POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

Katedra kriminální policie

Fakulta bezpečnostně právní

Kryptoměna jako potencionální nástroj legalizace výnosů z trestné činnosti

Diplomová práce

Cryptocurrency as a potential tool legalization of proceeds from crime

Diploma thesis

VEDOUCÍ PRÁCE

Ing. Vratislav Dvořák Ph.D.

AUTOR PRÁCE

Bc. Petr Pavelka

PRAHA

2022

Čestné prohlášení

Prohlašuji, že předložená práce je mým původním autorským dílem, které jsem vypracoval samostatně. Veškerou literaturu a další zdroje, z nichž jsem čerpal, v práci řádně cituji a jsou uvedeny v seznamu použité literatury.

V Libiši, dne 7. března 2022

Petr Pavelka

Tímto bych chtěl poděkovat vedoucímu mé diplomové práce panu Ing. Vratislavu Dvořákovi Ph.D. za odborné vedení, cenné rady, vstřícný přístup a shovívavost při mém vedení. Dále bych chtěl poděkovat všem, kteří mi poskytli informace z praxe a čas strávený při konzultacích.

Anotace:

V této diplomové práci se zmiňuji o kryptoměně jako potencionální hrozbě, která díky svému prvotnímu úmyslu decentralizace nad jakýmkoliv dohledem státu či jiného subjektu, vytvořila i nástroj k legalizaci výnosů z trestné činnosti. Práce zachycuje bitcoin jako nejznámější kryptoměnu současnosti a pravděpodobně i blízké budoucnosti, ale i jeho alternativy a zejména pak možnosti legalizace výnosů z trestné činnosti. Práce vymezuje způsob uchování bitcoinu, jeho rozvíjení a změnu po uskutečnění převodu až po zanechání stopy v blockchainu. Součástí diplomové práce je doložení několika případů, při kterých byly kryptoměny užity, ale také výzkum v prostředí orgánů činných v trestním řízení a navazující státní správy, které se podílí na zajištění výnosů z trestné činnosti.

Klíčová slova:

Kryptoměna – legalizace výnosů z trestné činnosti – bitcoin – přeměna výnosů – blockchain – NFT – swap

Annotation:

In this diploma thesis I mention the cryptocurrency as a potential threat which, thanks to its initial intention to decentralize over any supervision of the state or another entity, has also created a tool to launder the proceeds of crime. The thesis captures bitcoin as the most well-known cryptocurrency of the present and probably in the near future, but also its alternatives and especially the possibilities of legalization of proceeds from crime. The work defines the method of bitcoin preservation, its development and change after the transfer takes place after leaving a trace in the blockchain. Part of the diploma thesis is to document several cases in which cryptocurrencies were used, but also research in the environment of law enforcement agencies and related state administration, which is involved in securing the proceeds of crime.

Key words:

Cryptocurency – legalization of proceed of crime – bitcoin – transformation proceeds – blockchain – NFT – swap

Obsah

	Obsah	5
	Úvod	7
1.	Normy a regulace	9
1.1.	Vymezení kryptoměn v ČR	9
1.2.	Vymezení a regulace kryptoměn ve světě	11
1.3.	Shrnutí regulace	15
2.	Kryptoměna	16
2.1.	Bitcoin a altcoiny	17
2.2.	Kryptografie	22
2.3.	Blockchain a dvojitá útrata	23
2.4.	Peer to peer	25
2.5.	Swapovací služby	27
2.6.	Pračky bitcoinů	30
2.7.	Jiné formy směny a anonymita	31
2.8.	Krypto peněženky	32
2.9.	ICO, NFT, tokenizace	33
3.	Aplikace trestní odpovědnosti a dalších povinností	36
3.1.	Legalizace výnosů z trestné činnosti	38
3.2.	Nástroj legalizace trestné činnosti	41
3.3.	Výnos z trestné činnosti	42
4.	Vývoj kyberkriminality za užití kryptoměn	44
4.1.	Operativní rozpracování nelegálních aktivit	46
4.2.	Trasování	48
4.3.	Kyberútoky	48
4.3.1.	Phishing	49
4.3.2.	Vishing	50
4.3.3.	Ransom DDos atack	50
4.4.	Dokumentace pomocí případů	51
4.4.1.	Vývoj kyberkriminality za užití kryptoměn	51
4.4.2.	Carlos	52
4.4.3.	Phishing v praxi	53
5.	Zhodnocení postoje regulatorních orgánů a jejich kritika	53

Metody výzkumu a použité zdroje 54
Závěr 56
Použitá literatura 59
Zákonná úprava a prováděcí předpisy 60
Internetové zdroje 60

Úvod

Při pohledu na historický vývoj obchodu v kontextu se zavedením fiat měny, se lze podívat na Evropu v druhé polovině 17. století, kdy byly zavedením bankovek postupně nahrazovány směnky, které v té době nahrazovaly skutečné peníze uložené v bance. Tyto skutečné peníze z drahých kovů byly samy o sobě uchovatelem skutečné hodnoty v podobě ceny zlata a stříbra. Postupné zavedení papírových peněz došlo k usnadnění obchodování i jejich přesunům. I přes tento přechod na bankovky bylo uchováno krytí peněz a jejich hodnoty pomocí drahých kovů, zejména zlata, čímž bylo bráněno inflačním výkyvům.[1] Od plného krytí hodnoty peněz však došlo k částečnému či úplnému ústupu v průběhu 20. století a krytí drahými kovy bylo nahrazeno dluhem, tedy slibem splácet úvěr.

Obdobně překotný vynález přineslo ve 20. století zavedení bezhotovostních digitálních peněz, které ale nevytlačily skutečné peníze, ale jen finanční trh doplnily. S postupným rozmachem internetu a jeho zavedením do našich denních životů došlo i k rozsáhlému rozšíření internetového bankovnictví, zavedení platebních karet a jejich přenesení do chytrých mobilů a hodinek.

20. století toho přineslo více než dost, a tak počátek nového tisíciletí a prostředí internetu čekala opět další inovace a vznik kryptoměn. Ne absolutně prvním, ale zato zcela jistě nejznámějším se stal jejich průkopník bitcoin, který spatřil světlo světa v roce 2008 rukou jeho tvůrce Satoshi Nakamoto, který vyvinul celý systém těžení kryptoměn a účetní systém blockchain. Ačkoli je bitcoin dle obecně používaného sousloví označován jako krypto-měna, současná legislativa se na tento produkt dívá spíše jako na investiční aktivum. I přesto, že bitcoin nemá fyzickou podobu ani žádné krytí, získává oblibu a je možné ho u některých obchodníku skutečně jako platidlo užít, či ho v daném kurzu směnovat za konvenční měnu, za kterou však není skutečně označován, a to v důsledku jeho dosud vysoké volatility. Jak bylo zmíněno, bitcoin není jedinou kryptoměnou, vysoká obliba bitcoinu vedla k velkému rozmachu kryptoměn, což skutečně

---

[1] *NOVOTNÝ, Radovan. Čím jsou dnes peníze kryty? Dluhem. Mesec.cz [online]. 3.2.2016 [cit. 2022-03-01]. Dostupné z: https://www.mesec.cz/clanky/cim-jsou-dnes-penize-kryty-dluhem/*

nahrává tvrzení, že jde o investiční nástroj, protože v současné době lze na internetových stránkách coinmarketcap.com nalézt přibližně 9170 obchodovatelných kryptoměn. Nicméně výsadní místo si stále drží bitcoin, na který se tato diplomová práce jako synonymum kryptoměn zaměří.

