Kryptoměny a legalizace výnosů z trestné činnosti

V poslední době by bylo možné jen stěží najít i mimo odbornou veřejnost někoho, kdo by přinejmenším neslyšel o termínech jako kryptoměna, virtuální měna, bitcoin, blockchain či těžba virtuálních měn. Veřejná média publikují řadu článků o technologických souvislostech tohoto relativně nového fenoménu, většinou s pozitivním vyzněním. V menší míře se však také čtenář může dozvědět, že kryptoměny jsou užívány jako nástroj k legalizaci výnosů z trestné činnosti, v České republice navíc stále populárnější.

Finanční analytický úřad (FAÚ), k jehož hlavním úkolům patří zabraňování zneužívání finančního systému České republiky k legalizaci výnosů z trestné činnosti a k financování terorismu, se v rámci své činnosti věnuje i tématu kryptoměn, obecněji virtuálních měn (VM). S účinností od 1. 1. 2017 bylo v novele zákona č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu (AML zákon), zavedeno z tohoto pohledu důležité ustanovení v § 2 odst. 1 písm. l), ve kterém se jako povinná osoba pro účely tohoto zákona rozumí také osoba poskytující služby spojené s virtuální měnou, tedy (dle § 4 odst. 8 téhož zákona) konkrétněji každá osoba, která v rámci předmětu své podnikatelské činnosti kupuje, prodává, uchovává, pro jiného spravuje nebo zprostředkovává nákup nebo prodej VM, případně poskytuje další služby spojené s VM. V současné době tak k provozování tohoto podnikání není třeba žádné zvláštní oprávnění, a povinné osobě tak dosud zcela postačuje dispozice živnostenským oprávněním umožňujícím poskytování služeb v oboru „zprostředkování obchodu a služeb“, obsaženým v živnosti „výroba, obchod a služby neuvedené v přílohách 1 až 3 živnostenského zákona“. VM ani služby na ně vázané nejsou v České republice regulovány právními předpisy upravujícími platební služby a nespadají pod regulaci a dohled České národní banky. Z pohledu FAÚ tak v současné době není zřejmé, jaké povinné osoby v této oblasti v České republice aktuálně působí, neexistuje žádný oficiální seznam či rejstřík těchto osob, přičemž jejich vznik, fungování na trhu, ale i zánik jsou v poslední době mnohdy velmi dynamické. FAÚ v praxi tak vychází z informací, jež jsou obsahem zpracovávaných oznámení o podezřelých obchodech, případně z veřejných zdrojů, doplněných informacemi z pořádaných odborných diskusí k tomuto tématu. Tyto diskuse však navštěvují pouze ty PO, jež mají zájem na řádném fungování svého podnikání v souladu se zákonným rámcem předpisů České republiky.

Dle dosavadní koncepce i do budoucna AML zákon bude jako povinné osoby v oblasti virtuálních měn chápat všechny osoby, které, zjednodušeně řečeno, budou poskytovat služby s virtuální měnou.

5. AML směrnice přináší změnu

V této směrnici, která novelizuje směrnici předchozí, se mj. objevuje úprava (čl. 47, odst. 1), která zavazuje členské státy zajistit, aby poskytovatelé směnárenských služeb mezi VM a měnami s nuceným oběhem a poskytovatelé virtuálních peněženek podléhali nějaké formě registrace. Dle posledních informací z prací na novele AML zákona lze usoudit, že touto registrací bude samostatné živnostenské oprávnění, kterým bude muset být povinná osoba vybavena pro podnikání v tomto segmentu trhu. Dle dosavadní koncepce i do budoucna AML zákon bude jako povinné osoby v oblasti virtuálních měn (POVM) chápat všechny osoby, které, zjednodušeně řečeno, budou poskytovat služby s virtuální měnou. Tento fakt je v poslední době předmětem mnoha odborných debat a ze strany POVM je podrobován kritice kvůli (podle jejich názoru) velmi široce stanovenému okruhu osob, kterých by se do budoucna týkalo plnění povinností dle AML zákona.

