zameraných na podporu digitálnych financií a jej prijatie je považované za kľúčový krok k harmonizácii prístupu kryptoaktív v rámci celej Európskej únie. Týmto nariadením sa začala právna regulácia vo vzťahu k tomuto aktívu zo strany EÚ.

Nariadením Európskeho parlamentu a Rady (EÚ) č. 2023/1114 o trhoch s kryptoaktívami (MiCA) sa už vymedzujú pojmy „služba kryptoaktív“, ktoré sa vzťahujú na zoznam služieb a činností súvisiacich s kryptoaktívami, ktorý primerane odzrkadľuje úplný súbor činností, na ktoré sa vzťahujú nové normy FATF; ako aj vymedzenie pojmu „kryptoaktívum“, ktorý je definovaný ako „*digitálne vyjadrenie hodnoty alebo práv, ktoré možno prenášať a elektronicky uchovávať s použitím technológie distribuovanej databáz y transakcií alebo podobnej technológie*“ a ktorý by takisto mal zodpovedať vymedzeniu pojmu „virtuálne aktíva“ stanovenému v odporúčaniach Finančnej akčnej skupiny (FATF).

Podobne ako Európska centrálna banka (ďalej „ECB“), aj Medzinárodný menový fond (ďalej „MMF“) kategorizoval kryptomeny ako podskupinu virtuálnych mien, ktoré definuje ako digitálne vyjadrenia hodnoty vydávané súkromnými vývojármi a denominované v ich vlastných účtovných jednotkách. Podľa MMF pojem virtuálnych mien pokrýva širšiu škálu „mien“, od jednoduchých IOU („I owe you“ – „neformálne dlžobné certifikáty“) emitentov (ako sú internetové alebo mobilné kupóny), virtuálnych mien krytých aktívami, ako je zlato a kryptomeny, akou je bitcoin. Rovnaký názor zdieľa aj Svetová banka, ktorá definovala samotné kryptomeny ako virtuálne meny, ktoré sa spoliehajú na kryptografické techniky na dosiahnutie konsenzu.

<sup>1</sup> Dostupné z: <https://nbs.sk/dohlad-nad-financnym-trhom/fintech/financne-technologie/co-su-kryptoaktiva/> [cit. 1. 1. 2025].

V závislosti od interakcie s tradičnými menami a reálnou ekonomikou možno rozlíšiť tri typy mien:

- 1) virtuálne meny, ktoré je možné použiť len v uzavretom virtuálnom systéme (zvyčajne v online hrách),
- 2) virtuálne meny, ktoré sú jednostranne prepojené s reálnou ekonomikou – existuje konverzný kurz na nákup meny (za tradičné peniaze, napr. kupónov) a nakúpenú menu je možné následne použiť na nákup virtuálnych tovarov a služieb (a výnimočne aj na nákup reálnych tovarov a služieb),
- 3) virtuálne meny, ktoré sú bilaterálne prepojené s reálnou ekonomikou – existujú výmenné kurzy tak pre nákup virtuálnej meny, ako aj pre predaj takejto meny; nakúpenú menu je možné použiť na nákup virtuálnych aj skutočných tovarov a služieb.

Veľkú časť tretej spomenutej kategórie virtuálnych mien v súčasnosti tvoria tzv. kryptomeny. Kryptomenu možno definovať ako digitálnu reprezentáciu hodnoty, ktorá:

- 1) funguje na báze *peer-to-peer* siete (P2P) ako alternatíva k zákonnému platidlu, ktoré je emitované štátom,
- 2) vo všeobecnosti slúži ako prostriedok výmeny, ktorý je decentralizovaný a nezávislý od akejkoľvek centrálnej banky,
- 3) je zabezpečená na báze mechanizmu kryptografie a
- 4) je vymeniteľná za reálne meny a naopak.

Ich hodnota je určovaná na báze ponuky a dopytu. V súčasnosti existuje už niekoľko tisíc rozdielnych kryptomien, medzi najznámejšie patrí Bitcoin, Ethereum, Tether, Cardano, Stellar, Litecoin, Ripple XRP, NEO, ChainLink a iné.

Vzhľadom na uvedené je potom možné opätovne konštatovať, že pojem **virtuálna mena je širší ako pojem kryptomena** a virtuálnu menu tak môže kľudne tvoriť platidlo používané aj v online hrách.

Predmetom predkladaného príspevku bude problematika virtuálnej meny z pohľadu slovenského trestného práva a tiež inštitút, ktorý bol zavedený do zákona č. 301/2005 Z.z. Trestný poriadok v znení neskorších predpisov (ďalej „Trestný poriadok“), konkrétne **zaistenie kryptoaktíva**. Autori nebudú zaošávať ani v analyzovaní právnej úpravy Českej republiky a poskytnú pohľad aj na európsky rozmer tejto problematiky, a to v totožnom rozsahu. Výsledkom týchto analýz budú identifikované nedostatky právnych úprav a následne sa budú autori snažiť prostredníctvom návrhov *de lege ferenda*, priniesť do skúmanej problematiky viac jednoznačnosti a právnej istoty.

V neposlednom rade bude v predloženom texte vymedzená aj právna rovina digitálneho eura, a to najmä z dôvodu zabezpečenia komplexnosti a nadväznosti informácií previazaných s nosnou témou príspevku, ktorou sú kryptoaktíva. Návrhom nariadenia o zavedení **digitálneho eura**<sup>2</sup> je zabezpečiť, aby peniaze centrálnej banky so statusom zákonného platidla ponúkali moderný a nákladovo efektívny platobný prostriedok, zabezpečovali vysokú

<sup>2</sup> Dostupné z: [https://eur-lex.europa.eu/resource.html?uri=cellar:6f2f669f-1686-11ee-806b-01aa-75ed71a1.0014.02/DOC\\_2&format=PDF](https://eur-lex.europa.eu/resource.html?uri=cellar:6f2f669f-1686-11ee-806b-01aa-75ed71a1.0014.02/DOC_2&format=PDF) [cit. 1. 1. 2025].

úroveň ochrany súkromia pri digitálnych platbách a zachovali finančnú stabilitu. Podobne ako dnes hotovosť, aj digitálne euro by malo byť dostupné popri existujúcich vnútroštátnych a medzinárodných súkromných platobných prostriedkoch (napr. karty, aplikácie). Fungovalo by tak ako digitálna peňaženka, t. j. ľudia a podniky by mohli platiť digitálnym eukrom kedykoľvek, kdekoľvek a bez poplatkov v eurozóne. Samozrejme digitálnemu eukrom sa udeľuje status zákonného platidla, čo okrem iného znamená jeho povinné prijímanie príjemcami a trestnoprávnu ochranu. Na dôvažok je potrebné spomenúť aj ochranu hotovosti, ktorá je súčasťou právnej ochrany Slovenskej republiky, avšak je skôr tuzemským unikátom, ako pravidlom. Táto ochrana meny v súčasnej dobe rozvoja virtuálnych mien, najmä pripravovaného digitálneho eura bude určite adresátom viacerých zmien.

## 1 BITCOIN

Koniec dvadsiateho a začiatok tohto storočia môžeme charakterizovať ako obdobie rozvoja bezhotovostných platieb. Ruka v ruke s rozmachom internetu došlo aj k rozšíreniu internetového bankovníctva, zavedeniu platobných kariet a ich virtuálnemu preneseniu do mobilných telefónov, hodínok, prsteňov. Začiatkom druhého tisícročia, konkrétne v roku 2009 došlo k predstaveniu prvej decentralizovanej virtuálnej meny – Bitcoinu<sup>3</sup>. Zatiaľ čo existujúce virtuálne meny mali centralizované subjekty ako sprostredkovateľov, táto nová mena sa stala populárnou kvôli absencii tretej strany v transakciách. Jeho používanie online technológiami v kombinácii s kryptografiou vyústilo do úplne nového prenosového systému, kde môže byť platba odoslaná priamo bez použitia sprostredkovateľa, akými sú centrálna banka alebo orgán verejnej moci. Kvôli svojej „virtuálnej podobe“ sa tento typ meny bežne označuje ako virtuálna mena.<sup>4</sup> O virtuálnych menách je nutné uviesť, že sa objavujú vedľa slova „kryptomena“ a často bývajú zamieňané. Na čo je však nutné upriamiť pozornosť je fakt, že označenie virtuálna mena sa spája s menou, ktorá nestojí na kryptografickom základe. Európska centrálna banka definovala vo svojej správe virtuálne meny, ešte v roku 2015 ako: „*Digitálne vyjadrenie hodnoty, ktorá nie je vydaná centrálnou bankou, úverovou inštitúciou alebo inštitúciou elektronických peňazí, ktorú je možné za určitých okolností použiť.*“<sup>5</sup> V tomto smere preto autori konštatujú, že pojem **virtuálna mena je všeobecnejším pojmom, ako je pojem kryptomena.**

<sup>3</sup> Za najznámejšieho tvorca Bitcoinu sa považuje Satoshi Nakamoto, ktorý vyvinul celý systém ťaženia kryptomien a účtovný systém blockchain už v roku 2008. V histórii kryptomien však nie je bitcoin prvou virtuálnou menou, a to aj napriek tomu, že je známy v rámci širokej verejnosti naprieč celým svetom. V dobe pred vznikom Bitcoinu existovalo niekoľko iným, menej známym virtuálnym mien, napr. DigiCash, E-gold a Liberty Reserve. Všetky boli centralizované, teda im chýbala základná vlastnosť, ktorú má Bitcoin, a síce decentralizácia, teda nezávislosť na bankovom sektore, neexistencia riadiaceho systému spravovaného centrálnou bankou.

<sup>4</sup> Europol spotlight – cryptocurrencies: tracing the evolution of criminal finances. *Europol* [online]. 2021 [cit. 1. 1. 2025]. Dostupné z: <https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf>

<sup>5</sup> Virtual currency schemes – a further analysis. *Európska centrálna banka* [online]. S. 4 [cit. 28. 1. 2025]. Dostupné z: <http://ecb.europa.eu>

Virtuálne meny sa odvtedy vyvinuli do rozšíreného spôsobu platby, investícií a prevodu finančných prostriedkov. Zavedenie inovatívneho platobného systému, ktorý umožňuje spoľahlivé, nezvratné transakcie typu end-to-end v reálnom čase a v globálnom meradle, vyvolalo regulačné obavy. Revolučný charakter tohto typu meny neumožňoval okamžitú legislatívnu reakciu. Procesy AML (Anti-Money Laundering) a KYC (Know-Your-Customer) neboli pôvodne navrhnuté tak, aby sa starali o virtuálne meny a kryptomeny. Niektoré novšie právne predpisy v oblasti boja proti praniu špinavých peňazí však začínajú brať do úvahy oblasť kryptomien.