Rostoucí popularita bitcoinu, která přenesla kryptoměny téměř z výhradního prostředí IT komunity do globálního světa sebou přinesla i nové problémy a zájem regulatorních úřadu o vymezení nového fenoménu. Proto je první část této diplomové práce zaměřena na jeho domácí i částečně světové legislativní vymezení s krátkým zhodnocení možného dalšího vývoje v podobě regulace trhu, spolu s popisem dění kolem posledního období zaměřeného na užití kryptoměn v oblasti legalizace výnosů z trestné činnosti.

Druhá a třetí část se pak zaměřuje na obecné pojmy kolem kryptoměn, se zaměřením na prvky, které umožňují život virtuálních měn, a to za vymezení základních prvků kryptografie, peer to peer prostředí, swapovacích služeb, bitcoin automatů a překážek, které znesnadňují monitorování obchodů kryptoměnami a s cílem podpořit hypotézu kryptoměn jako možného nástroje legalizace výnosů z trestné činnosti. Avizovaná třetí část se pak zaobírá trestní odpovědností a pojmy vysvětlující termíny nástroj, výnos a legalizaci trestné činnosti. Ve čtvrté části je pak zmíněn vývoj kyberkriminality za užití kryptoměn, spolu s hypotézou možného rozpracování trestné činnosti za pomoci dostupných nástrojů operativních. Dále je zde uvedena i další možnost pátrání po kyberměnách v blockchainu pomocí trasování a typy možných útoků, které jsou doloženy uskutečněnými případy na území České republiky, včetně jednoho rozsáhlého případu s pracovním názvem Carlos, který realizovala NPC. Tento případ se pak zaměřuje na drogovou scénu působící na darknetu, kde jako způsob platby její organizátoři využívali plateb pomocí kryptoměn.

V poslední části jsou pak shrnuty výzkumu a závěrečné shrnutí nastíněných hypotéz.

1. Normy a regulace

1.1. Vymezení kryptoměn v ČR

K vymezení kryptoměn, které jsou často chybně označovány za elektronickou měnu se nabízí zákon č. 284/2009 Sb. o platebním styku, který v § 4 vymezuje pojem elektronické peníze jako peněžní hodnotu, která představuje pohledávku vůči tomu, kdo ji vydal, je uchovávaná elektronicky, je vydávaná proti přijetí peněžních prostředků za účelem provádění platebních transakcí, či je přijímána jinými osobami než tím, kdo je vydal, což by se ve svém smyslu mohlo ukázat na virtuální měnu. Při snaze získat jasnou definici k vymezení kryptoměn se tak jako logické nabízí seznat stanovisko Česné národní banky, která vykonává dohled nad finančním trhem v České republice. Z pohledu ČNB je však kryptoměna chápána jako investiční nástroj, jelikož ze své podstaty neplní funkce měny. K otázce její regulace zastává víceguvernér ČNB Mojmír Hampl názor, že kryptoměnám není třeba pomáhat ani je regulovat a ve svém článku z prosince z roku 2017 uvádí: *„Nesnažme se vytvářet nějaká preskriptivní, detailní pravidla pro regulaci kryptoměn, protože to bude ve finále kontraproduktivní,“.* [2] Své tvrzení dále podkládá myšlenkovým základem, na kterém kryptoměny vznikly. Tím je vize decentralizace, která je pak ve zjevném kontrastu s politikou centrální banky. Kryptoměny považuje za tržní komoditu stejně jako kukuřici, tabák, či například zemní plyn. Současně uvádí, že kryptoměna oproti fiat měně neslouží k uchování hodnoty, její hodnota může denně kolísat o desítky procent, neslouží jako zúčtovací jednotka, jelikož stále dochází k přepočtu kryptoměn na konvenční měnu a stejně tak svůj závěr opírá o její doposud obtížnější užití coby platidla v běžném životě.[3] Jelikož ČNB neshledává v současné době regulaci kryptoměn

---

[2] HAMPL, Mojmír. *Náš postoj ke kryptoměnám? Nepomáhat, nechránit, neškodit, nevodit za ruku* [online]. ČNB, 2017, 21. 12. 2017 [cit. 2021-12-21]. Dostupné z: https://www.cnb.cz/cs/verejnost/servis-pro-media/autorske-clanky-rozhovory-s-predstaviteli-cnb/Nas-postoj-ke-kryptomenam-Nepomahat-nechranit-neskodit-nevodit-za-ruku/

[3] HAMPL, Mojmír. *Nejlepší využití kryptoměn – baterie?* [online]. ČNB, 2018, 21.3.2018 [cit. 2021-12-21]. Dostupné z: https://www.cnb.cz/cs/verejnost/servis-pro-media/autorske-clanky-rozhovory-s-predstaviteli-cnb/Nejlepsi-vyuziti-kryptomen-baterie/

jako důvodnou, neexistuje pro ně ani zákonné vymezení a tedy ačkoli o kryptoměnách hovoří jako o investiční komoditě, nelze je v současné době považovat ani za komoditu, potažmo za investiční nástroj a podřadit ji pod § 3 zákona č. 256/2004 Sb. o podnikání na kapitálovém trhu. V kontextu s existencí směnáren orientujícími se přímo na kryptoměny se jako další potencionální zákon nabízí ustanovení č. 277/2013 Sb. o směnárenské činnosti, jelikož však chybí její vymezení v přechozím zákoně č. 284/2009 Sb. nevztahuje se na kryptoměny ani jeden z nich. K dohledu nad virtuální měnou ČNB odkazuje na Finančně analytický úřad.

Z pohledu Finančně analytického úřadu (FAÚ) se jako nástroj sloužící k dohledu nad trhem s kryptoměnami jeví zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, obecně známého pod jeho anglickou zkratkou AML (Anti Money Laudering) zák. č. 253/2008 Sb. Zmíněný zákon a zejména pak jeho novelizace reaguje na fenomén kryptoměn a definuje kryptoměny jako virtuální aktivum. Současně ve svém znění zavádí určitá opatření při ochraně zájmu jmenovaného zákona. Vymezuje seznam povinných osob a jejich povinnosti při styku s tímto virtuálním aktivem a klientem. Povinnosti zákon spojuje s dvěma významnými hranicemi a to hranicí 1000 Eur, jejímž dosažením dochází k identifikaci klientů a druhým mezníkem 15000 Eur, který zakládá povinnost kontroly klienta. Spolu s povinnostmi dává tato norma nástroj k dohledu nad podezřelými obchody s virtuálními měnami. Tento zákon je pak doplněn řadou prováděcích předpisů a to vyhláškou č. 67 z roku 2018 Sb. o některých požadavcích na systém vnitřních zásad, postupů a kontrolních opatření proti legalizaci výnosů z trestné činnosti a financování terorismu, a dále metodickými pokyny z dílny FAÚ.