Vybrané povinnosti POVM

Při podrobnějším pohledu na vybrané povinnosti POVM, jež dle stávajícího znění AML zákona mají, lze z pohledu FAÚ dojít k závěru, že ne ve všech případech dochází k plnění těchto povinností řádným způsobem, což přináší jako logický důsledek zvýšení atraktivity VM pro legalizaci výnosů z trestné činnosti. Typicky lze uvést chyby při identifikaci klienta (§ 7 AML zákona) a povinnost provedení kontroly (§ 9 AML zákona). POVM je povinna provést identifikaci klienta nejpozději tehdy, kdy je zřejmé, že hodnota obchodu překročí částku 1000 eur. Z pohledu komunity příznivců VM je předpokládané fyzické ověření klienta (tzv. identifikace face-to-face) výrazně omezující, neboť působí proti principu decentralizace transakčního systému, odstraňuje anonymitu plátce a ovlivňuje limity prováděných obchodů. Možná z podobných důvodů s přihlédnutím k mylné argumentaci, že fyzická kontrola klienta v prostředí VM je prakticky neproveditelná, přistupují – v rozporu se zákonem – POVM k akceptaci tzv. vzdálené identifikace klienta nevhodným užíváním postupu dle § 11 odst. 7 AML zákona. Tím však bohužel přispívají ke stále se zvyšujícímu trendu zneužívání odcizených identit pro zakládání (nejen) bankovních účtů sloužících ke shromažďování a transferu nelegálně získaných finančních prostředků (viz níže). S potěšením lze ale sledovat, že většina subjektů působících v ČR v oblasti směnárenství VM přistupuje k tvorbě a provozování takových AML mechanismů, které jsou i v prostředí VM, typických bleskovými transfery, schopné odhalit tzv. podezřelé obchody a podrobit je hlubší kontrole a rozboru, což v řadě případů vyústí v blokaci finančních prostředků pro následné trestní řízení a jejich faktické odstranění z moci pachatele pro vrácení osobám poškozeným. V naprosté většině případů ke kontrole a rozboru obchodu dochází na pomezí přeměny fiat měny a VM, jsou však evidovány i případy neuskutečnění obchodu s již směněnou VM jejím převodem z peněženky POVM na peněženku třetího subjektu.

K dalším ustanovením AML zákona, s jejichž aplikací mají POVM v praxi nejčastěji problémy, patří povinnost neuskutečnění obchodu (§ 15 AMLZ), povinnost oznámení podezřelého obchodu (§ 18 AMLZ) a povinnost mlčenlivosti (§ 39 AMLZ). Za komplikovanou lze příkladně označit formu oznámení o podezřelém obchodu, které by v ideálním případě mělo podat analytikovi a následně i orgánu činnému v trestním řízení odpověď na sedm základních otázek, zde vtělených do rubriky „popis případu“.

V tomto ohledu nepostačuje pouhé vygenerování tabulky informací o proběhlém/neproběhlém obchodu, tedy surová data transakce, ale je nutné je doplnit slovním popisem, přesněji deklarujícím, z jakých okolností POVM při identifikaci podezřelého obchodu vycházela. Nezbytným se jeví také tento popis doplnit např. uchovanou komunikací s klientem a dalšími rozšířenými identifikačními údaji klienta, pokud jimi POVM disponuje.

Schémata zdrojové trestné činnosti využívající VM

Hypoteticky lze uvažovat, že do VM lze transferovat výnos pocházející z jakékoli trestné činnosti, z níž pochází majetkový prospěch, i když ji dle systematiky trestního zákoníku nelze primárně podřadit pod trestnou činnost majetkovou (např. vydírání, šíření pornografie apod.). V praxi se však jedná v drtivé převaze o legalizaci výnosů z majetkové trestné činnosti, typicky podvodů ve všech jejich podobách. Pro využití této legalizační metody hovoří možnost rychlého transferu prostředků jak do směnárny VM, tak následně mezi jednotlivými peněženkami VM, v případě tuzemské směnárny využití absence nutnosti konverze fiat měny nutné např. u zahraničních burz, anonymita prostředí VM i navázanost oblasti VM na prostředí internetu, jehož je jako nástroje k páchání tohoto typu trestné činnosti převážně využíváno.

Podvodné weby

Nejčastějším typem vylákání finančních prostředků od poškozených jsou podvodné e-shopy a webové bazary, nabízející především nápadně levnou elektroniku, domácí zboží či léčebné přípravky. Při této trestné činnosti vyniká masivní zakládání bankovních účtů prostřednictvím tzv. vzdálené identifikace při užití odcizených, nalezených či padělaných dokladů. Narůstajícím a převažujícím trendem je využití kopie osobních dokladů, které pachatelé získají od poškozených s příslibem zajištění nebankovní půjčky. Výjimkou není založení většího počtu bankovních účtů na jednu odcizenou identitu. V této souvislosti byly zjištěny již celé legalizační sítě vytvořené z vědomě či nevědomě participujících osob, tzv. money mules. Po kumulaci prostředků následuje transfer do VM přes tuzemské směnárny, často jde o řadu paralelních transferů. Zjištěno bylo i zapojení BTC bankomatů a následné vylákané zaslání scanů papírových peněženek od poškozené osoby.