Páchatelia trestnej činnosti, najmä počítačovej kriminality, využili priaznivé prostredie a začali využívať virtuálne meny a špeciálne kryptomeny na účely obchodovania na dark webe a v rámci podvodov či vydieračských schém. Virtuálna mena bola vždy vysledovateľná a nie úplne anonymná. Aby mohli využiť svoje zisky, páchatelia trestnej činnosti začali využívať služby akými sú zmenárne na vyplatenie kryptomien a ich premenu na fiat money („tradičné“ peniaze). Zlepšená regulácia prostredia kryptomien vyžaduje, aby poskytovatelia služieb a platformy zachytávali viac informácií o používateľoch a transakciách, čo zlepšilo reakciu orgánov činných v trestnom konaní na kriminálne používanie kryptomien.<sup>6</sup>

Využívanie virtuálnych mien na trestnú činnosť za posledné roky vzrástlo, pokiaľ ide o objem získaných peňazí a sofistikovanosť páchatel'ov<sup>7</sup>. Nástroje uľahčujúce používanie kryptomien sú v súčasnosti široko dostupné pre celú spoločnosť. V dôsledku toho sa kriminálne používanie kryptomeny už neobmedzuje na činnosti súvisiace s počítačovou kriminalitou, ale vzťahuje sa na všetky druhy kriminality, ktoré si vyžadujú prevod peňazí. Za rok 2021 boli obeť podvodov založených na kryptomenách pripravené po celom svete o viac ako 7,7 miliárd dolárov. V porovnaní s rokom 2020, keď tento typ podvodov oproti roku 2019 výrazne klesol, to predstavuje nárast o 81 % [vplyv globálnych opatrení proti pandémie Covidu mohli ovplyvňovať ekonomické a trhové faktory aj v tejto oblasti a tak skresliť vývojové trendy – pozn. aut.]. Hlavný *modus operandi* spočíval v takzvaných Ponzihových schémach. Tie označujú investičné operácie v kryptomene, ktoré sa však neuskutočnia a investor o svoje peniaze príde.<sup>8</sup>

Súkromný sektor<sup>9</sup> uvádza, že nezákonné používanie kryptomien predstavuje malú časť ich celkového používania, pričom predstavuje 0,34 % transakcií. Na rozdiel od toho, výskum z akademickej obce odhadol oveľa vyšší objem a uvádza, že približne 23 % transakcií je spojených s trestnou činnosťou. Výrazný rozdiel v odhadoch môže byť čiastočne spôsobený rozdielnymi prístupmi a metodikami v transakčnej analýze. Výskum súhlasí s tým, že podiel

<sup>6</sup> Cryptocurrency Enforcement Framework. *US Department of Justice* [online]. 2020 [cit. 1. 1. 2025]. Dostupné z: <https://www.justice.gov/archives/ag/page/file/1326061/download>

<sup>7</sup> KRÁSNA, P. Virtuálna identita a s ňou spojené riziká pri vyšetrovaní. In: ŤAZKÁ, V. (zost.). *Milníky práva v stredo európskom priestore 2024*. 2024, s. 670. ISBN 978-80-7160-723-6. Dostupné z: [https://www.flaw.uniba.sk/fileadmin/praf/Veda/Konferencie\\_a\\_podujatia/Milniky\\_zborniky/Milniky\\_2024.pdf](https://www.flaw.uniba.sk/fileadmin/praf/Veda/Konferencie_a_podujatia/Milniky_zborniky/Milniky_2024.pdf)

<sup>8</sup> The Biggest Threat to Trust in Cryptocurrency: Rug Pulls Put 2021 Cryptocurrency Scam Revenue Close to All-time Highs. *Chainalysis* [online]. 16. 12. 2021 [cit. 1. 1. 2025]. Dostupné z: <https://blog.chainalysis.com/reports/2021-crypto-scam-revenues/>

<sup>9</sup> The 2021 Crypto Crime report. *Chainalysis* [online]. 2021 [cit. 1. 1. 2025]. Dostupné z: <https://go.chainalysis.com/2021-Crypto-Crime-Report.html>

používania kryptomien spojeného s nezákonnými aktivitami v porovnaní s legitímnym používaním sa časom znížil, zatiaľ čo absolútna suma sa naďalej zvyšovala. Nezákonné používanie kryptomien je spojené predovšetkým s účelom prania špinavých peňazí, (online) obchodovania s nezákonným tovarom a službami a podvodmi.<sup>10</sup>

Na účely nasledujúceho textu sa autori rozhodli, že termín kryptoaktíva, virtuálne aktíva a virtuálna mena budú používať ako totožné pojmy, a to z dôvodu, že sa stotožňujú s názorom, že tieto výrazy sú obsahovo takmer identické, resp. vyjadrujúce veľmi obdobné inštitúty, pričom vymedzenie pojmu kryptoaktívum by malo zodpovedať aj termínu virtuálne aktívum, a to v zmysle odporúčania Finančnej akčnej skupiny FATF.

S rastúcou hodnotou bitcoinu na trhu sa čoraz častejšie objavujú aj ich krádeže. V marci 2012 bolo odcudzených 50 tisíc bitcoinov. Hackerom sa podarilo prelomiť ochranu internetového hostingu a bitcoiny previedli do svojich vlastných peňaženiek. Podobne dopadli aj burzy Bitomat, prípadne peňaženka MyBitcoin, kedy zmizla z jej účtu polovica bitcoinov (asi 78 tisíc). V poslednom čase zarezonovala najmä krádež bitcoinov na digitálnej burze Bitfinex, sídliacej v Hongkongu, ktorá musela v dôsledku útokov hackerov zastaviť obchodovanie. Bez stopy zmizli bitcoiny v hodnote 65 miliónov dolárov, v prepočte asi 59 miliónov eur.<sup>11</sup>

Riziká spojené s Bitcoinom sú verejnou otázkou čím ďalej viacej rozoberané. V tomto období dochádza aj k obchodom v rámci tzv. „ilegálneho chodníku“, čo je názov pre ilegálne servery, napr. Silk Road, na ktorom sa predávali drogy a zbrane. Na tento server sa dalo pripojiť iba anonymne a predaj fungoval na báze doporučení a referencií. Pre Silk Road boli bitcoiny ako stvorené – anonymné a ťažko zdaniteľné. A na trhu tak začala rásť hodnota tejto novej meny.

Z hľadiska bezpečnosti sa v súčasnosti považuje prelomenie bezpečnostných prvkov celej bitcoinovej siete za veľmi ťažko realizovateľné. Preto dochádza najčastejšie ku krádeži z nezabezpečeného počítača. Páchateľ napríklad, najprv nainštaluje špeciálny škodlivý software, ktorý mu umožňuje ovládať počítač. Bitcoiny poškodeného si potom štandardnou cestou prevedie do svojej napr. elektronickej peňaženky. K spusteniu poškodzujúceho kódu môže prísť napríklad elektronickou poštou. Možnosti útoku tak zodpovedajú klasickým počítačovým vírusom. K ochrane proti takýmto krádežiam sa používajú okrem štandardnej softwarovej ochrany aj napríklad hardwarová peňaženka s názvom Trezor<sup>12</sup>. Populárnym sa tiež stáva tzv. papierová peňaženka. Tieto „peňaženky“ sa nedajú „hacknut“ a nie je nutné sa spoliehať na bezpečnosť serveru tretej strany atď. Na druhej strane, ale so sebou nesú podobné riziká ako papierové peniaze, t. j. môžu byť fyzicky odcudzené,

<sup>10</sup> Europol spotlight – cryptocurrencies, op. cit.

<sup>11</sup> Ďalšia rana pre Bitcoin. Hackeri ukradli menu za takmer 59 miliónov eur. *Finweb* [online]. [cit. 3. 1. 2025]. Dostupné z: <https://hnonline.sk/finweb/financie-a-burzy/804121-dalsia-rana-pre-bitcoin-hackeri-ukradli-menu-za-takmer-59-milionov-eur>

<sup>12</sup> Ide o malé zariadenie (tzv. hardwarová peňaženka), podobné USB, v ktorom sa skrýva malý jednoúčelový počítač. Trezor zabezpečuje, že pri pokuse odoslať bitcoiny z počítača, ku ktorému je Trezor pripojený, musí dôjsť ešte k fyzickému stlačeniu potvrdzovacieho tlačidla na samotnom zariadení. Trezor tak funguje na princípe, že aj v prípade zasiahnutia počítača pirátskym softwarom, privátne kľúče k adresám sú uložené mimo neho.

zničené ohňom a pod., resp., k získaniu takejto „bankovky“ je potrebné nájsť poskytovateľa papierových peňaženiek. Po zadaní údajov užívateľ na monitore uvidí takúto „bankovku“, ktorá v ľavej časti obsahuje adresu a QR kód, ktorý umožňuje sledovať a prijímať transakcie. V pravej časti súkromný kľúč a QR kód pre odoslanie peňazí z účtu.

Počet detekcií malvéru [počítačového vírusu – pozn. aut.] špeciálne navrhnutého na krádež kryptomien od prvého do druhého polroka 2023 vzrástol o 68 percent. Útočníci však používajú aj iné premyslené podvody, ako napríklad phishingové techniky či investičné podvody. Medzi ďalšie hrozby malvéru zameraného na krádež kryptomien patrí aj crypto drainer. Je to typ malvéru navrhnutý na identifikáciu hodnoty aktív v peňaženkách, používanie škodlivých smart kontraktov na rýchle odčerpanie finančných prostriedkov a následné použitie viacnásobných prevodov na zakrytie stôp.

Malvér na krádež kryptomien sa podľa spoločnosti často skrýva vo falošných aplikáciách (WhatsApp, Telegram).<sup>13</sup>

Útočníci často využívajú aj rôzne phishingové techniky. Používajú sa na to, aby nalákali obeť kliknúť na škodlivé odkazy určené na krádež informácií či finančných prostriedkov z kryptomenových peňaženiek. Prvý kontakt je pritom často iniciovaný prostredníctvom reklám publikovaných podvrhnutými účtami na sociálnych sieťach, ktoré vyzerať legitímne a dôveryhodne.

Pig butchering je zas kombináciou falošného romániku a investičného podvodu. „*Podvodníci na rozoznamkách vytvoria v obetiach falošný pocit bezpečia a potom sa ich snažia presvedčiť, aby investovali do fiktívnych kryptoschém. Niektorí môžu dokonca predstierať, že používateľ na svojej ‚investícii‘ zarába, a až kým sa nepokúsia vybieliť mu finančné prostriedky*“.<sup>14</sup>

Skupiny páchajúce počítačovou kriminalitou sa podľa spoločnosti čoraz častejšie zameriavajú aj na burzu alebo iné legitímne organizácie. **Vyšetrovanie toku finančných prostriedkov pritom sťažuje najmä decentralizovaná povaha virtuálnej meny.**

## 2 Virtuálna mena, kryptoaktívum a blockchain

S kryptomenami je prepojená aj technológia Blockchain, ktorú možno definovať ako transakčnú databázu. Ide o konkrétny typ alebo podskupinu takzvanej technológie distribuovaných záznamov (Distributed ledger technology – DLT). DLT je spôsob zaznamenávania a zdieľania údajov v rámci viacerých dátových záznamov a ich úložísk (známych aj ako „účtovné knihy“), z ktorých každý má presne rovnaké dátové záznamy a sú kolektívne udržiavané a kontrolované distribuovanou sieťou počítačových serverov nazývaných **uzly**. Blockchain je mechanizmus, ktorý využíva metódu šifrovania, známu ako kryptografia a využíva špecifické matematické algoritmy na vytváranie a overovanie neustále rastúcej

<sup>13</sup> Útočníci používajú okrem malvéru aj ďalšie techniky na krádež kryptomien. *TREND.sk* [online]. 16. 6. 2024 [cit. 14. 6. 2025]. Dostupné z: <https://www.trend.sk/spravy/utocnici-pouzivaju-okrem-malveru-aj-dalsie-techniky-kradez-kryptomien>

<sup>14</sup> Ibid.

dátovej štruktúry – do ktorej možno iba pridávať dáta a z ktorej nie je možné odstrániť už existujúce dáta.<sup>15</sup>

**Verejný blockchain** je prístupný každému bez akéhokoľvek schválenia. Neexistuje žiadny centrálny vlastník siete a softvéru a identické kópie účtovnej knihy sú distribuované do všetkých uzlov v sieti. Väčšina kryptomien, ktoré sú v súčasnosti v obehu, vrátane Bitcoinu, je založená na verejných blockchainoch bez povolenia. Povolený blockchain je koordinovaný centrálnou entitou a overovatelia transakcií (t. j. uzly) musia byť vopred schválení, aby sa mohli pripojiť k sieti. Tento typ blockchainu môže byť aj verejný, čo umožňuje komukoľvek zobraziť účtovnú knihu, ktorú môžu aktualizovať iba oprávnení účastníci.<sup>16</sup>

**Kryptomenová peňaženka** je aplikácia, ktorá sa používa na držanie, ukladanie a prevod virtuálnych mien. Obsahuje kryptografické kľúče používateľa tej-ktorej virtuálnej meny. Poskytovateľ peňaženky zvyčajne prekladá históriu transakcií používateľa kryptomeny do ľahko čitateľného formátu, ktorý vyzerá podobne ako bežný výpis z bankového účtu. Kryptomenové peňaženky sa delia na hardvérové (poskytujú používateľom virtuálnych mien špecifické hardvérové riešenia na súkromné ukladanie ich kryptografických kľúčov) a softvérové (poskytujú používateľom virtuálnych mien softvérové aplikácie, ktoré im umožňujú prístup k sieti, odosielanie a prijímanie virtuálnych mien a lokálne ukladanie ich kryptografických kľúčov).

S virtuálnymi menami je ďalej spojená aj kryptomenová burza, resp. zmenáreň, ktorá slúži na výmenu kryptomien. Ide o osoby alebo subjekty, ktoré ponúkajú zmenárenské služby používateľom kryptomien, zvyčajne za zapltenie určitého poplatku (t. j. provízie). Umožňujú používateľom kryptomien predávať svoje virtuálne meny za fiat meny alebo nakupovať nové virtuálne meny za fiat menu. Medzi takéto burzy patria napr. Bitfinex91, HitBTC92, Kraken93 a Coinbase GDAX a i. Je dôležité poznamenať, že niektoré burzy sú čisté kryptomenové burzy čo znamená, že prijímajú platby iba v iných kryptomenách, zvyčajne v bitcoíne (napríklad Binance96), zatiaľ čo iné prijímajú aj platby vo fiat menách, ako je americký dolár alebo euro (napr. Coinbase).