Právní úprava v oblasti zdanění kryptoměn dosud neexistuje a k tomuto účelu je třeba vycházet ze současné daňové legislativy, ačkoli pro takový případ není v současné době dostatečně přiléhavá. Z povahy virtuální měny ji lze označit za nehmotnou movitou věc, která je vyčíslitelná jak v době jejího nákupu, tak v době jejího prodeje konvenční měnou. Rozdíl v podobě zisku pak podléhá zdanění dle daně z příjmu podle § 3 odst. 2 zákona č. 586/1992 Sb., o daních z příjmů. Pro tyto účely je pak doporučováno uchovávat doklady o jejich pořízení i

doklady o jejich prodeji u fyzických osob či provést jejich inventarizaci u podnikatelských subjektů. Oproti nákupu krypta je těžba vnímána jako činnost, která by měla podléhat živnostenskému oprávnění, navzdory tomu je taková činnost osvobozena od DPH a to na základě závěru Soudního dvora EU, *„podle kterého samotná těžba kryptoměn není předmětem daně z přidané hodnoty, o předmět DPH se jedná, pokud existuje jednoznačná spojitost mezi poskytnutou službou a přijatou úplatou. Těžba kryptoměn však často skončí bez výsledku a získání odměny za tuto činnost je čistě náhodné.“*[4] *V případě dědění či darování kryptoměn se postupuje podle zákona o dani z příjmu, jelikož samostatná ustanovení a zákon o dani dědické a darovací byl zrušen k datu 1.1.2014.*[5]

Jedním nepřímým a spíše doplňujícím je pak zákon č. 254/2004 Sb. o omezení plateb v hotovosti a jeho novelizace zákon č. 261/2014 Sb. o změně zákona o omezení plateb v hotovosti, kterou došlo ke změně horní hranice částky pro hotovostní platby na 270.000,- Kč.

1.2. Vymezení a regulace kryptoměn ve světě

Ačkoli se České republice podařilo vymezit kryptoměny z pohledu centrální banky coby investiční nástroj, který je v kontextu s občanským právem chápán jako věc, není takový pohled z mezinárodního hlediska pohledem jednotným, a to ani v rámci evropského celku. Jak je vidět jedná se o velmi dynamicky rozvíjející otázku. Jako jedno z prvních se rozhodlo regulovat kryptoměny Německo, které k postavení bitcoinu přistoupilo velmi aktivně a již v roce 2013 mu přiznalo statut

---

[4] *Kryptoměny z účetního a daňového hlediska* [online]. *14.9.*2018. [cit. 2022-01-25]. Dostupné z: https://www.epravo.cz/top/clanky/kryptomeny-z-ucetniho-a-danoveho-hlediska-108117.htmll

[5] *Zdanění kryptoměn – Kompletní návod pro rok 2022* [online]. 2022 [cit. 2022-01-26]. Dostupné z: https://finex.cz/zdaneni-kryptomen-kompletni-navod/

virtuální měny a s ní i spojené výhody při odvádění daní jako u konvenčních měn.[6] Německo tak v EU patří mezi nejaktivnější státy, které bitcoin přijímají na svém trhu. Ministerstvo financí v srpnu 2013 klasifikovalo bitcoin jako „soukromé peníze". Současně se k bitcoinu vymezil německý BaFin[7], který zmínil, že bitcoiny *„nejsou elektronickými penězi ve smyslu zákona o dohledu nad platebními službami (ZAG), jelikož neexistuje žádný emitent, který by bitcoiny vydával na základě reklamace vůči nim. To je jiné s digitálními měnami, které jsou podporovány centrální autoritou (např. Liberty Reserve). Bitcoiny také nejsou zákonným platidlem, a tedy ani devizami, ani jinými obdobnými prostředky."* [8] Směnárenskou činnost s bitcoiny pak Německo spojilo se zákonem o bankách (KWG) a povolením s jejich obchodováním, které schvaluje právě BaFin. Obchod bitcoiny je považována jako soukromá prodejní činnost, takže veškeré zisky jsou daněny podle § 23 EStG. To znamená, že pokud osoba je vlastníkem bitcoinů před jejich prodejem déle než jeden rok, je osvobozena od daně z příjmů. Mimo to Německo transponovalo směrnice Evropského parlamentu a rady (EU) č. 2018/843, které Česká republika zahrnula v novele zákona AML.

Zajímavý je pohled na Turecký přístup ke kryptoměnám. Turecko v roce v dubnu 2021 cestou centrální banky bránilo obchodům prostřednictvím bitcoinů a dalších altcoinů, v obavě, že jde o rizikový nástroj s nedostatečným krytím. Avšak vysoká a neřízená inflace v zemi ve výši 21 procent, srazila hodnotu turecké lyry v září 2021 ke ztrátě 40 procent ze své běžné hodnoty vůči americkému dolaru. Tento vývoj Turky bránící se inflaci přivedl k investicím do ještě volatelnějšího bitcoinu jako uchovateli hodnoty v kratším časovém horizontu. Při takovémto vývoji předložil turecký prezident Erdogan v prosinci 2021 návrh zákon

---

6 *Bitcoin & Co.: Digitalwährungen auf dem Prüfstand* [online]. [cit. 2022-01-25]. Dostupné z: https://www.sparkasse.de/themen/geldanlage/bitcoin.html

7 *BaFin - Bundesanstalt für Finanzdienstleistungsaufsicht – Spolkový úřad pro dohled nad finančním trhem*

8 *Bitcoins: Aufsichtliche Bewertung und Risiken für Nutzer* [online]. 19.12.2013 [cit. 2022-01-25]. Dostupné z: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2014/fa_bj_1401_bitcoins.html

regulující tento fenomén, přičemž se předpokládá, že vůči kryptoměnám dojde k uvalení daně z příjmu.

Obdobným vývojem ode zdi ke zdi si prošly kryptoměny i na území Ruské federace. Jejich centrální banka se do poloviny roku 2014 držela celosvětového názoru a byla jim predikována budoucnost, přičemž víceguvernér banky uvedl, *„že stejně jako vše nové se i kryptoměny dostávají do rukou kriminálníků, především v oblasti drog a zbraní“*.[9] 13. ledna 2015 však následovalo, tamním úřadem Roskomnadzor[10] pro kontrolu dění na internetu, k zablokování přístupu na internetové stránky jako je bitcoin.org, bitcoin.it, indacoin.com či btcsec.com, které přinášely zejména informace ke kryptoměnám. Ve spojitosti se zablokováním stránek došlo k zákazu vydávání jiných peněžních jednotek a substitutů, za které byly považovány kryptoměny s cílem zabránit růstu stínové ekonomice, a to za současného zákazu jejich používaní občany a právnickými osobami na území Ruské federace, tak jak rozhodl Oblastní soud v Nevjansku. Současně však panoval názor ministra vnitra Alexeje Moškova, že kryptoměny je nutné regulovat, aby byli ochráněni jeho uživatelé. Nadto se však Rusko v roce 2021 po zákazu těžby bitcoinu v Číně vyhouplo na 11,2 procenta podílu na jeho těžbě, ke které docházelo i zejména díky nízké ceně energií. V roce 2021 přibyly další úvahy, zákaz těžby kryptoměn, vydání digitálního rublu a nakonec v lednu 2022 padlo rozhodnutí regulovat kryptoměny a zavézt daň z jejich těžby. Rozhodnutí o regulaci měla být známé do 18.2.2022, ale jelikož centrální banka požadovala úplný zákaz držení i těžby kryptoměn, nedošlo k žádnému konsenzu.