CEO fraudy

Dalším častým typem podvodů, který je charakteristický působením rozsáhlejších škod zejména právnickým osobám, je oblast tzv. CEO podvodů a obecně celková oblast kybernetické kriminality. Bylo registrováno již několik generací těchto CEO podvodů, od původních primitivnějších, kdy pachatel kontaktuje účetní podniku telefonicky, přičemž vystupuje jako ředitel společnosti, s požadavkem na urychlený transfer peněz za úhradu údajné zakázky, až po velmi sofistikované prolomení ochrany poštovních serverů a změnu platebních údajů na jinak oficiální faktuře, která má reálný základ a vazbu na podnikatelskou činnost společnosti. Do této kategorie lze také vřadit vylákání přístupových informací do počítače poškozeného a ovládnutí jeho elektronického bankovnictví, a to jak klasickou metodou phishingu, tak aktuálně se rozmáhajícími metodami smishingu (formou SMS zpráv, popř. zpráv v komunikačních messengerech) či vishingu (telefonický hovor s pachatelem vydávajícím se za pracovníka IT společnosti nebo banky s využitím prvků sociálního inženýrství). Pro poslední jmenovaný typ je charakteristické využívání směny VM s fyzickou osobou v různých státech za pomoci webového zprostředkovatele působícího ve Finsku (LocalBitcoins.com).

Romance fraudy

Za podstatný segment zdrojové trestné činnosti lze označit i tzv. romance fraudy, kdy pachatelé oslovují zvláště prostřednictvím sociálních sítí osamělé či partnersky strádající osoby a s využitím legendy o nutné potřebě pomoci od nich vylákají finanční prostředky, mnohdy přímo zasílané do zahraničních VM směnáren. Známá je např. legenda o americkém vojákovi v Afghánistánu, jehož nadřízenému je třeba poslat peníze, aby svolil ke sňatku s vojákem, nebo voják odesílající do ČR balík s cennostmi či hotovostí a požadující finanční prostředky na zaplacení cla apod. Tento segment volně rozvíjí známou problematiku tzv. nigerijských dopisů.

Financování terorismu

Při řešení otázky rizikovosti VM pro legalizaci výnosů z trestné činnosti byla zkoumána i hypotéza, zda prostřednictvím VM může docházet k financování terorismu. Při tom byla uvažována jak kategorie tzv. osamělého vlka či financování přípravy útoku malého rozsahu, tak možnost financování či podpora chodu teroristické sítě. Ačkoli zahraniční informace o pokusech využití VM pro tyto účely již existují, v tuzemských podmínkách zatím takové signály nebyly zjištěny.

Jsou tedy VM vhodným legalizačním nástrojem?

Na základě výše uvedeného a s podporou vytvářených statistických výstupů, které hovoří o stále se zvyšujícím nápadu řešených oznámení o podezřelém obchodu v návaznosti na zneužití VM, ale i o zvyšujícím se podílu trestních oznámení s prvkem zneužití VM na celkovém počtu trestních oznámení podaných FAÚ, lze uzavřít, že VM jako nástroj pro legalizaci výnosů z trestné činnosti jsou čím dál populárnější. Je možné přistoupit i k myšlence, že v době poklesu dřívějšího masivního investičního zájmu o VM je nutné na celou řadu transakcí do VM pohlížet jako na kriminálně relevantní transakce.

Pro snížení atraktivity tohoto nástroje pro kriminální komunitu se jako žádoucí jeví nové uchopení partnerství POVM a bankovního sektoru neulpívajícího na dosavadním chápání vztahu typu banka–klient, ale rozvíjejícího se do vzájemné komunikace partnerů důsledně uplatňujících AML opatření v tomto segmentu. Jak se zdá, některými zatracované, jinými glorifikované virtuální měny se stávají neoddělitelnou součástí finančního sektoru, kterou nelze již do budoucna ignorovat.

B | Text David Plecitý, vrchní rada, Finanční analytický úřad
www.bankovnictvionline.cz