Okrem toho mnohé burzy kryptomien umožňujú svojim používateľom nakupovať iba určitý typ mien. Treba tiež poznamenať, že mnohé burzy s kryptomenami (t. j. bežné aj čisté burzy s kryptomenami) fungujú ako správcovia peňaženiek (napríklad Bitfinex). Kryptomenové burzy vo všeobecnosti ponúkajú svojim používateľom širokú škálu platobných možností, ako sú bankové prevody, prevody cez PayPal, kreditné karty a i. Niektoré burzy s kryptomenami tiež poskytujú štatistiky o trhu s kryptomenami (ako sú objemy obchodov a volatilita obchodovaných mincí) a ponúkajú konverzné služby obchodníkom, ktorí prijímajú platby v kryptomenách.

Pre úplnosť, na tomto mieste uvádzame, že právny poriadok Slovenskej republiky rozlišuje už iba pojem **kryptaktívum**. Podľa § 131 ods. 6 Trestného zákona platobným prostriedkom

<sup>15</sup> Cryptocurrencies and blockchain – Legal context and implications for financial crime, money laundering and tax evasion. *Európsky parlament* [online]. [cit. 1. 1. 2025]. Dostupné z: <https://op.europa.eu/en/publication-detail/-/publication/631f847c-b4aa-11e8-99ec-01aa75ed71a1>

<sup>16</sup> Ibid.

sa na účely tohto zákona rozumie nehmotné alebo hmotné chránené zariadenie, predmet, záznam alebo ich kombinácia vrátane platobnej karty, ktorá je chránená pred falšovaním alebo neoprávneným použitím a ktorá držiteľovi alebo používateľovi sama alebo spolu s nejakým postupom alebo súborom postupov umožňuje prevod peňazí, elektronických peňazí alebo kryptoaktív. **Kryptoaktívum** máme definované v článku 3 ods. 1 bode 5 nariadenia (EÚ) 2023/1114 ako digitálne vyjadrenie hodnoty alebo práva, ktoré možno prevádzať a elektronicky uchovávať použitím technológie distribuovanej databázy transakcií alebo podobnej technológie. Táto definícia je záväzná pre všetky štáty EÚ.

V zmysle dôvodovej správy k zákonu č. 312/2020 Z.z., **virtuálne meny** (napr. Bitcoin, Litecoin, Ethereum, IOTA, Ripple, Stellar a i.) **nie sú v Slovenskej republike uznané ako oficiálna tuzemská či zahraničná mena, nepredstavujú elektronické peniaze v zmysle zákona o platobných službách a nemajú ani fyzickú protihodnotu vo forme zákonného platidla.**<sup>17</sup> Zákonodarca v dôvodovej správe vymenúva len kryptomeny, pričom virtuálnou menou môže byť v zmysle medzinárodného ponímania aj mena, ktorú je možné použiť len v uzavretom virtuálnom systéme.

S kryptoaktívami sa stretávame v zákone 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, kde máme nové ustanovenie 24a) ktoré upravuje poskytovateľov služieb kryptoaktív a vychádza z aktuálnej európskej právnej úpravy a jej regulačného právneho rámca. Na základe uvedeného môžeme uviesť, že pojem **kryptoaktívum v práve EÚ nahradil pojem virtuálna mena a tento vývoj boli povinné v národnom právnom rámci zaznamenať a upraviť aj jednotlivé členské štáty EÚ.** Trajektória bádania autorov v tomto smere vedie k vyjadreniu pozitívneho ohlasu na margo nariadenia MiCA, ktoré so sebou prinieslo všeobecný termín „kryptoaktíva“, pod ktorý sú radené viaceré druhy tokenov (elektronické peňažné tokony – stablecoiny), tokeny viazané na aktíva a ostatné virtuálne meny a kryptomeny, ktorými sú napríklad Bitcoin. Autori vyjadrujú v tomto smere nádej, že zovšeobecnenie pojmológie v tomto smere prinesie jednotnosť používania označenia do budúcnosti vo všetkých členských krajinách Európskej únie a ich právnych poriadkoch.

### 3 Trestnoprávna úprava virtuálnych mien v Českej republike

Názov virtuálna mena by mohla u značnej skupiny ľudí navodiť domnienku, že ide o medzinárodne uznávanú menu existujúcu však vo virtuálnom prostredí. S ohľadom na skutočný význam virtuálnych mien, je takýto názov zavádzajúci. Najrozšírenejšou a najznámejšou virtuálnou menou je Bitcoin, ktorý rovnako nie je menou v pravom slova zmysle, a to z dôvodu, že mena ako taká je štátom stanovený druh platidla, ktorý je na danom území používaný na účely platobného styku. Zároveň platí, že **mena je chránená priamo zákonom a ďalšími právnymi predpismi, nielen na národnej úrovni.** V kontexte trestného práva vieme, že mena a bezproblémový obeh platobných prostriedkov sú chránené v českom Trestnom zákone prostredníctvom niekoľkých skutkových podstát trestných činov

<sup>17</sup> Dôvodová správa k zákonu č. 312/2020 Z.z. Dostupné z: <https://www.nrsr.sk/web/Dynamic/DocumentPreview.aspx?DocID=482301> [cit. 1. 1. 2025].

v šiestej hlave Zvláštnej časti Trestného zákonníku. V tomto smere preto platí, že virtuálna mena kvôli absencii takejto základnej požiadavky nespĺňa atribút na to, aby *de iure* išlo o menu, aj keď prostredníctvom nej môžu byť napĺňané niektoré základné funkcie meny. Už z uvedeného je zrejmé, že všetko previazané s virtuálnymi menami prináša nové výzvy, a to nie len pre českú právnu úpravu a pre českého zákonodarcu, ale pre celý svet. Preto možno skonštatovať, že v súčasnosti už nie je možné, aby finančné inštitúcie nepovažovali virtuálne meny za peňažný prostriedok či investičný nástroj.

Právne otázky spojené s virtuálnymi menami boli v poslednom období diskutované najmä v zahraničnej literatúre<sup>18</sup> a v niekoľkých záverečných prácach<sup>19</sup>. Legálna definícia **virtuálnej meny** bola prvýkrát do českého právneho poriadku zavedená novelou zákona č. 368/2016 Sb., ktorým sa menil zákon č. 253/2008 Sb. o niektorých opatreniach proti legalizácii výnosů z trestné činnosti a financování terorismu (ďalej „AML zákon“), účinná od 1. 1. 2017. V súčasnosti však v § 4 ods. 8 predmetného zákona obsahuje definíciu virtuálnej meny, ktorá bola novelizovaná na podklade Nariadenia Európskeho parlamentu a Rady (EU) 2023/1114, zo dňa 31. 5. 2023 o trhoch kryptoaktív a o zmene nariadenia (EU) č. 1093/2010 a (EU) č. 1095/2010 a smerníc 2013/36/EU a (EU) 2019/1937, v platnom znení:

*„Virtuálním aktívom se pro účely tohoto zákona rozumí kryptoaktivum podle přímo použitelného předpisu Evropské unie upravujícího trhy kryptoaktív s výjimkou*

- a) *kryptoaktiva podle čl. 2 odst. 4 nařízení Evropského parlamentu a Rady (EU) 2023/1114 a*
- b) *kryptoaktiva, které je jedinečné, není zastupitelné jiným kryptoaktivem a nelze jej využít pro platbu nebo investici.“* V tomto smere je potrebné zmieniť, že **nové označenie virtuálne aktívum nahrádza predchádzajúci pojem virtuálna mena** a podľa novelizovaného AML zákona je ním „uchovateľná a prevoditeľná jednotka“, ktorá musí spĺňať funkciu platobnú, výmennú a investičnú, pričom nie je rozhodujúca, či bola vydaná emitentom alebo nie. V zmysle dôvodovej správy k zákonu č. 527/2020 Sb., ktorý túto definíciu a terminologickú zmenu vykonal, bolo dôvodom tejto zmeny najmä rozšírenie okruhu prípadov „kedy je potlačená jej platobná funkcia a naopak, je zdôraznená funkcia investičná, ako je tomu v prípade rôznych inštrumentov, ktoré sa podobajú cenným papierom.“<sup>20</sup>

Odseky 9 a 10 § 4 rovnako súvisia s virtuálnym aktívom, resp. so **službou spojenou s virtuálnym aktívom**, ktorou sa rozumie: „*pro účely tohoto zákona rozumí služba související s kryptoaktívny podle přímo použitelného předpisu Evropské unie upravujícího trhy kryptoaktív s výjimkou služby*

<sup>18</sup> Napr. LASTOWKA, G. F., HUNTER, D. The Laws of Virtual Worlds. *California Law Review*. 2004, roč. 92, č. 1, s. 36–37.

<sup>19</sup> BULINSKÝ, V. *Kryptoměny v právním řádu České republiky*. Diplomová práce. Brno. Masarykova univerzita, 2024; PAVELKA, P. *Kryptoměna jako potenciální nástroj legalizace výnosů z trestné činnosti*. Diplomová práce. Policiální akademie České republiky.

<sup>20</sup> Důvodová zpráva k zákonu č. 527/2020 Sb. kterým se mění zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů.

*poskytování poradenství týkajícího se kryptoaktiv podle přímo použitelného předpisu Evropské unie upravujícího trhy kryptoaktiv.*<sup>21</sup>

A posledným previazaným termínom je **osoba poskytujúca služby spojené s virtuálnym aktívom**, ktorou sa na účely daného zákona rozumie: „osoba alebo svěřenský fond, které jsou oprávněny poskytovat službu spojenou s virtuálním aktivem, jiní než poskytovatel služeb souvisejících s kryptoaktivy podle přímo použitelného předpisu Evropské unie upravujícího trhy kryptoaktiv.“<sup>22</sup>

V neposlednom rade doplníme, že uvedený zákon má vyriešenú aj otázku kontroly povinností stanovených týmto zákonom, ak sa jedná o kryptoaktiva, a to cez Finančný analytický úrad Českej republiky. Na podklade uvedeného je teda možné skonštatovať, že kryptoaktívum ako virtuálna mena má legálnu definíciu priamo v zákone o ochrane pred legalizáciou z trestnej činnosti a podlieha minimálne ochrane na úrovni Finančného analytického úradu, ktorý prípadné porušenia hlási Českej národnej banke, teda neplatí, že by neboli regulované ani dozorované žiadnym príslušným orgánom verejnej moci.

Na tomto mieste je tiež nevyhnutné upriamiť pozornosť na veľmi aktuálnu skutočnosť, ktorá sa udiala v Českej republike, a síce, prijatie zákona o implementácii predpisov Európskej únie v oblasti digitalizácie finančného trhu (ďalej „Zákon o digitalizácii finančného trhu“), ktorý bol schválený poslaneckou sněmovňou 6. 12. 2024 a následne dňa 22. 1. 2025 schválený Senátom parlamentu Českej republiky.<sup>23</sup> „Návrh zákona obsahuje především úpravu kategorizace přestupků a také pravomocí České národní banky, která bude licencovat poskytovatele služeb souvisejících s kryptoaktivy, dohlížet na dodržování stanovených povinností a řešit jejich případná porušení. Některá další ustanovení reagují na nařízení MiCA a jejich cílem je hladká aplikace nařízení v České republice, například zvláštní režim rezervy aktiv vydavatelů tokenů vázaných na aktiva či elektronických peněžních tokenů.“<sup>24</sup> Teda, na trh s kryptoaktívami bude od účinnosti predmetného zákona dohliadať Česká národná banka. Uvedené je možné rozhodne považovať za pozitívny krok vpred na strane Českej republiky, nakoľko samotné Európske nariadenie MiCA predstavuje prvý komplexný predpis upravujúci možné ponuky kryptoaktív verejnosti a poskytovanie s tým súvisiacich služieb. Nariadenie nastavuje pravidlá na ochranu spotrebiteľa. Nariadenie DORA zjednocuje pravidlá digitálnej prevádzkovej odolnosti finančného sektora, ktoré sú aktuálne roztrieštené v rôznych európskych sektorových predpisoch, konkrétne v smerniciach a nariadeniach.