Čína jako největší kryptoměnový trh prošel rovněž řadou vývojových změn a postojů ke kryptoměnám. V 2013, 2017 a v květnu 2021 Čína zakázala finančním

---

[9] STROUKAL, Dominik. Kryptoměna bitcoin se v Rusku stala veřejným nepřítelem. *Ekonomickydenik.cz* [online]. 2015 [cit. 2022-01-15]. Dostupné z: https://ekonomickydenik.cz/kryptomena-bitcoin-se-v-rusku-stala-verejnym-nepritelem/

[10] Roskonadzor je ruskou federální službou pro dohled nad komunikacemi, informačními technologiemi a hromadnými sdělovacími prostředky v RF, byla založena v roce 2009, (http://eng.rkn.gov.ru).

institucím a platebním společnostem poskytovat služby související s transakcemi kryptoměn. Poslední a úplný zákaz všech kryptotransakcí a těžby na čínském území zazněl 24. září 2021. Zákaz byl vydán nejen z důvodu možného poškození finančního trhu, sociálního řádu, pro možné spojení s legalizací výnosů z trestné činnosti, ale také z důvodů energetické náročnosti při těžbě a převodu kryptoměn, což již v minulosti vedlo odstřihnutí miningových poolů od elektrické energie. Návrat ke coinům však není vyloučen z důvodu hrozící ztráty na těžbě a přenechání zisku mezi další výrazné hráče jako USA, Rusko a Kazachstán. Uvedené důvody pro odklon od cizích kryptoměn nemusí být hlavním důvodem, jelikož Čína spustila svůj vlastní digitální jüan, který je v pokročilé pilotní fázi.

Postoj spojených států je pak konstantní. Internal Revenue Service (IRS), která plní úlohu daňové služby pro federální vládu Spojených států vydala směrnice IRS Notice 2014-21, IRB 2014-16, jako vodítko pro jednotlivce a firmy jako vodítko daňové povinnosti vyplývající z transakcí spojených s virtuálními měnami.[11] IRS také zveřejnila vyjádření s názvem Frequently Asked Questions on Virtual Currency Transactions, jako doporučení pro jednotlivce, kteří drží kryptoměnu jako kapitálové aktivum a nezabývají se obchodem nebo podnikáním v oblasti prodeje kryptoměn.

Kryptoměny jsou však velkým tématem i ostatních státech. Salvador uznal bitcoin jako oficiální měnu, což vedlo k nárůstu poštu turistů, to ale prozatím nic nemění na kritické hospodářské situaci.

Na půdě EU padlo v roce 2015 vyjádření k tématu kryptoměn, které vydala Evropská centrální banka. Její definice zazněla v analytické zprávě Schémata virtuální měny, kde byly kryptoměny vymezeny jako *„digitální vyjádření hodnoty, nevydané centrální bankou, úvěrovou institucí nebo institucí elektronických peněz, které lze za určitých okolností použít jako alternativu k penězům“.* [12] K tomuto však

---

[11] Virtual Currencies. Irs.gov [online]. [cit. 2022-02-17]. Dostupné z: https://www.irs.gov/businesses/small-businesses-self-employed/virtual-currencies

[12] Virtual currency schemes – a further analysis. *Coindesk.com* [online]. 2015, únor 2015 [cit. 2021-12-24]. Dostupné z: https://ec.europa.eu/commission/presscorner/detail/en/IP_20_1684

vydal své stanovisko i Evropský soudní dvůr, který uvedl, že *„bitcoinové transakce „jsou osvobozeny od DPH na základě ustanovení o transakcích týkajících se oběživa, bankovek a mincí používaných jako zákonné platidlo.“* [13] Jelikož šlo o rozhodnutí ESD jde o stanovisko nadřazené a jiným rozhodnutím členských zemí EU. K samotné regulaci kryptoměn existují na půdě EU i další obavy z energetické náročnosti při těžbě kryptoměn generovaných z práce cestou proof of work dotýkajících se bitcoinu a etherum. Díky energetické náročnosti tak mělo dojít k jejich omezení. Prozatím se však jednalo jen o návrh, který měl být projednán 28.2.2022. Vzhledem však k válečnému stavu mezi Ukrajinou a Ruskem, které je hlavním dodavatelem ropy a zemního plynu na trh EU, lze vývoj takovým směrem předpokládat. Z důvodů sankcí uvalených v únoru 2022 vůči Rusku a Bělorusku v souvislosti s válečným konfliktem lze předjímat i rychlejší regulaci kryptoměn, které by umocnili dosažení hospodářské izolace cestou většího monitoringu a potlačení anonymity kryptoměn, které by pak byly obsaženy legislativě známé jako Markets in Crypto Assets (MiCA).

1.3. Shrnutí regulace

Z uvedených příkladů týkajících se regulace na našem a zejména pak i světovém trhu lze konstatovat, že kryptoměny jsou v současné době převážně chápány jako investiční nástroj a nikoli jako skutečné peníze, ačkoli v Německu lze v pojetí této problematiky nalézt jistou názorovou rozpolcenost. V České republice jsou kryptoměny neregulované a víceguvernér České národní banky zastává názor, že by k regulaci nemělo dojít ani v současné době ani v budoucnu, jelikož by to mohlo vést k tomu, že by lidé začali považovat kryptoměny jako tradiční měny, za což je ČNB nepovažuje a ni si takový vývoj nepřeje, jelikož by ztěžovalo měnovou politiku ČR. Budoucí regulační opatření jsou však velkou

---

[13] FILLNER, Karel. Soudní dvůr EU: Bitcoinové transakce osvobozeny od DPH. *Btctip.cz* [online]. 2015, 22.10.2015 [cit. 2021-12-24]. Dostupné z: https://ec.europa.eu/commission/presscorner/detail/en/IP_20_1684

výzvou i velkou neznámou. Jak by se dalo předpokládat z jejich velkého rozmachu, dochází v současné době i k čím dál častějšímu spojování s legalizací výnosů z trestné činnosti a současně i s energetickou náročností těžby potažmo ověřování obchodů kryptoměnami, což v současné době přináší další problém a otázku nad skutečným provozováním těžby, která je ve své podstatě, spolu s blockchainem jediným dohledem nad osudy a pohybem kryptoměn založeným na tomto principu. Nicméně dochází spolu s postupným rozmachem bitcoinu, velikosti blockchainu a zejména náročnosti na početní výkon potřebný pro těžbu ke spojování těžařů do spolků (poolů), kteří se na těžbě podílí, takovým přístupem dochází k částečnému vytlačení malých těžařů a tím i prozatím mírné centralizaci. K částečné centralizaci prostředí dochází i například v případě lightcoinu (odnož bitcoinu), který zajišťuje rychlejší platební operace s dohledem soukromé společnosti bez potřeby ověření v blockchainu. Navíc kryptoměnový sektor v předchozím roce postihl výrazné regulace, zejména s ohledem na největší kryptoměnový trh, jakým je Čína, která zakázala těžbu. Zákaz byl převážně motivován právě zmíněným nedostatkem energií, který by mohl v současné době výrazně ovlivnit rozhodování o dalším vývoji regulace na evropském trhu. Regulace se tak bude i s ohledem na současné dění na Ukrajině, pokles hodnoty rublu a ukládaných sankcí proti Rusku výrazně měnit. Zásadní kroky v regulaci lze předpokládat i zejména s omezením nákupu deviz na ruském trhu, což by mohlo vést ke zvýšenému zájmu o investice do kryptoměn, jako nástroje na uchování hodnoty, jako k tomu došlo ve už ve zmíněném Turecku. Takovýto vývoj by pak mohl významným způsobem upravit a možná dokonce i zastavit těžbu, ale také užívání kryptoměn, aby ukládaná sankční opatření nemohla být obcházena.

2. Kryptoměna

Kryptoměna z anglického cryptocurrency je spojením dvou slov, které ji ve své samostatné podobě téměř plně vystihují či naznačují její ambice. První část složeniny „krypto“ je odvozeno od slova kryptografie, které je označením pro

samostatný vědní obor matematického šifrování, jež je v případě kryptoměn užíváno k zabezpečení uskutečněných transakcí. Druhé slovo měna v tomto kontextu nenaplňuje svůj doslovný význam, ale spíše nastiňuje své ambice či potenciál skutečnou měnou být. Za skutečnou měnu nelze kryptoměny v současné době a v celosvětovém měřítku považovat, ačkoli už se takové trendy objevili, jako například v Salvadoru, kde byl bitcoin uznán jako zákonné platidlo. Aby bylo kryptoměny možné užívat bylo nutné vypořádat se s bezpečností při jednotlivých převodech. S tím se vypořádal jako první Satoshi Nakamoto, tvůrce bitcoinu, který vyřešil problematiku dvojího účtování tzv. „double spend“, za pomocí blockchainu. Ačkoli nejznámějším tvůrcem je Satochi Nakamoto a jeho bitcoin, není zdaleka první kryptoměnou, před rokem 2008 existovaly digitální měny DigiCash a e-gold, které existovaly ryze v prostředí internetu a bez dostatečného zabezpečení. Hlavním charakteristickým znakem dnešních kryptoměn je jejich decentralizace, tedy jejich svobodný přístup bez existence centralizovaného ústředního orgánu, který by se za ni zaručoval a mohl ji spravovat.

2.1. Bitcoin a altcoiny

V historii kryptoměn není bitcoin první elektronickou měnou, rozhodně je však nejznámější, nejrozšířenější. Na bitcoin lze nahlížet jako na největšího průkopníka mezi kryptoměnami, který vešel v široké povědomí. V době před vznikem bitcoinu existovalo několik jiných a méně známých elektronických měn, jako DigiCash, E-gold a Liberty Reserve. Všechny měly však jedno společné pojítko a tou byla centralizace. Osud všech měn byl pevně spojen s jejich tvůrci, oproti Bicoinu jim chyběla ta hlavní vlastnost, která činí bitcoin nezávislým a tou je decentralizace.

Nejznámější kryptoměna Bitcoin se zrodila v letech 2008 - 2009 jako dílo osoby Satoshi Nakamoto, která vytvořila v prvním roce nejprve samotný protokol a software. Následně pak Satoshi v roce 2009 vydal fungující platformu a spustil

celou fungující síť generující, dnes nejznámější kryptoměnu bitcoin. Cíleně jsem zmínil osobu, jelikož kolem samotného tvůrce není dosud jasná jeho skutečná totožnost, původ a dokonce ani zda jde o jednotlivce či uskupení více kooperujících lidí. Jedna z hypotéz se zmiňuje o tom, že Satoshi Nakamoto je pseudonymem týmu vývojářů, kteří tuto měnu vytvořili a uvedli do života. Existuje však i jiná teorie, kdy se pod tímto jménem přihlásil australský vědec Craig Steven Wright. Této hypotéze nasvědčuje mnoho jazykových podobností odhalených pomocí stylometrie[14], které panu Wrightovi jeho autorství přisuzuje. Dalším důkazem byl i čas zobrazující se u příspěvků, kterými Satochi Nakamoto odpovídal na dotazy na fórech zabývající se problematikou kolem Bitcoinu. Sám Wright se k vytvoření kryptoměny přihlásil a před novináři předvedl několik operací potvrzující jeho tvrzení. Původ Bitcoinu i autorství stojí za zmínku, jelikož se tímto problém zaobírala i americká NSA, která tento produkt neboli měnu zkoumala jako možný nástroj, jež by mohl způsobit destabilizaci měnového trhu a vedl by tak k případnému rozpadu hospodářství. NSA Bitcoin prověřovalo jako možnou zbraň z dílny Ruska nebo Číny. V tomto ohledu by se dalo bitcoin nebo kryptoměny celkově považovat za makroekonomický nástroj.

Osud DigiCash se vyvíjel slibně, její tvůrce David Chaum, využil k jejímu vzniku a ochraně kryptografii veřejného a soukromého klíče. Její osud chtěl spojit s bankovním sektorem, k jejímu získání měla vést bankovní výměna fiat za anonymní elektronickou měnu. Něž zákazníci zatoužili používat k platbám DigiCash, uběhlo skoro 10 let. Celá jeho myšlenka měla být završena podepsáním dohody Chauma s ING bank, ale dohoda se mu nezdála v pořádku a z celého projektu vycouval. Následně DigiCash dostal další velkou šanci, když Microsoft údajně nabídl 100 milionů dolarů na integraci DigiCash do každé instalace Windows 95, ale Chaum odmítl i tuto dohodu, údajně nepovažoval dohodu za

---

14 Stylometrie je aplikací studia lingvistického stylu, obvykle psaného jazyka, ale úspěšně se uplatňuje i na hudbu a na umělecké malby. Jedná se o statistickou definici nebo potvrzení vlastností stylu nebo díla. Stylometrie se často používá k přiřazování autorství, času a původu k anonymním nebo sporným dokumentům.

přínosnou. V obou těchto případech tak DigiCash doplatila na svou centralizaci spojenou se svým tvůrcem. To poté znamenalo konec projektu, společnost DigiCash se vzbouřila a Chaum odstoupil a nedlouho poté se DigiCash rozpustil.

E-gold byla digitální měna, kterou přivedli na svět Douglas Jackson a Barry Downey v roce 1996. Myšlenka byla jednoduchá a vycházela z principů běžného oběživa, které bylo ve svých počátcích kryto zásobami zlata. Princip E-gold spočíval v jeho krytí skutečným zlatem, které mělo být uloženo v bezpečnostní schránce na Floridě. V jeho největší slávě existovali zásoby zhruba 4 tun drahého kovu (přibližně 85 milionů dolarů). E-gold získali online uživatelé výměnou fiat za virtuální měnu, která představovala gramy tohoto zlata (později také stříbra, platiny a paladia). Získáním E-gold pak mohli okamžitě anonymně posílat peníze komukoli. E-gold se stal první digitální měnou, kterou používalo více než 1 milion lidí, a prvním způsobem platby bez kreditní karty, který bylo možné integrovat do e-shopů. E-gold se také dal rozdělit na miligramy zlata a byl tedy prvním fungujícím mikroplatebním systémem. E-gold dosáhl svého vrcholu v roce 2006, jeho převody dosahovaly výše 2 miliard dolarů ročně. Největší oblibu získal mezi obchodníky s drahými kovy, aukčními domy, online kasiny a politickými a neziskovými organizacemi, ale také mezi lidmi, kteří chtěli při svých platbách zůstat v anonymitě. Jedním z jeho problémů bylo, že nebyl dostatečně kryptograficky zabezpečen, čelil mnoha hackerským útokům. Díky tomu se E-goldu dostalo zvýšené pozornosti státu a regulačnímu dozoru. Tomu nepřispělo ani to, že byl E-gold označen za měnu zločinců a teroristů. Souběžně s provozováním tohoto aktiva došlo k zamítnutí žádosti o převod měn. Poté finanční úřady přistoupily ke zmrazení fyzických rezerv e-gold, což způsobilo, že většina uživatelů platformu opustila. Poté Jackson dostal dohodu, kde se mohl přiznat k praní špinavých peněz a získat 300 hodin veřejně prospěšných prací, pokutu 200 dolarů, 6 měsíců domácího vězení a 3 roky zkušební doby, stejně jako šanci požádat o licenci na převod peněz. místo maximálního trestu 20 let vězení a pokuty 500.000 dolarů.

Nakonec se Jacksonovi nepodařilo získat licenci na převod peněz pro e-gold, protože odsouzeným zločincům není povoleno získat licenci na převod peněz, což ukazuje, že dohoda o vině a viny byla tajným nastavením k zabití e-gold. Příběh e-gold ukazuje mnohá selhání centralizace. Pokud má digitální měna fyzické rezervy, může je snadno zabavit vláda, a pokud digitální měnu provozují známí jednotlivci, mohou být tito jednotlivci zatčeni a stíháni. Také centralizované úložiště e-gold způsobilo, že je vysoce náchylné k hackerům.