Od virtuálnych mien je potrebné odlišovať **elektronické peniaze**, a to aj napriek tomu, že tieto dva názvy značne splyvajú. Definíciu elektronických peňazí v českej právnej úprave nájdeme v zákone č. 284/2009 Sb. o platebním styku v znení pozdějších predpisu (ďalej „ZPS“), ktorý stanovuje, že elektronické peniaze sú v podstate elektronicky uchovávané

<sup>21</sup> § 4 ods. 9 Zákona č. 253/2008 Sb. o některých opatřeních proti legalizaci výnosů z trestné činnosti.

<sup>22</sup> § 4 ods. 10 Zákona č. 253/2008 Sb. o některých opatřeních proti legalizaci výnosů z trestné činnosti.

<sup>23</sup> 92. uznesením Senátu z 5. schůzde konanej dňa 22. 1. 2025 k návrhu zákona, kterým se mění některé zákony v souvislosti s implementací předpisů Evropské unie v oblasti digitalizace finančního trhu a financování udržitelosti /senátní tisk č. 31/ senát schvaluje návrh zákona v znení postúpenom Poslaneckou sněmovňou. Dostupné z: <https://www.senat.cz/xqw/xervlet/psssenat/historie?action=detail&value=5375> [cit. 27. 1. 2025].

<sup>24</sup> Dostupné z: <https://www.mfcr.cz/cs/ministerstvo/media/tiskove-zpravy/2024/zakon-o-digitalnich-finan-cich-schvalen-poslaneckou-57514> [cit. 27. 1. 2025].

pohľadávka, ktorá je vydaná proti prijatiu peňažných prostriedkov, a je prijímaná niekým iným, než osobou, ktorá ju vydala. Po nahliadnutí hlbšie do predmetného zákona sme zistili, že virtuálna mena nespĺňa hneď dve požiadavky, ktoré sú kladené na elektronické peniaze, a to konkrétne v § 4 ods. 1 písm. a) – „*virtuálna mena nepredstavuje pohľadávku voči inému vydávateľovi*“ a v § 4 ods. 1 písm. c) „*virtuálna mena nie je vydávaná proti prijímaniu peňažných prostriedkov*“.

Zaujímavý je pohľad Krajského súdu v Brne, ktorý sa v správnom súdnictve zaoberal právnu povahou Bitcoinov. Krajský súd v Brne<sup>25</sup> totiž na adresu Bitcoinov uviedol, že: „*jde o virtuální neregulovanou měnu, která nespadá pod regulaci a dohled žádné centrální banky na světě. To je i její hlavním principem, který ji odlišuje od tradičních měn emitovaných centrálními bankami. Bitcoin tedy nelze považovat za bankovku a ani minci. Pokud jde o bezhotovostní platební styk, tak bitcoin nepředstavuje pohledávku vůči tomu, kdo ji vydal. Primárně vůbec nejde o pohledávku. Proto bitcoiny nepředstavují bezhotovostní peněžní prostředky ani elektronické peníze.*“ V danom správnom súdnictve síce nešlo o trestnoprávnu problematiku, ale o konanie vo veci správy daní, resp. daní z príjmov fyzických osôb. Čo je však aplikovateľné aj v trestnom práve je tá skutočnosť, ktorú uviedol Krajský súd, a síce, že: „*Bitcoin je měnou virtuální, která nemá ekvivalent v podobě hotovostních peněz. Bitcoiny proto nepředstavují peníze, protože nejsou tradičními penězi existujícími v hotovostní podobě. Bitcoin není proto ‚cizí měna‘, protože cizí měnou jsou myšleny pouze peníze emitované zahraničními centrálními bankami, jejichž oběh je těmito bankami regulován a je uzákoněn na území určitého státu nebo skupiny států. Cizí měnou je tedy jen měna, na kterou se vztahují v zahraničí obdobné pravidla jako na tuzemskou měnu.*“<sup>26</sup> Z uvedeného abstrahujeme, že na virtuálne meny nazeráme ako na veci. V tomto smere, autorov príspevku problematika virtuálnych aktív a jej nekonvenčnosť odkázala na hľadanie iných právnych rámcov tohto pojmu. Zhodu našli v zákone č. 89/2012 Sb. Občanský zákonník, konkrétne v ustanovení § 489, ktorý uvádza, nasledovne: „*Věc v právním smyslu (dále jen ‚věc‘) je vše, co je rozdílné od osoby a slouží potřebě lidí.*“ Na základe takto široko posadenej definície je možné nájsť zhodu s vlastnosťami virtuálnych aktív, ktoré rovnako ako veci sú rozdielne od osôb a slúžia potrebám ľudí. Na druhej strane, je možné ich zneužívať na páchanie trestnej činnosti, a to v rôznych obmenách. Záverom je teda možné uznieť sa, že **virtuálne aktíva sú vecou v právnom slova zmysle.**

Vyššie v texte autori vymedzili základné definičné princípy a kritéria virtuálnych mien v Českej republike. V nasledujúcej časti textu nasmerujú pohľad na trestnoprávnu rovinu virtuálnych aktív. Ešte predtým je však potrebné zmieniť sa o fakte, že virtuálne meny u našich západných susedov sú skôr skúmané v rovine kriminologickej, ktorá sa zaoberá kybernetickou kriminalitou, ako v rovine trestnoprávnej. Napriek tejto skutočnosti však Polícia Českej republiky nedisponuje fenomenologickými ukazovateľmi, ktoré by vierohodne preukázali stav, štruktúru a dynamiku trestnej činnosti okolo virtuálnych aktív a jednotlivých útokov súvisiacich s virtuálnymi menami. Pod pojmom „kyberkriminalita“ je subsumovaná všetka trestná činnosť spojená s internetom a jeho virtuálnym vyjadrením. V tomto smere platí, že zatiaľ neexistuje nástroj k vykázaní nárastu nových trestných činov spojených s kryptoaktívami. Na druhej strane je v Českej republike regulácia virtuálnych aktív primárne sústredená

<sup>25</sup> Rozsudek Krajského soudu v Brně ze dne 24. 3. 2022, sp. zn. 30 Af 41/2020.

<sup>26</sup> Ibid.

aj v rámci zákona č. 181/2014 Sb. o kybernetické bezpečnosti, ktorý sa týka bezpečnosti digitálnych aktív a zabezpečenia kryptomien pred hackermi, či kybernetickými útokmi.

V tomto smere však autori príspevku v zmysle zákona č. 106/1999 Sb. o svobodnom prístupe k informáciám v platnom znení, dotazovali český Úrad pre zastupovanie štátu vo veciach majetkových (ďalej „ÚZŠVM“), v zmysle ktorého im bola dňa 10. 2. 2025 doručená odpoveď, že tento úrad síce virtuálne meny nezaistuje, nakoľko tento úkon spadá do kompetencie Polície Českej republiky, najmä Národnej centrály proti organizovanému zločinu, avšak v niektorých prípadoch, keď sa jedná o zaistený majetok potom tento úrad vykonáva správu tohto majetku. V prípade, že sa virtuálne meny prepadnú štátu na základe právoplatného rozhodnutia súdu, tento úrad ich následne ponúka v transparentných výberových konaniach s elektronickou akciou na webových stránkach [nabidkamajetku.gov.cz](http://nabidkamajetku.gov.cz). Zároveň v danej odpovedi na dotaz bola informácia, že historicky prvá elektronická aukcia virtuálnych mien prebehla v roku 2021 a v roku 2024 patrila aukcia virtuálnych mien k najúspešnejším v rámci hnutel'ného majetku. ÚZŠVM predal v elektronickej aukcii päť jednotiek virtuálnej meny bitcoin, ktoré štát získal na základe trestov udelených organizovanej skupine za distribúciu drog, pričom výsledná čiastka bola 8 098 000 českých korún. V priebehu roku 2024 sa uskutočnilo 20 elektronických aukcií virtuálnej meny bitcoin, pričom v nich štát získal viac ako 167 miliónov korún. Príjmy z predaja virtuálnych mien ÚZŠVM odvádza do štátneho rozpočtu, v niektorých prípadoch je potom finančná čiastka odvedená na špeciálny účet Ministerstva spravodlivosti na pomoc obetiam trestných činov.

V rámci verejnoprávnej úpravy a postavenia virtuálnych aktív majú autori za to, že je nanajvyššie vhodné vyjadriť sa k tzv. protipólu ochrany virtuálnych aktív, a to k **ochrane meny**, ako takej. Každá krajina, Česká republika nevynímajúc, má svoje zákonné tuzemské platidlo. Ochrana tuzemskej meny je spojená so zákonnou povinnosťou takúto menu, resp. jej mince a bankovky prijímať v zmysle osobitných právnych predpisov (v kontexte právnej úpravy Českej republiky v zmysle zákona č. 136/2011 Sb. o obehu bankoviek a mincí). V prípade porušenia takejto povinnosti, teda napríklad pri odmietnutí prijatia českej koruny, resp. mincí pri akejkoľvek úhrade, sa páchatel' môže dopustiť trestného činu ohrozovania obehu tuzemských peňazí v zmysle § 239 českého Trestného zákona. Teda, v spojení s virtuálnymi menami by uvedené protiprávne konanie naplnila taká situácia, kedy by osoba napríklad v obchode odmietla prijať platbu v českých korunách alebo v eurách a požadovala by plnenie iba napr. v Bitcoinoch. Platba kryptomenami totižto môže slúžiť iba ako akási doplnková, resp. alternatívna, vedľa platby v zákonnej mene. Na tomto mieste ďalej konštatujeme, že používanie kryptomien býva spájané s vykonávaním platieb cez internet, ktoré smeruje k získaniu prístupu napr. k detskej pornografii alebo k nákupu nezákonného tovaru v podobe drog či zbraní.<sup>27</sup>

Aplikácia trestného práva voči virtuálnym aktívam nie je samostatne vymedzená, resp. v zákone č. 141/1961 Sb. o trestním řízení soudním (ďalej „Trestní řád“ alebo „český Trestný poriadok“) neexistujú inštitúty, ktoré by ju akýmkoľvek spôsobom upravovali, resp. postihovali. O niečo iná situácia je prítomná v rámci zákona č. 40/2009 Sb. Trestní

<sup>27</sup> NÁHLLOVSKÁ, L. Trestněprávní aspekty virtuálních měn. *Bulletin Advokacie* [online]. 1.3.2018 [cit. 28. 1. 2025]. Dostupné z: <http://www.bulletin-advokacie.cz/clanky/?browser=full&strana=22>

zákonník (ďalej „Trestní zákoník“ alebo „český Trestný zákon“), nakoľko v jeho ustanovení § 234 sa nachádza skutková podstata trestného činu „*Neoprávněné opatření, padělání a pozměnění platebního prostředku*“, pričom v jej základnej skutkovej podstate zákonodarca trestnoprávne postihuje osobu, ktorá *sebe, alebo inému bez súhlasu oprávněného uživateľa opatří, sprístupní, přijme alebo prechováva platobný prostředek, který umožňuje výber hotovosti alebo převod peňažných prostředkov alebo virtuálních aktív používaných namiesto peňažných prostředkov a který patří inému, a to trestom odňatia slobody až na dva roky, zákazom činnosti alebo prepadením majetku*. V zmysle uvedeného je teda možné vyvodit', že český zákonodarca umožňuje vo vzťahu k neoprávněnému užívateľovi virtuálnych aktív používaných namiesto peňažných prostriedkov aplikovať nielen trest odňatia slobody, ale aj trest zákazu činnosti alebo trest prepadenia majetku. Na druhej strane je nutné skonštatovať, že uvedená skutková podstata nepostihuje priamo virtuálne prostredie a jeho prípadné protiprávne aspekty súvisiace s virtuálnymi aktívami. Uvedenú právnu úpravu preto hodnotíme ako nedostatočnú.

V tomto smere je ešte nutné upozorniť na jednu skutočnosť, a síce, že v českom Trestnom zákone nie je nikde vymedzený termín ktorý vyššie zmienená skutková podstata trestného činu používa. V teórii trestného práva takúto skutkovú podstatu odkazujúcu na právny predpis netrestnej povahy, nazývame ako tzv. **blanketová skutková podstata**. Uvedené vychádza zo skutočnosti, že termín virtuálne aktíva je termínom zafinovaným v rámci zákona o AML, ktorý uvádzame vyššie v texte.