Dalším byla Liberty Reserve, ta se stala velmi populární a přitahovala aktivity na černém trhu, jako je obchodování s ukradenými kreditními kartami, krádeže identity, služby počítačového hackingu, Ponziho schémata a trestné praní špinavých peněz obecně. Vzhledem k tomu, že Budovský byl již hledaný zločinec, úřady ho zatkly, jakmile to bylo možné, což bylo v roce 2013. V té chvíli byl zabaven veškerý Budovského majetek a Liberty Reserve byla zabavena a ukončena, ale ne dříve, než bylo úspěšně odčerpáno 8 miliard dolarů z Liberty Reserve. Za svou nelegální činnost dostal Budovský 20 let vězení a pokutu 500.000 dolarů. Konec Liberty Reserve v tomto případě neprovedl přímo její tvůrce, ale americká vláda.

Příběhy raných digitálních měn DigiCash, e-gold a Liberty Reserve jsou tedy důkazem toho, že digitální měny lze snadno zabít centralizací. Bitcoin nevlastní nikdo. Funguje na principu open-source, takže jej může kdokoli používat zdarma a jeho přijetí nebo použití nelze potlačit centralizovaným rozhodováním, narozdíl od DigiCash. Ačkoli existují tendence zavést přísné regulace bitcoinů, jde zatím jen o úvahy. Nelze si zatím představit omezení, kterým by šlo bez souhlasu provozovatelů bitcoinu takový krok uvést do praxe. Jde o to, že bitcoiny jako celek nikdo nevlastní a neexistuje způsob, jak někoho zatknout, donutit k takovému kroku, nebo zaútočit na konkrétní počítač, aby došlo k zmrazení či odebrání veškerých bitcoinů. Bitcoin existuje v každém počítači, na kterém je provozován, díky čemuž je decentralizovaný a nedostupný nedobrovolné regulaci, což je také důvod proč stále existuje i dnes. Nelze vyloužit, že v budocnu dojde k uričitému

konsenzu příznivců bitcoinu s vládnoucími celky, ale v současné dob ěto lze vyloučit.

Bitcoin (BTC) řeší všechny tyto problémy tím, že je decentralizovaný a kryptograficky bezpečný. Je nemožné hacknout soukromý klíč bitcoinu (BTC), pokud tento klíč není uložen nikde online mimo peněženku a vláda nemůže jednoduše zatknout vůdce bitcoinu bez chybějícího centrálního prvku, protože bitcoiny nikdo neřídí. Podstata bitcoinů je, že jsou uloženy v kryptograficky zabezpečené a decentralizované účetní knize a nemohou být zabaveny vládou.[15], [16]

Hlavními principy vzniku bitcoinu, potažmo kryptoměn, bylo oproštění od závislosti na bankovním sektoru, oproštění na centrálním řídícím systému spravovaném centrální bankou a jeho monetární politikou, ale zejména byl postaven s cílem vlastní měnové svrchovanosti. Ta spočívá zejména ve vyloučení třetí osoby dohlížející na převod měn, čímž dochází k jejímu odstřihnutí od zdrojů příjmů, ale současně tím dochází k odstranění kontrolních mechanismů nad tokem peněz. Výhodou vzniku takového svrchovaného systému pak došlo k vlastnímu a přímému dohledu nakládáním s takovými prostředky a vytěsněním zprostředkovatele tedy banky. V době vzniku kryptoměn neexistoval trh umožňující obchod tradičními finančními prostředky. Neexistovala ani poptávka po takovém nástroji, a to zejména s ohledem na cíl, kterým měla být zmíněna decentralizace. Proto následoval vznik obchodu mezi oběma koncovými uživateli tedy anglicky peer to peer, který byl zkrácena s použitím foneticky znějící číslovky 2 na zkratku P2P. Způsob takové obchodu byl tedy v počátku limitován na klasickou výměnu a důvěru mezi oběma stranami.

---

15 *Liberty Reserve, E-gold, and DigiCash: How Early Digital Currencies Proved That Centralization Is a Death Knell* [online]. In: MASHIACH, Zachary. 23.1.2020 [cit. 2021-12-19]. Dostupné z: https://www.cryptoiqtrading.com/liberty-reserve-e-gold-and-digicash-how-early-digital-currencies-proved-that-centralization-is-a-death-knell/

16 *Liberty Reserve, E-gold, and DigiCash: How Early Digital Currencies Proved That Centralization Is a Death Knell* [online]. In: MASHIACH, Zachary. 23.1.2020 [cit. 2021-12-19]. Dostupné z: https://www.cryptoiqtrading.com/liberty-reserve-e-gold-and-digicash-how-early-digital-currencies-proved-that-centralization-is-a-death-knell/

Krátce po vzniku Bitcoinu se začaly objevovat i další kryptoměny, kterým se stal bitcoin předlohou. Začaly kopírovat i systém zabezpečení blockchain. Takové kryptoměny jsou obecně označovány jako altcoiny, což pochází z anglického názvu *„altcoins“. „Altocins“* je složenina slov *„alternativní“* a *„coin“* jako druhá slabika slova bitcoin. V současnosti době existuje téměř 10.000 různých altcoinů. Některé altcoiny se od bitcoinu zase tak moc neliší, dokonce kopírují blockchain, jedná se o klasické deriváty, příkladem může být Litecoin nebo Dash. Jiné altcoiny se mohou od bitcoinu lišit v několika aspektech, například mírou anonymity. Obecně se alternativní mince snaží bitcoin vylepšit či zdokonalit jeho nedostatky, ne vždy však úspěšně.

2.2. Kryptografie

Současné kryptoměny a Bitcoin fungují na základě několika vědních oborů, a to ekonomie, matematiky a jejího odvětví kryptografie. Kryptografie se zabývá šifrováním, tedy převodem zpráv do utajované podoby a zpět, které jsou poté čitelné jen se znalostí šifrovacího klíče. Takovéto jednoduché vysvětlení je principem symetrické kryptografie, při které je užit k zašifrování a odšifrování shodný klíč, který musí oba uživatelé sdílet, což je v případě bezpečného předání mezi dvěma neznámými osobami velmi problematické. Proto je k provádění transakcí bitcoinů v blockchainu a síti P2P užito asymetrické kryptografie, která umožňuje obou uživatelům používat vlastní klíč. Asymetrická kryptografie je postavena na páru kryptografických klíčů, z nichž jeden je veřejný a druhý privátní. Veřejný klíč slouží jako adresa, na kterou může kdokoli poslat bitcoiny. Druhý soukromý klíč je obdobou hesla k účtu a slouží k manipulaci se svázanou adresou. Jen držitel soukromého klíče může bitcoinovou transakci podepsat a odeslat mezi uživateli. [17] Spolu s asymetrickou kryptografií je užito hashovací jednocestné

[17] TESAŘ, Jaromír. Základy kryptografie a její využití pro kryptoměny. Btctip.cz [online]. 21.1.2021 [cit. 2022-03-08]. Dostupné z: https://btctip.cz/zaklady-kryptografie-a-jeji-vyuziti-pro-kryptomeny/

funkce, která přemění jakékoli vstupní číslo o variabilní délce změnit ve výstup o konstantní délce, který můžeme chápat jako určitý otisk. V tomto případě jde o 56bitový SHA-2, také známý jako SHA-256.[18]