V tomto smere je preto potrebné upriamiť pozornosť aj na fakt, že virtuálne aktíva sú súčasťou kriminálnej trestnej činnosti. Podľa vzoru Smejkal, je možné rozdeliť ich na dve kategórie. *Prvou kategóriou* je klasická kriminalita, v ktorej virtuálne aktíva hrajú iba úlohu určitého nástroja na spáchanie a *druhou kategóriou* je kryptomenová kriminalita.<sup>28</sup> Do oblasti klasickej kriminality je možné zaradiť prípad z Českej republiky, kedy páchatel' bol trestne stíhaný za obzvlášť závažný zločin nedovolennej výroby a iného nakladania s omamnými a psychotropnými látkami a jedmi v zmysle § 283 ods. 1, ods. 4 písm. b) českého Trestného zákona a obzvlášť závažný zločin krádeže podľa § 205 ods. 1, ods. 5 českého Trestného zákona, a to na tom skutkovom základe, že prevádzkoval internetový obchod, ktorý vytvoril za účelom sprostredkovania predaja rôzneho tovaru či služieb, predovšetkým však návykových látok, pričom za sprostredkovanie jednotlivých platieb v tomto internetovom obchode získaval provízie v podobe digitálnej meny bitcoin. Za sprostredkovanie jednotlivých obchodov s návykovými látkami obvinený získal takmer 1200 bitcoinov, čo v čase jednotlivých obchodov zodpovedalo čiastke najmenej 250 000 €. Okrem toho odcudzil svojim zákazníkom aj ďalšie bitcoiny, v celkovej hodnote presahujúcej pol milióna eur, a to na základe prístupu k digitálnej peňaženke celého obchodu. Za protiprávne konanie bol páchatel' odsúdený českými súdmi k úhrnnému nepodmienečnému trestu odňatia slobody vo výške deväť rokov.<sup>29</sup>

Ničím nevídaným nie je ani nakupovanie drog prostredníctvom siete Darknet, zaplatených Bitcoinami. S uvedeným má Česká republika vlastnú skúsenosť, nakoľko Najvyšší súd ČR rozhodoval prípad, kde si obvinený objednal amfetamín prostredníctvom internetového

<sup>28</sup> SMEJKAL, V. *Kybernetická kriminalita*. 3. vyd. Plzeň: Aleš Čeněk, 2022, s. 960. ISBN 978-80-7380-849-5.

<sup>29</sup> Usnesení Ústavního soudu ČR ze dne 31. 1. 2017, sp. zn. IV. ÚS 3864/16-1.

„trhoviska“ Silk Road, zaplatil zaň Bitcoinami a odhalený bol iba vďaka tomu, že balíček zastavila colná služba. Množstvo drog v balíčku nebolo nijako veľké, preto Obvodný súd pre Prahu 6 aj Mestský súd v Praze obžalobu neprejednali, ale postúpili Úradu mestskej časti Praha 6 na prejednanie veci ako priestupku s odôvodnením, že množstvo látky v balíčku nebolo menšie než malé. Najvyšší súd ČR však s touto argumentáciou nesúhlasil, naopak zdôraznil, že: „*jednání obviněného rozhodně nelze bagatelizovat, neboť zapadá do širšího rámce nových trendů v rozvoji nelegálního obchodu s drogami, který se projevuje i v mezinárodním měřítku.*“<sup>30</sup>

### 3.1 Zaistenie virtuálnych aktív (kryptoaktív) v Českej republike na účely trestného konania

Novelizáciou českého Trestného poriadku prostredníctvom zákona č. 55/2017 Sb., ktorá nadobudla účinnosť dňa 18. 3. 2017, bola nanovo definovaná **vec dôležitá pre trestné konania**, ktorou sa na účely § 77b ods. 1 rozumie vec, ktorá: a) môže slúžiť na dôkazné účely, b) bola nástrojom trestnej činnosti, c) bola výnosom z trestnej činnosti, d) alebo je náhradnou hodnotou za vec uvedenú v predchádzajúcich alternatívach. Predmetnou novelizáciou došlo k systematickému rozlišovaniu režimu predloženia a zaistenia vecí slúžiacich na dôkazné účely a režimom zaistenia vecí, ktoré sú nástrojmi, resp. výnosmi z trestnej činnosti. Autori predkladaného textu nasledujúce riadky venujú práve trestno-procesnému inštitútu **zaistenia vecí, ktoré sú nástrojom, resp. výnosom z trestnej činnosti**. Uvedený inštitút pomáha objasňovaniu a reparácii trestnej činnosti, ktorého základnou podstatou nie je zhabanie majetku, resp. jeho konfiškácia ale iba obmedzenie s jeho nakladaním. Teda, ide síce o zásah do vlastníckeho práva, ktorý však pri dodržaní všetkých zákonom stanovených podmienok je primeraný cieľu sledovanému zákonom, teda náležitému objasneniu trestnej činnosti a náprave škody spôsobenej takou trestnou činnosťou.<sup>31</sup>

Čo sa týka procesnoprávnych aspektov virtuálnych mien, resp. možnosti ich zaistenia na účely trestného konania, v prvom rade je nutné uviesť, že virtuálna mena, vyplývajúca z predchádzajúceho textu nie je hmotnou menou, ale nehmotnou vecou. Rovnako platí, že český Trestný poriadok neobsahuje, na rozdiel od slovenského Trestného poriadku, konkrétne ustanovenia, ktoré by sa špeciálne venovali iba zaistovaniu virtuálnych aktív. V tomto smere preto autori konštatujú, že virtuálne aktívum zaistené podľa § 79a českého Trestného poriadku, v zmysle ktorého, ak zistené skutočnosti nasvedčujú tomu, že určitá vec je **nástrojom** alebo **výnosom z trestnej činnosti**, môže predseda senátu a v prípravnom konaní štátny zástupca, resp. policajný orgán rozhodnúť o zaistení takejto veci. Policajný orgán k takémuto rozhodnutiu potrebuje predchádzajúci súhlas štátneho zástupcu. Tento predchádzajúci súhlas štátneho zástupcu nie je potrebný iba v naliehavých prípadoch, ktoré neznesú odklad. Policajný orgán je v takom prípade povinný do 48 hodín svoju rozhodnutie predložiť štátnemu zástupcovi, ktorý s ním buď vysloví súhlas alebo ho zruší. Proti takémuto rozhodnutiu o zaistení je prípustná sťažnosť.

<sup>30</sup> Usnesení Nejvyššího soudu ČR ze dne 20. 11. 2014, sp. zn. 7 Tdo 1307/2014.

<sup>31</sup> Nález Ústavního soudu ČR ze dne 19. 3. 2009, sp. zn. III. ÚS 1396/07.

Teda prvotnou podmienkou na zaistenie virtuálnych aktív v Českej republike je, aby zistené skutočnosti nasvedčovali tomu, že určitá vec, v danom prípade virtuálne aktíva sú nástrojom alebo výnosom z trestnej činnosti. Aby bolo možné dospieť k záveru, že virtuálne aktívum je nástrojom, resp. výnosom z trestnej činnosti a pristúpiť k zaist'ovacím úkonom, musí byť splnený akýsi **vyšší stupeň pravdepodobnosti, že virtuálne aktívum skutočne je nástrojom, resp. výnosom z trestnej činnosti**. *Argumentum a contrario* teda platí, že nie je potrebné, aby skutočnosť, že virtuálne aktívum je výnosom z trestnej činnosti bola preukázaná, postačí aj záver o vyššom stupni pravdepodobnosti, že tomu tak je. Tento záver, samozrejme, musí byť dostatočne odôvodnený konkrétnymi skutočnosťami. *In genere*, nestačia iba všeobecné podozrenia. *In concreto*, medzi takéto podklady môžeme zaradiť, napríklad údaje uvedené v trestných oznámeniach, v podaných vysvetleniach, či v ďalších písomnostiach obsiahnutých v spise. S ohľadom na skutočnosť, že v danom prípade dochádza k zásahu do ústavne garantovaných práv osôb, je ďalšou nevyhnutnou podmienkou k možnosti využitia inštitútu zaistenia **podmienka primeranosti**, v zmysle ktorej musí existovať rozumný a opodstatnený vzťah proporcionality medzi použitými prostriedkami, teda použitými zaist'ovacími úkonmi trestného konania a sledovanými cieľmi. Oprávnenosť postupu orgánov činných v trestnom konaní by následne mala byť posudzovaná už iba v rámci trestného konania, a to tak, aby v prípade pochybenia mohli orgány činné v trestnom konaní vykonať nápravu na tejto úrovni.<sup>32</sup> V tejto podmienke vidíme aj odzrkadlenie výzvy, ktorú smerovala Európska únia členským štátom, aby poskytli vyšetrovacím orgánom väčšiu právomoc, ktorá by im umožnila odhaľovať páchatel'ov ktorí využívajú kryptomeny a virtuálne meny na páchanie trestnej činnosti na internete, špeciálne sa týkajúc prania špinavých peňazí, resp. legalizácie výnosov z trestnej činnosti.<sup>33</sup>

V kontexte s legálnym nástrojom na zaistenie nástrojov a výnosov z trestnej činnosti, vyvstáva do popredia otázka, ako je technicky možné zaistiť napríklad účet obsahujúci virtuálne meny. Pre nakladanie s virtuálnymi aktívami sa používajú tzv. kryptopeňaženky, o ktorých sme hovorili na začiatku textu. Vlastniť kryptopeňaženku znamená vlastniť jedinečný súkromný kľúč, ktorým môžete odomknúť konkrétnu, napr. bitcoinovú verejnú adresu. Tento kľúč je jediný spôsob ako disponovať s bitcoinami na danej adrese. Akékoľvek transakcie teda môže realizovať iba ten, kto má prístupové kľúče k účtom vedeným v bitcoinoch, či v kryptopeňaženke, v ktorej má užívateľ uložený svoj súkromný kľúč, ktorým kryptograficky podpisuje bitcoinové transakcie, tzv. recovery kľúč (SEED). V prvom rade je potrebné uviesť, že súkromný kľúč (SEED) má vlastníč účtu alebo ním poverená osoba a pokiaľ nechce alebo nemôže kľúč prezradiť, či ho dokonca stratí a nemá k dispozícii SEED, stane sa obsah účtu neprístupný a žiadne úradné rozhodnutie túto skutočnosť nezvráti. V tejto súvislosti upriamime pozornosť aj na odlišnú situáciu, v prípade zaist'ovania klasických mien a kryptomien. Ak dôjde k zaisteniu finančných prostriedkov na účte, majiteľ účtu nemôže s týmto disponovať, konkrétne vyberať hotovosť, vydávať príkazy na prevod či akékoľvek ďalšie dispozície. Pri kryptomenách je situácia iná. Účet je anonymný, rovnako sú anonymné aj informácie

<sup>32</sup> Nález Ústavného soudu ČR ze dne 19. 3. 2009, sp. III. ÚS 1396/07.

<sup>33</sup> Dostupné z: <https://www.itpro.com/public-sector/21903/europol-calls-for-greater-bitcoin-policing-powers> [cit. 27. 1. 2025].

o transakciách, ktoré boli prevedené. Skrátka, pri kryptomenách nezistíme kto bol príjemca čiastky odoslanej z kryptopeňaženky, pokiaľ k samotnej kryptopeňaženke nemáme prístup. V tomto smere máme za to, že v rámci právnej úpravy *de lege lata* nie je v rámci trestného konania v Českej republike jednotne nastavený postup zaist'ovania virtuálnych aktív.

V kontexte s trestnoprávnou rovinou je možné uviesť, že informáciu o existencii virtuálnych aktív, kryptoaktív, môžu orgány činné v trestnom konaní získať napríklad na základe vlastnej operatívnej činnosti, alebo ďalších inštitútov v zmysle českého Trestného poriadku. Následne je možné aplikovať postup v zmysle § 78 českého Trestného poriadku, na základe ktorého policajný orgán získa prístup, napr. ku kryptopeňaženke. V prípade, ak má policajný orgán podozrenie, že ide o vec pochádzajúcu z trestnej činnosti aplikuje v danom prípade § 79a českého Trestného poriadku. Teda, ak sa zistí, že virtuálne aktíva sú napr. držané na burze alebo v kryptopeňaženke poskytovateľa, sú tieto subjekty povinné spolupracovať s orgánmi činnými v trestnom konaní a vykonať potrebné kroky, aby tieto prostriedky zablokovali, kým sa uvedené nevyrieši. V tomto smere je tiež nutné dodať, že český zákonodarca zaradil medzi mechanizmy kontroly postupu orgánov činných v trestnom konaní, **st'ažnosť**, v zmysle § 79a ods. 1 českého Trestného poriadku.