2.3. Blockchain a dvojitá útrata

Blockchain je primárně technologií kryptoměn. Je to síť, kde uživatelé mohou provádět platby, zpracovávat je a ověřovat takové operace bez centrálního emitenta měny nebo clearingového centra. Technologie blockchain umožňuje lidem obchodovat pomocí kryptoměn a uzavírat a vynucovat chytré smlouvy.[19] Autorem blockchainu je Satoshi Nakamoto, který ho přivedl na svět kolem roku 2008, kdy ho představil ve svém článku „Bitcoin: A Peer-to-Peer Electronic Cash Systém“[20]. Ze samotného názvu článku plyne, že byl vyvinut pro bitcoin a jeho zabezpečení. Nakamotovi se podařilo vyřešit problém dvojí útraty. Posléze tento systém přejaly i další tvůrci altcoinů. Nakamoto ve svém systému pospojoval několik vzájemně kooperujících disciplín, jehož hlavním úkolem je zajistit zabezpečení virtuálních měn, přičemž k tomuto účelu užil asymetrickou kryptografii a zejména její hashovací funkce spolu s neměnným kryptografickým podpisem[21]. Termín blockchain se do češtiny nepřekládá a používá se jeho

---

[18] Co je kryptografická funkce hash? Ssl.com [online]. 10.11.2015 [cit. 2022-03-08]. Dostupné z: https://www.ssl.com/cs/Nej%C4%8Dast%C4%9Bj%C5%A1%C3%AD-dotazy/co-je-kryptografick%C3%A1-hashovac%C3%AD-funkce/ash

[19] *Služba Peer-to-Peer (P2P)* [online]. In: HAYES, ADAM. [cit. 2021-12-19]. Dostupné z: https://www.investopedia.com/terms/p/peertopeer-p2p-service.asp

[20] NAKAMOTO, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System. *Microstrategy.com* [online]. 2009, 2009 [cit. 2022-02-15]. Dostupné z: https://www.microstrategy.com/en/bitcoin/documents/bitcoin-a-peer-to-peer-electronic-cash-system.

[21] Hash je kryptografickým podpisem.

původní anglický název. Jedná se o řetězec bloků sepsaného do protokolu, který je distribuován uživateli bitcoinu pomocí Distributed Ledger Technology (DLT) a síťovým systémem na principu Peer To Peer (P2P). Díky rozšíření blockchainu mezi jeho uživatele, se stal veřejně přístupnou databází, v dnešní době o velikosti více jak 380 gigabytů[22], která je provozována prostřednictvím jednotlivých účastníků na uzlech (nodech)[23].

Blockchain nepřinesl jen ochranu před dvojitou útratou, ale také další funkce jako ochranu před kopírováním bitcoinu a souběžně s tímto systémem přenesl i větší důvěru v provozu na P2P síti a samozřejmě i schopnost vlastního ověřování transakce bez přítomnosti centrální autority.

Problém dvojité útraty je reálná obavy z opakovaného placení stejným bitcoinem, k takovému placení by mohlo dojít buď v rychlém časovém sledu, kdy by ještě nedošlo k zaúčtování bitcoinu a převedení na nového vlastníka nebo při úmyslném kopírování dat obsahující bitcoin. V případě existence důvěryhodné centrální autority je takový problém potlačen, ale centralizace a princip fungování takového přístupu je protikladem požadavku decentralizace. Navíc v případě existence centrální autority se takový systém jeví jako snáze napadnutelný rukou hackera v jednom bodě. Satochi Nakamoto problém dvojité platby vyřešil veřejnou účetní knihou, kterou je blockchain. Prvním zápisem byl takzvaný genesis block, na který se těžbou nabalují další bloky a postupně vytváří blockchain. Ten vzniká těžbou, kterou je vlastně ověření proběhlé transakce pomocí poskytnutého výpočetního výkonu. Těžbou se dochází k přiřazení hashe, neboli zašifrovaného čísla obsahujícího časové razítko, informace z předchozího bloku a transakční data. Vše dohromady je zašifrováno pomocí bezpečnostního protokolu, jako je algoritmus SHA-256, který používají bitcoiny. Díky takovému postupu při ověření každé nové operace dochází k rozšiřování blockchainu. Motivací k provozování blockchainu a poskytnutí výpočetního výkonu se tak stává okruh osob, které

---

[22] Size of the Bitcoin blockchain from January 2009 to February 7, 2022. *Statista.com* [online]. 2022, 24.2.2022 [cit. 2022-02-15]. Dostupné z: https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/

[23] Nod, označení pro uzel zajišťující ověření platnosti transakce, nod má několik úrovní od peněženky s malou částí blockchainu, k full nodu s plným obsahem až po mining nod, který provádí potvrzení transakce.

podporují technologii blockchainu a zároveň jsou za takovou službu ohodnoceni vytěženými bitcoiny. Ověření kryptoměnových transakcí nějakou dobu trvá, protože proces zahrnuje náhodný výběr čísel k vyřešení složitého úkolu, který je limitován dostupným výpočetním výkonem, proto je nesmírně obtížné duplikovat nebo falšovat blockchainm jelikož by takový operace vyžadovala obdobný výkon v reálném čase, kdy dochází k zápisu nového bloku. K takové události by mohlo dojít s příchodem nových kvantových počítačů. Nicméně k dvojité platbě skutečně došlo 17.9.2018, chyba nesoucí označení CVE-2018–17144 zůstala evidována rok a odstraněna byla až po aktualizaci klientů a to s varováním před hrozícími DoS útoky vyřazující nody z provozu.

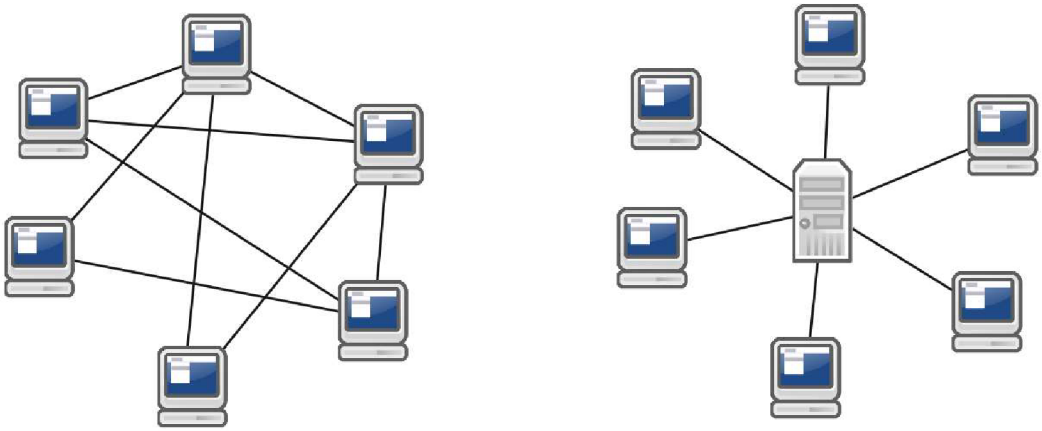
2.4. Peer to peer

Peer-to-peer, nebo také její zkrácené označení P2P, které bylo odvozeno z počátečních písmen a foneticky obdobně znějícího anglického slova „to“ a číslovky dvě. Peer to peer je doslovně přeložené jako rovný s rovným, ale její zkrácená podoba je obecněji vykládáno také jako person to person, které tak jednodušeji vysvětluje vztah mezi oběma účastníky v daném procesu. P2P je označením typu symetrických počítačových sítí, ve které spolu komunikují přímo jednotliví klienti. Typické je pro tento druh sítí označení rovný s rovným. Opakem P2P je běžnější uživatelská asymetrická síť klient-server, ve které jednotliví klienti komunikují skrze centrální server či servery, díky čemuž dochází ke spojení s cílovým klientem. Nevýhodou této symetrické sítě tak bývá počáteční obtížnost při navázání spojení.