Na tomto mieste je možné konštatovať, že zaist'ovanie virtuálnych mien sa v rámci českej právnej úpravy nedeje na základe samostatného trestno-procesného inštitútu, ale analogicky sa aplikujú všeobecné ustanovenia českého Trestného poriadku. V tomto smere majú autori preto za to, že by bolo vhodné **rozšíriť právnu úpravu zaist'ovania vecí dôležitých pre trestné konania, priamo na kryptoaktíva**, ako je tomu v Slovenskej republike. V tomto smere by niektorí mohli namietat' a tvrdit', že uvedená novelizácia by sa mohla na prvý pohľad javit' ako nedôvodná, nakoľko český zákonodarca, totožne ako slovenský, v rámci právnej úpravy zaist'ovania vecí dôležitých pre trestné konanie, konkrétne v ustanovení § 79g českého Trestného poriadku, dáva možnosť zaistiť aj náhradnú hodnotu, a to v prípade, ak nie je možné zaistiť vec, ktorá je nástrojom alebo výnosom z trestnej činnosti. Dotknuté ustanovenie síce hodnotíme veľmi pozitívne, v tomto smere však podľa názoru autorov, uvedené ustanovenie nie je možné uplatňovať na virtuálne aktíva *in genere*, pretože odlišnosti, ktoré so sebou priniesla doba virtuality a kryptoaktív si zasluhujú aj špecifické metódy uplatňovania zaist'ovacích úkonov. V tomto smere máme za to, že by český Trestný poriadok mal byť rozšírený, a to konkrétne v rámci § 79, kde by bolo doplnené ustanovenie § 79i, ktoré by znelo nasledovne:

### **§ 79i Zaistenie kryptoaktíva**

- 1) *Ak zistené skutočnosti nasvedčujú tomu, že kryptoaktívum je nástrojom trestnej činnosti alebo výnosom z trestnej činnosti, môže predseda senátu a v prípravnom konaní prokurátor vydat' príkaz na zaistenie kryptoaktíva.*
- 2) *Ak vec neznesie odklad, môže vydat' príkaz podľa odseku 1 prokurátor aj pred začatím trestného stíhania. Taký príkaz musí najneskôr do 48 hodín potvrdit' sudca pre prípravné konanie, inak stráca platnosť.*
- 3) *V príkaze podľa odsekov 1 a 2 sa zakáže akékoľvek dispozície s kryptoaktívom a prikáže sa jeho vydanie vrátane vydania hesla, prístupového kódu alebo podobných údajov umožňujúcich nakladanie s kryptoaktívom. Právne úkony urobené v rozpore so zákazom podľa predchádzajúcej vety sú neplatné.*

- 4) *Príkaz doručí predseda senátu a v prípravnom konaní prokurátor bezodkladne vlastníkovi kryptoaktíva alebo osobe, o ktorej možno dôvodne predpokladať, že má prístupové údaje ku kryptoaktívu.*
- 5) *Ak pominuli dôvody na zaistenie kryptoaktíva, vydá predseda senátu a v prípravnom konaní prokurátor bezodkladne príkaz na zrušenie zaistenia kryptoaktíva.*
- 6) *Príkaz podľa odsekov 1 a 2 musí byť vydaný písomne a musí byť odôvodnený. V príkaze sa uvedie adresa úložiska kryptoaktíva orgánu, ktorý zaistený majetok spravuje podľa osobitného predpisu, označenie kryptoaktíva a počet jednotiek.*
- 7) *Vlastník kryptoaktíva, ktoré bolo zaistené, alebo iná osoba, ktorej bolo kryptoaktívum zaistené, má právo žiadať o zrušenie alebo obmedzenie zaistenia. O takejto žiadosti musí predseda senátu a v prípravnom konaní prokurátor bezodkladne rozhodnúť. Proti tomuto rozhodnutiu je prípustná sťažnosť. Ak bola žiadosť zamietnutá, vlastník kryptoaktíva, ktoré bolo zaistené, alebo iná osoba, ktorej bolo kryptoaktívum zaistené, ju môže, ak v nej neuvedie iné dôvody, opakovať až po uplynutí 30 dní odo dňa, keď rozhodnutie o jeho predchádzajúcej žiadosti nadobudlo právoplatnosť; inak sa o nej nekoná.*
- 8) *Ak je v trestnom konaní potrebné zaistiť kryptoaktívum na zabezpečenie nároku poškodeného na náhradu škody, postupuje sa primerane podľa odsekov 1 až 7.*

Na podklade autormi navrhovaného ustanovenia týkajúceho sa zaist'ovania kryptoaktív je možné vyvodit', že podkladom im bola právna úprava zaist'ovania kryptoaktív v Slovenskej republike, ktorá je odzrkadlením európskej legislatívy zaist'ovania kryptoaktív. V tomto smere je preto potrebné aj uviesť, že tak Slovenská republika, ako aj Česká republika, ktoré sú súčasťou Európskej únie spolupracujú s inými krajinami v oblasti regulácie virtuálnych aktív. V prípade medzinárodného charakteru trestnej činnosti (napr. v rámci transakcií cez rôzne jurisdikcie) je možné získať pomoc aj od medzinárodných organizácií, ktorými sú napríklad Europol, resp. Interpol, ktoré zároveň môžu koordinovať vyšetrovanie a zabezpečenie aktív na globálnej úrovni. Aj z dôvodu medzinárodnej spolupráce je tak potrebné zabezpečiť, aby národné právne úpravy boli čo najviac harmonizované a zabezpečila sa tak rýchla realizácia rozhodnutí v trestnom konaní.

V neposlednom rade si dovoľíme uviesť, že za účelom podania čo najkomplexnejších a najaktuálnejších informácií, autori dňa 12. 6. 2025, dotazovali Úrad pre správu zaisteného majetku, ako povinnú osobu v zmysle zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám v znení neskorších predpisov, aby si vyžiadali informácie ohľadom aktuálne zaistených kryptoaktívach. V toto smere im dňa 19. 6. 2025 bola doručená informácia, že Úrad pre správu zaisteného majetku má zaistenú virtuálnu menu v troch konaniach na dvoch účtoch peňaženiek. V prvom konaní sú na účte zaistené kryptoaktíva v počte 0,11909966 BTC, čo sa rovná v prepočte 12 482,28 USD amerického dolára, v druhom konaní ide o zaistené kryptoaktíva v počte 0,24769373 BTC, čo sa rovná v prepočte 25 959,63 USD amerického dolára a v poslednom konaní je na samostatnom účte zaistených 0,16633810 BTC, čo je v prepočte 17 422,31 USD amerického dolára.<sup>34</sup>

V kontexte možných právnych problémov, ktoré by mohli vyvstať v Českej republike, je možné konštatovať, že iba dostatočná právna úprava zabráni problémom súvisiacim

<sup>34</sup> Informácie poskytnuté na základe žiadosti zo dňa 12. 6. 2025, o sprístupnenie informácií v zmysle zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám v znení neskorších predpisov.

s virtuálnymi aktívami tak, aby orgány činné v trestnom konaní k transakciám neprístupovali tak, že všetky sú obligatórne nezákonné. Máme za to, že je dôležité presne definovať aké konania s virtuálnymi aktívami sú zakázané, podriaadiť ich pod centralizovaný dozor a následne určiť, akým spôsobom bude vynucovaná transparentnosť užívateľov takýchto virtuálnych aktív. Na druhej strane máme za to, že právna úprava Českej republiky je na dobrej ceste k adekvátnej právnej úprave, a naše slová potvrdzuje aj nedávno prijatý zákon o digitalizácii finančného trhu zo začiatku roka 2025. **Regulovanú trestnoprávnú úpravu virtuálnych aktív, najmä ich zaisťovanie v trestnom konaní, považujeme za kľúčový nástroj na zabránenie a potieranie legalizácie výnosov z trestnej činnosti.**

#### 4 **Zaistenie kryptoaktíva v Slovenskej republike pre účely trestného konania**

Zákomom č. 312/2020 Z.z. o výkone rozhodnutia o zaistení majetku a správe zaisteného majetku a o zmene a doplnení niektorých zákonov s účinnosťou od 1. januára 2021 došlo o. i. aj k novelizácii Trestného poriadku a k zavedeniu nových inštitútov zaistenia nástrojov trestnej činnosti a výnosov z trestnej činnosti, akými sú ustanovenia § 96a a § 96b o zaistení a obhliadke nehnuteľnosti, ust. § 96c o zaistení majetkovej účasti v právnickej osobe, zaistenie inej majetkovej hodnoty v zmysle § 96e, zaistenie hnutelnej veci podľa § 96f a zaistenie náhradnej hodnoty v zmysle § 96g.

Na účely tohto príspevku je najvýznamnejší inštitút upravený v **§ 96d Trestného poriadku, a to zaistenie kryptoaktíva**<sup>35</sup>. Zavedením predmetného § 96d TP došlo k zabezpečeniu transpozície smernice Európskeho parlamentu a Rady (EÚ) 2019/713 zo dňa 17. 4. 2019 o boji proti podvodom s bezhotovostnými platobnými prostriedkami a proti ich falšovaniu a pozmeňovaniu, ktorou sa nahrádza rámcové rozhodnutie Rady 2001/413/SVV. Vzhľadom na ich decentralizáciu, prvky kryptografického zabezpečenia a vysokú mieru anonymity, ktorú môžu kryptomeny poskytovať je často pre orgány činné v trestnom konaní náročné zachytiť, sledovať a vystopovať nelegálne transakcie virtuálnych mien.

V zmysle predmetného ustanovenia, ak zistené skutočnosti nasvedčujú tomu, že kryptoaktívum je nástrojom trestnej činnosti<sup>36</sup> alebo výnosom z trestnej činnosti,<sup>37</sup> môže predseda senátu a v prípravnom konaní prokurátor vydať príkaz na zaistenie kryptoaktíva nakoľko je to nevyhnutné pre úspešné zabezpečenie účelu trestného stíhania a pozastaviť právo nakladať s kryptoaktívom tak, aby mohla byť predmetom sankcie postihujúcej majetok,

<sup>35</sup> Zákomom č. 248/2024 Z. z. o niektorých povinnostiach a oprávneniach v oblasti kryptoaktív v znení neskorších predpisov došlo s účinnosťou od 30. 12. 2024 v rámci celého zákona č. 301/2005 Z. z. Trestný poriadok v znení neskorších predpisov, k náhrade slov, z pôvodných „virtuálna mena“ na aktuálne „kryptoaktívum“

<sup>36</sup> Pod pojmom **nástroj trestnej činnosti** sa podľa § 89 ods. 1 písm. b) Trestného poriadku rozumie vec, ktorá bola použitá na spáchanie trestného činu alebo bola určená na spáchanie trestného činu.

<sup>37</sup> V zmysle § 130 ods. 9 Trestného zákona sa **výnosom z trestnej činnosti** sa na účely tohto zákona rozumie a) vec, ktorá bola získaná trestným činom, b) vec, ktorá bola získaná ako odmena za trestný čin, c) vec, ktorá bola nadobudnutá, hoci aj len sčasti za vec, ktorá bola získaná trestným činom alebo ako odmena zaň, d) vec, na ktorú bola hoci aj len sčasti premenená vec, ktorá bola získaná trestným činom alebo ako odmena zaň, alebo e) plody a úžitky veci uvedenej v písmenách a) až d).

ktorou sa tento výnos odčerpá. Ak vec neznesie odklad, môže vydat' príkaz prokurátor aj pred začatím trestného st'uhania. Taký príkaz musí najneskôr do 48 hodín potvrdiť sudca pre prípravné konanie, inak stráca platnosť. Ide o n'ovum, ktoré sa zavádza do právneho poriadku Slovenskej republiky z dôvodu jej špecifického charakteru a potreby osobitného prístupu. Taktiež tieto orgány sú oprávnené vydat' príkaz na zrušenie predmetného zaistenia. Ak sa bude kryptoaktívum zaisťovať v rámci inštitútu prehliadok podľa § 99 Trestného poriadku a nasl., nie je potrebné vo veci vydávať samostatný príkaz na zaistenie kryptoaktíva.<sup>38</sup>

Keďže je kryptoaktívum počítačovým údajom s objektívnou hospodárskou hodnotou, uvedený príkaz vychádza z § 91 TP, avšak odlišuje sa čo do účelu zaistenia, ktorým je odčerpánie výnosu. Zaistenie virtuálnej meny je vždy na neurčitú dobu, a to až do okamihu právoplatného skončenia trestného konania a prípadného rozhodnutia o zaistenom kryptoaktíve alebo až do okamihu, kedy pominú dôvody zaistenia, najviac však na päť rokov s možnosťou predĺženia o 7 mesiacov, a to aj opakovane (porovnaj § 98a ods. 4 TP). Kryptoaktívum je možné zaisťiť aj ako náhradnú hodnotu (k tomu porovnaj § 96f TP), náležitosti príkazu na zaistenie náhradnej hodnoty vo forme virtuálnej meny sa spravujú ustanovením § 96d TP.<sup>39</sup>

Špecifická úprava je obsiahnutá v § 96d ods. 3 TP podľa ktorého sa zakáže akékoľvek dispozícia s kryptoaktívom a zároveň sa prikáže vydanie kryptoaktíva vrátane vydania hesla, prístupového kódu alebo podobných údajov umožňujúcich nakladanie s ním. Súčasne sa explicitne ustanovuje, že právne úkony urobené v rozpore so zákazom sú neplatné. Príkaz doručí predseda senátu a v prípravnom konaní prokurátor bezodkladne vlastníkovi kryptoaktíva alebo osobe, o ktorej možno dôvodne predpokladať, že má prístupové údaje k nemu. V zmysle dikcie § 96d ods. 6 TP takýto príkaz musí byť písomný a musí byť náležite odôvodnený. Osobitosť kryptoaktív zákonodarca v odseku 6 vyjadruje aj stanovením osobitných obsahových náležitostí odôvodnenia príkazu, ktorými sú:<sup>40</sup>

- uvedenie adresy úložiska kryptoaktíva orgánu, ktorý spravuje zaistenú virtuálnu menu,
- označenie kryptoaktíva (najmä s poukazom na mnohosť jej jednotlivých foriem a druhov),
- určenie počtu jednotiek, konkrétneho kryptoaktíva.

V § 96d ods. 7 TP je upravené právo žiadať o zrušenie alebo obmedzenie zaistenia kryptoaktíva. Proti negatívne rozhodnutiu o zamietnutí žiadosti o obmedzení alebo zrušení zaistenia je prípustná sťažnosť. V prípade negatívneho rozhodnutia o takejto žiadosti má vlastníak nehnuteľnosti možnosť podať opakovanú žiadosť po uplynutí 30 dní. V § 96d ods. 8 TP sa explicitne uvádza, že tento zaisťovací inštitút sa použije aj v prípade zaistenia nároku poškodeného, ktorý si ho v trestnom konaní riadne a včas uplatnil.

<sup>38</sup> Pozri (NS SR) R 47/2017 per analogiam.

<sup>39</sup> ČENTÉŠ, J. a kol. *Trestný poriadok – Veľký komentár*. Eurokódex, 2022. ISBN 978-80-8155-109-3.

<sup>40</sup> ČENTÉŠ, J., KURILOVSKÁ, L., ŠIMOVICEK, I., BURDA, E. a kol. *Trestný poriadok I, komentár*, 1. vyd. C. H. Beck, 2021. ISBN 978-80-89603-88-6.

Zákon bližšie nešpecifikuje kto je subjektom, u ktorého môže byť zaistené kryptoaktívum a preto sa môžeme v aplikačnej praxi následne stretnúť, že takým subjektom môže byť podozrivý, obvinený, svedok či iný subjekt, ktorý disponuje s kryptoaktívom, alebo má k nemu prístupové údaje a ten je nástrojom trestnej činnosti alebo výnosom z trestnej činnosti. Otázkou je, ako dochádza k „reálnemu“ zaisteniu. K jeho zaisteniu je potrebná znalosť údajov spojených s kryptoaktívami, akými sú kryptomenová peňaženka, kryptomenová burza, resp. kryptomenová zmenáreň.

Je ale otázne, ako postupovať v prípade, ak sa takýto subjekt nachádza mimo územia Slovenskej republiky, najmä v tretích štátoch (napr. USA, Ázia). Túto situáciu inštitút zaistenia kryptoaktíva v Trestnom poriadku **neupravuje** a s takouto možnosťou sa ani v Trestnom poriadku nestretávame. V takýchto prípadoch prichádza do úvahy vzájomná spolupráca v rámci dožiadania, čo je ale zdĺhavý proces a môže sa minúť účinku zaistenia virtuálnej meny.

Ďalším problémom je skutočnosť, ak subjekty neplnia uložené zákazy alebo príkazy. Ako už bolo uvedené, subjektom na účely zaistenia virtuálnej meny môže byť osoba podozrivá, resp. obvinená zo spáchania trestného činu, na ktorú sa vzťahuje zákaz nútenia k sebaobviňovaniu (*nemo tenetur se ipsum accusare*) vyjadrený v čl. 6 ods. 2, ods. 3 písm. c) Dohovoru o ochrane ľudských práv a základných slobôd, ako aj čl. 14 ods. 2, ods. 3 písm. g) Medzinárodného paktu o občianskych a politických právach. K **vydaniu kryptoaktíva nemožno žiadnym spôsobom takéto subjekty nútiť a opäť dochádza k minutiu sa účinku zaistenia.**

V takomto prípade je z nášho pohľadu najpriateľnejšie použitie ust. § 90 Trestného poriadku upravujúceho inštitút odňatia veci, ktoré je podozrivý alebo obvinený povinný strpieť. V uvedenom prípade ide o postup bez vyvíjania vlastnej aktivity podozrivého či obvineného definovaného ako zákaz sebaobviňovania v zmysle zásady *nemo tenetur se ipsum accusare* (porovnaj rozhodnutia ÚS ČR II. ÚS 255/05, II. ÚS 79 /07 a i.). Rovnako ústavné konformné je aj použitie § 91 Trestného poriadku – uchovanie, vydanie a odňatie počítačových údajov, vzhľadom na skutočnosť, že kryptoaktívum je počítačovým údajom. Na zariadenie, ktoré je nositeľom počítačových údajov nie je potrebné na zabezpečenie samotných údajov v ňom uložených následne uplatňovať postup podľa § 90 Trestného poriadku, resp. podľa § 116 Trestného poriadku. V tom prípade sa vec obsahujúca počítačové údaje (ku kryptoaktívu) legálne „dostala“ do rúk orgánov činných v trestnom konaní, napr. formou vydania či odňatia veci a následne sa zistilo, že obsahuje aj tieto údaje vo forme dôležitých pre trestné konanie. Podmienkou pre takýto postup však bude zachovanie všetkých podmienok pre zaistenie takejto veci – vrátane podmienky legálnosti, legitimacy a proporcionality.

V kontexte uvedeného je zaujímavou a legitímnou otázkou či možno ustanovenie § 96d Trestného poriadku o zaistení kryptoaktíva použiť aj na digitálne euro? Podľa nášho názoru **nie**, a to z dôvodu, že digitálne euro je/bude zákonné platidlo a nejde tak o kryptoaktívum v zmysle definície článku 3 ods. 1 bode 5 nariadenia (EÚ) 2023/1114. V takomto prípade by tak prichádzal do úvahy inštitút zaistenia digitálneho eura podľa ustanovenia § 95 Trestného poriadku, t. j. zaistenie peňažných prostriedkov na účte v zmysle ktorého

„Ak skutočnosti nasvedčujú tomu, že peňažné prostriedky na účte v banke alebo pobočke zahraničnej banky alebo iné peňažné prostriedky sú nástrojom trestnej činnosti alebo výnosom z trestnej činnosti, môže predseda senátu a v prípravnom konaní prokurátor vydať príkaz, aby peňažné prostriedky boli zaisťované. Príkaz na zaisťovanie podľa prvej vety sa môže týkať aj peňažných prostriedkov dodatočne dosiahlych na tento účet vrátane príslušenstva, ak sa dôvod zaisťovania vzťahuje aj na ne.“ Vo vzťahu k digitálnemu euru tiež vyvstáva ďalšia otázka súvisiaca s právnou ochranou takéhoto zákonného platidla. Trestný zákon v § 270 (*Falšovanie, pozmeňovanie a neoprávnená výroba peňazí a cenných papierov*) a § 271 (*Uvádzanie falšovaných, pozmenených a neoprávnených vyrobených peňazí a cenných papierov*) [podobné skutkové podstaty pozná aj český trestný zákon – pozn. aut.] poskytujú zákonnú ochranu najmä papierovým peniazom. Peniazmi sa rozumejú mince a bankovky domácej meny (t.j. nie peniaze na účte) alebo akejkoľvek inej zahraničnej meny, keďže tento znak skutkovej podstaty nerozlišuje medzi tuzemskými a zahraničnými peniazmi (napr. českou korunou). Smernica Európskeho parlamentu a Rady 2014/62/EÚ zo dňa 15. 5. 2014 o trestnoprávnej ochrane eura a ostatných mien proti falšovaniu, je prameňom sekundárneho práva v rámci právneho poriadku Európskej únie. Ochrana sa podľa tejto smernice (čl. 2) poskytuje mene euro (teda bankovkám a minciam tejto meny podľa nariadenia Rady (ES) č. 974/98 zo dňa 3. 5. 1998 o zavedení eura), ako aj iným menám, ak ide o bankovky a mince, ktorých obeh je zákonne povolený. Článok 3 tejto smernice podrobne špecifikuje druhy konaní, ktorých trestnosť majú členské štáty povinnosť ustanoviť, a to v podobnom rozsahu ako v prípade skôr uvedeného dohovoru: okrem falšovania peňazí, uvádzania falšovaných peňazí do obehu a distribúcie falšovaných peňazí sa postihuje aj výroba, distribúcia a držba potrebných materiálov na falšovanie). Smernica je pre členský štát záväzná v súvislosti s cieľom, ktorý sa má dosiahnuť (čl. 288 ZFEÚ) a členský štát má povinnosť – v súlade s prednosťou práva Európskej únie pred vnútroštátnym právom) – smernicu transponovať. Predmetné ustanovenia predstavujú transpozíciu tejto smernice. Taktiež nariadenie Rady (ES) č. 974/98 zo dňa 3. 5. 1998 o zavedení eura ustanovuje podľa článku 12 povinnosť členských štátov prijať primerané sankcie proti falšovaniu a napodobňovaniu eurobankoviek a eurominci.

Danie falšovaných, pozmenených alebo neoprávnených vyrobených peňazí alebo cenných papierov ako pravých znamená použitie takýchto peňazí alebo cenných papierov v obchodnom alebo hospodárskom styku. To znamená, že páchatel použije takéto peniaze alebo cenné papiere, teda platí peniazmi, resp. uplatňuje si cenný papier (napr. zmenku) voči osobe, ktorá z pohľadu páchatela považuje alebo má považovať tieto falšované, pozmenené alebo neoprávnené vyrobené peniaze alebo cenné papiere za pravé. Daním do obehu (vo vzťahu k peniazom) môže byť okrem platenia za tovary a služby tiež darovanie takýchto peňazí alebo ich danie ako zálohy, a to aj spôsob ich uvedenia prostredníctvom technického zariadenia.<sup>41</sup> Nie je pritom rozhodujúce, akým spôsobom potom s takýmito peniazmi alebo cennými papiermi osoba, ktorá ich prijala, následne naložila.<sup>42</sup>

Procesnú kooperáciu medzi vnútroštátnymi centrálnymi bankami a Európskou centrálnou bankou vo sfére ochrany eura pred falšovaním upravuje nariadenie Rady (ES) č. 1338/2001

<sup>41</sup> (NS SR) R 2/2009.

<sup>42</sup> (NS SR) R 58/1978.

zo dňa 28. 6. 2001 stanovujúce opatrenia nevyhnutné na ochranu eura proti falšovaniu. Úlohu ústredného orgánu Európskej únie na potláčanie falšovania eura plní Agentúra Európskej únie pre spoluprácu v oblasti presadzovania práva (Europol), a to na základe rozhodnutia Rady 2005/511/SVV zo dňa 12. 7. 2005 o ochrane eura proti falšovaniu ustanovením Europolu ako ústredného úradu na boj proti falšovaniu eura. Táto kooperácia zahŕňa výmenu informácií o technických a štatistických údajoch o sfalšovaných bankovkách a minciach (čl. 3), ich skúmanie (čl. 4 a čl. 5), povinnosti bankových inštitúcií (čl. 6), povinnosť spolupráce medzi Komisiou, Európskou centrálnou bankou a Europolom (čl. 7) a ďalšie procesné otázky.

Treba uviesť, že podobne ako v prípade ďalších digitálnych infraštruktúr by aj digitálne euro mohlo byť cieľom kybernetických útokov – ako je tomu napríklad v prípade kryptoaktív. Na potlačenie tohto rizika by sa koncepcia digitálneho eura mala opierať o najmodernejšie technológie, ktoré by vytvorili prostredie odolné voči počítačovej kriminalite. V tomto vidíme spoločné znaky s inými virtuálnymi menami, ktoré však nie sú digitálnou menou centrálnej banky. Rozvoj a rast počítačovej kriminality tak v oblasti financií je úzko spojený aj s rozvojom digitálnych mien centrálnych bánk.

## Záver

Národná rada Slovenskej republiky prijala dňa 15. 6. 2023 ústavný zákon č. 241/2023 Z. z., ktorým sa dopĺňa zákon č. 460/1992 Zb. Ústava Slovenskej republiky, a to vložением článku 39a do piateho oddielu druhej hlavy ústavy. Cieľom nového ustanovenia je o. i., aby mal každý právo vykonať platbu za nákup tovarov a poskytnutie služieb v hotovosti zákonným platidlom, pričom prijatie takejto platby možno odmietnuť len z primeraných alebo všeobecne uplatňovaných dôvodov. Napokon ústava po zmenách uskutočnených ústavným zákonom stanovuje, že podmienky a obmedzenia používania hotovosti podľa článku 39a ods. 2 ústavy ustanoví zákon. V kontexte tejto zmeny ústavy je potrebné upozorniť na názor súdneho dvora EÚ, ktorý pod pojmom „zákonné platidlo“ potvrdil, že ide o pojem práva EÚ, ktorý si vyžaduje v celej Európskej únii autonómny a jednotný výklad.<sup>43</sup> Vidíme tak, že aj zákonodarcovia si uvedomujú vznik nových foriem platidiel, prípade sa snažia reagovať na projekt digitálneho eura a chrániť ústavne zákonné hotovostné platidlo, ktoré je zakotvené v právnom rámci práva EÚ. Z uvedeného vyplýva záver, že na úrovni národných štátov nie je právne jednoduché vykonať legálnu ochranu hotovostnej platby, ktorá je regulovaná právom EÚ.

Otázok spojených s kryptomenami je niekoľko, od právneho statusu, techniky ochrany takejto meny až po spôsob jej ochrany pred rizikami spojenými so zneužívaním na financovanie organizovaného zločinu, prípadne terorizmu. Napríklad Čína v tomto roku zakázala jednotlivcom a organizáciám získavať finančné prostriedky prostredníctvom primárnej

<sup>43</sup> Pozri rozsudok Súdneho dvora zo dňa 26. 1. 2021, vo veci *Hessischer Rundfunk*, C-422/19 a C-423/19, EU:C:2021:63, body 45 až 49.

ponuky mincí (ICO), ktorá sa používa na vydávanie nových kryptomien. Otázok je teda zatiaľ v súvislosti s kryptomenami viacej ako odpovedí.

S kryptomenami úzko súvisia aj problémy s ich krádežou vo virtuálnom priestore. Stopy takejto trestnej činnosti sú vo väčšine prípadov minimálne a šanca tak na zadržanie páchatel'a veľmi nízka. Odpoveďou zákonodarcu je snaha regulovať tento segment tak, aby začali mať orgány činné v trestnom konaní prehľad o vlastníkoch takýchto mien a obchodoch, ktoré sa s nimi vykonávajú. V súčasnosti sme iba na začiatku tohto procesu a možno predpokladať zosilňovanie snáh o reguláciu a postihovanie protiprávneho konania vo virtuálnom priestore.

Rozsah nezákonného používania kryptomien v rámci trestnej činnosti je ťažké odhadnúť. Toto spravodajské oznámenie však poskytuje prehľad o nezákonnom používaní kryptomien vrátane tých služieb, ktoré uľahčujú ich nezákonné použitie, čo ilustruje relevantný prípad použitia. Poznámka je založená na operačných informáciách poskytnutých Europolu, údaje zozbierané na účely hodnotenia hrozieb závažnej a organizovanej trestnej činnosti v EÚ (SOCTA) 20211, a na správy zo súkromného sektora, akademickej obce a iné relevantné otvorené zdroje. Kryptomeny sú technickou a finančnou inováciou, ktorá si svoj potenciál pre globálnu ekonomiku drží vysoko. Zároveň sa využívajú aj na trestné účely pri absencii účinnej úpravy.

Napriek tomu, že trend užívania kryptomien v kriminálnych schémach rastie a zrýchľuje sa, je nepravdivé tvrdiť, že sú pre zločincov hlavným platidlom. Kryptomeny v porovnaní s inými spôsobmi platenia, ako sú napríklad platby v hotovosti, stále predstavujú len malú časť ekonomickej kriminality. Kryptomeny so sebou nesú množstvo limitov, ako sú veľké fluktuácie a neochota využívať kryptomeny k dlhodobým investíciám. Čo však „hrá“ v prospech kryptomien, ako nezákonného platobného prostriedku je fakt, že ich ústredným znakom je ich decentralizácia, teda ich slobodný prístup bez existencie centralizovaného ústredného orgánu, ktorý by sa za ne zaručoval a mohol ich spravovať. V rámci predloženého textu autori deklarovali niekoľkými rozhodnutiami súdnych autorít, že medzi problémy kryptomien je možné zaradiť aj ich používanie na nelegálne činnosti (od nákupu drog, až po financovanie terorizmu), krádeže, sprenevery.

Positívne autori vyhodnotili úničné nariadenie MiCA, nakoľko v jeho prípade ide o rozsiahlu právnu úpravu poskytujúcu jednotný právny rámec v oblasti kryptoaktív, stanovením pevných podmienok pre podnikateľov, a to s cieľom ochrany spotrebiteľov a trhu, s dôrazom na právnu istotu, ktorá do prijatia tohto nariadenia chýbala. Máme za to, že termín virtuálne aktívum je dostatočným a vhodným na pokrytie všetkých prípadných ďalších kryptomien, ktoré môžu vzniknúť, a to najmä z dôvodu, že už zo samotného názvu je zrejmé, že nejde o menu v riadnom slova zmysle, ako pri termíne „virtuálna mena“, ktorý vyhodnocujeme ako zmätočný. Každá štátom uznávaná mena si zasluhuje ochranu nielen na úrovni štátu samotného, ale aj na úrovni Európskej únie, nariadenie MiCA s definičným rámcom virtuálne aktívum, rozhodne túto ochranu rešpektuje.

Za účelom zabezpečenia implementácie nariadenia MiCA do právnej úpravy Českej republiky, sa autori rozhodli navrhnúť možné znenie ustanovenia venujúceho sa zaisteniu

kryptoaktív, a to po vzore Slovenskej republiky, avšak po úprave nedostatkov, s ktorými sa potýka v rámci zaist'ovania kryptoaktív aj slovenský zákonodarca.

Kriminálne využívanie kryptomien sa už nedeje len v kybernetickom priestore, ale týka sa celej škály kriminálnych aktivít, ako napríklad pašovanie drog, či finančné podvody. Ako často a v akom rozsahu sa kryptomeny v kriminálnych činnostiach využívajú, je ťažké odhadnúť. Organizovaný zločin a iné kriminálne siete sa však spravidla stále spoliehajú na platenie v hotovosti a formou bankových prevodov.

Kriminálnici sú vo využívaní kryptomien čím ďalej tým sofistikovanejší. Nezákonné platby stále častejšie prebiehajú cez početné transakcie zahŕňajúce viac subjektov, ktoré sa schovávajú za komplikované a neštandardné platobné schémy. Tie sú často neregulované a idú mimo mainstreamového trhu. Kriminálnici neustále hľadajú nové spôsoby, ako zahmlievať a hľadať alternatívne spôsoby prevádzania peňazí tak, aby ich pôvod bol horšie dohľadateľný.

Kryptomeny nie sú anonymné. Každá transakcia je zapísaná do decentralizovanej databázy – takzvaného blockchainu, kde sú uchovávané informácie o všetkých transakciách. Väčšina týchto databáz je dostupná verejnosti, tým pádom je možné nájsť pôvod transakcie. To znamená, že polícia a iné štátne zložky majú prístup k oveľa viac informáciám, než v prípadoch, keď sa používa hotovosť. Pôvod niektorých súkromných mien sa dohľadáva horšie ako pri regulárnych transakciách, čo ale neznamená, že sú užívatelia kryptomien úplne anonymní.

Záverom možno skonštatovať, že povedľa trestnoprávnej úpravy hrá v Českej republike dôležitú úlohu v oblasti ochrany pred zneužívaním virtuálnych mien či iných virtuálnych aktív AML zákon. Týmto zákonom bol zriadený Finančný analytický úrad, ktorý je samostatným úradom s celoštátnou pôsobnosťou, podriadený Ministerstvu financií. Jeho pôsobnosť je na poli prešetrovania, analýzy a získavania informácií o všetkých podozrivých obchodoch. V správnom konaní vydáva v rozsahu svojej pôsobnosti rozhodnutia. Za podozrivé obchody sa v zmysle predmetného zákona považujú obchody uskutočnené za okolností vyvolávajúcich podozrenia zo snahy o legalizáciu výnosov z trestnej činnosti alebo podozrenie, že v obchode použité prostriedky sú určené na financovanie terorizmu alebo, že obchod inak súvisí alebo je prepojený s financovaním terorizmu. Konkrétne môže ísť napríklad o transakciu kedy klient vyberá peniaze, alebo vykonáva transakcie v tesnej nadväznosti na vykonané vklady hotovosti.<sup>44</sup>

Zaist'ovanie výnosov z trestnej činnosti v rámci právnej úpravy Českej republiky je možné na základe dvoch právnych predpisov. *Prvým* je český Trestný poriadok, v rámci ktorého kľúčovú úpravu nájdeme v ustanoveniach § 79a a nasledujúcich, ktoré túto problematiku upravujú. K zaist'ovaniu výnosov z trestnej činnosti v zmysle tohto zákona dochádza na základe vydania uznesenia policajného orgánu alebo štátneho zástupcu o zaistení veci. Pričom platí, že dané uznesenie smeruje proti osobe, u ktorej zistené skutočnosti nasvedčujú napojeniu či spáchaniu trestného činu legalizácie výnosu z trestnej činnosti. *Druhým* právnym predpisom je AML zákon, ktorý poskytuje inštitúciám veľmi širokú právomoc zaist'ovania peňažných prostriedkov. Pri splnení zákonom stanovených predpokladov, môže banka na určitú

<sup>44</sup> § 6 ods. 1 písm. a) AML zákona.

dobu zaistiť peňažné prostriedky na účte, a to aj v prípade, že tak nekoná na základe rozhodnutia štátneho zástupcu, ale koná v rámci vlastnej kontrolnej činnosti. Z uvedeného teda vyplýva, že k zaist'ovaniu výnosov z trestnej činnosti môže dochádzať na základe dvoch režimov a je nevyhnutné uvedomiť si hneď na začiatku, ktorý z nich je aplikovaný. V prípade, ak rozhodne orgán činný v trestnom konaní zaistiť výnosy, resp. nástroje z trestnej činnosti (aj keď *de lege lata*, nie je možné v zmysle českého Trestného poriadku zaistiť virtuálne meny), z dôvodu podozrenia na trestnú činnosť týkajúcu sa legalizácie výnosov, bude aplikovaný český Trestný poriadok. V rámci druhého režimu je možné, aby samotná povinná osoba, ktorou môže byť, či už úverová inštitúcia, platobná inštitúcia, inštitúcia elektronických peňazí, právnická osoba, ktorá spravuje majetok spôsobom porovnateľným s obhospodarovaním investičného fondu, finančná inštitúcia podľa § 2 ods. 1 písm. b) body 11 a povinná osoba podľa § 2 ods. 1 písm. c) a osoba poskytujúca služby spojené s virtuálnymi aktívami.<sup>45</sup>

Rýchlo sa vyvíjajúca legislatíva a technologické pokroky sú kľúčovými výzvami pri regulácii a zaist'ovaní virtuálnych aktív. Tento problém sa týka nielen Slovenskej republiky a Českej republiky ale má globálny charakter. Na záver nám neostáva nič iné len vysloviť pranie, aby zákonodarca v blízkej budúcnosti k predmetnému inštitútu zaistenia virtuálnej meny viedol novú odbornú diskusiu v rámci všetkých krajín Európskej únie.

Príspevek je zverejnen pod mezinárodní verzí licence  
Creative Commons 4.0 International (CC-BY-4.0).

<sup>45</sup> § 21 ods. 8 AML zákon.