Klíčové vlastnosti

- *Služba peer-to-peer je platforma, která přímo spojuje strany s transakcí bez prostředníka třetí strany.*
- *Služby peer-to-peer využívají technologii k překonání transakčních nákladů spojených s důvěrou, prosazováním a informačními asymetriemi, které se tradičně řeší používáním důvěryhodných třetích stran.*

- *Peer-to-peer platformy nabízejí svým uživatelům služby, jako je zpracování plateb, informace o kupujících a prodejcích a zajištění kvality.*[24]



Znázornění připojení několika uživatelů v peer to peer síti (vlevo), oproti klasické síti s centrálním serverem (vpravo). [25]

Moderní koncept peer-to-peer zpopularizovaly systémy pro sdílení souborů, jako je aplikace pro sdílení hudby Napster, nebo Kazaa, která se objevila v roce 1999. Síť peer-to-peer umožnilo milionům uživatelů sdílení velkého množství souborů. Výhodou sítě P2P je rozmělnění výpadku jednoho připojeného zařízení mezi ostatní uživatele sítě cestou internetu, možnost přímého připojení, vytváření skupin, vzájemná spolupráce nebo podílení při zbudování virtuálního superpočítače. P2P model uspořádání sítě se liší od modelu klient-server, kde je komunikace přímo orientovaná na centrální server. Nevýhodou je prodleva při čekání při navázání spojení.

---

[24] *Služba Peer-to-Peer (P2P)* [online]. In: HAYES, ADAM. [cit. 2021-12-19]. Dostupné z: https://www.investopedia.com/terms/p/peertopeer-p2p-service.asp

[25] *Peer-to-peer (P2P) sítě* [online]. In: DURČÁK, Pavel. [cit. 2021-12-19]. Dostupné z: https://www.napocitaci.cz/33/peer-to-peer-p2p-site-uniqueidgOkE4NvrWuNY54vrLeM679zvh6YhHnhkpLpGVMy1prA/

Dnes se P2P služby posunuly za hranice čistě internetových služeb, i když jsou většinou považovány alespoň za internetové. Služby peer-to-peer zahrnují činnosti, které sahají od jednoduchého nákupu a prodeje až po ty, které jsou považovány za součást ekonomiky sdílení. Některé peer-to-peer služby dokonce vůbec nezahrnují placenou transakci ze strany uživatelů, ale spojují jednotlivce, aby pracovali na společných projektech, sdíleli informace nebo komunikovali bez přímého zprostředkování. Současně takové služby nabízejí i zpoplatněnou variantu, která pak uživateli poskytuje výhody v rychlejším odbavení. Případně mohou být P2P provozovány jako bezplatné pro koncové uživatele, přičemž svůj provoz financují prodejem reklamního prostoru vizualizovaných v podobě banerů v prostředí aukční služby.

Nevýhodou, nebo dokonce rizikem služby P2P je v případě odpojení jedné ze stran. Při spojení tak hrozí, že poskytovatel služby nemusí dodat službu, nebo že nabízená služba nebude mít očekávanou kvalitu, kupující nezaplatí, nebo že jeden nebo obě strany by mohly být schopny využít asymetrické informace. Toto mimořádné riziko představuje dodatečné transakční náklady k P2P transakci. Často jsou P2P služby vytvářeny se záměrem usnadnit tyto transakce a snížit riziko pro kupujícího i prodávajícího. Kupující, prodávající nebo oba mohou zaplatit náklady na službu nebo služba může být nabízena zdarma a je generovat příjmy jiným způsobem.

2.5. Swapovací služby

Ke směně fiat oběživa za virtuální měnu je možné v českém prostředí užít specializovaných směnáren. Na našem českém trhu je lze nalézt od roku 2013, kdy se objevila jako první směnárna Simplecoin. S přibývající oblibou bitcoinu se přidaly i další, jako Anycoin, Bitbeli, Virtual Property, Bitstock, Finex, Loclabitcoins, CCshop. Směnárny se od sebe liší samozřejmě nabízeným kurzem, poplatky, minimální výší směny, preferovaným bankovním spojením, možností založení

vlastní virtuální peněženky a samozřejmě nabídkou virtuálních měn, kterými obchodují, či zda dokonce přijímají českou korunu. Rychlost směny je odvislá například od použití bankovního spojení preferovaného směnárnou, nebo zda se jedná o nového či již registrovaného klienta. Nabytí kryptoměny tedy může proběhnout téměř okamžitě nebo do několika hodin. Směnárny jsou samozřejmě obchodníci, takže v případě volby směnárny je nutné vybírat podle kurzu a poplatků za službu. Oproti směnárnám konvenčních měn, odkud si vyměněné prostředky odnesete v drtivé většině případů okamžitě je u směnáren krypta dobré znát i pověst zvolené směnárny, jelikož avizovaná délka převodu neprobíhá vždy okamžitě, nebo v případě, že se klienta rozhodl využít virtuální peněženku u oslovené směnárny. Znát pověst takové směnárny by mělo být automatické, aby bylo omezeno riziko ztráty kryptoměn. Jako příklad, kdy došlo k hackerskému útoku na směnárnu lze zmínit směnárnu CCshop, u které došlo v prosinci 2017 k útoku a vykradení několika peněženek. Rozsah útoku není znám a směnárna směrem ke klientům vydala zprávu, že vzniklou škodu uhradí. Evidentně se jednalo o nedostatečně zabezpečený systém směnárny.[26]

Další místem k pořízení virtuálních měn jsou krypto burzy. Burzy bývají oproti směnárnám levnějším způsobem, opět zde však platí, že se vyplatí znát pověst burzy a její hodnocení, kterým lze částečně eliminovat rizika obchodování. Burzy jsou pak vhodné pro klasické obchodování ve větších částkách a opakovaných objemech. Oproti směnárnám jsou uživatelé na burzách registrováni i při nižších finančních operacích, zpravidla se k tomuto kroku užívá dvou dokladů k prokázání totožnosti, přičemž dochází i k ověření klienta, takže jeho přístup na burzu a k pořízení virtuální měny není oproti směnárně okamžitý. Jako českou burzu lze v našem prostředí uvést burzu CoinMate, která je založena dvěma našinci, ačkoli její sídlo je v Anglii, burza pak nabízí dvě uživatelská prostředí, jedno se všemi burzovními nástroji a prostředím grafů sledující vývoj trhu a druhé zjednodušené

---

[26] Recenze ccShop. *Investplus.cz* [online]. 2018 [cit. 2022-02-17]. Dostupné z: https://investplus.cz/investice/nevyhodny-ccshop-recenze-zkusenosti-diskuze-navod-reference-je-ccshop-cz-podvod/

orientující se na směnárenské služby s jasně definovaným kurzem. Jako nejznámější zástupce světových burz lze uvést eToro, Binance, Libertex.

Mimo směnárny a kryptoměnové burzy se v České republice rozšířili i bitcoinové automaty a k počátku roku 2022 se jich zde nacházelo 72, z nichž více jak polovina (45) je na území Prahy.[27] Bitcoinové automaty jsou nejrychlejší a nejsnaděnjší cestou k pořízení bitcoinů, ale i dalších kryptoměn, které automaty nabízí. Velkou nevýhodou je však vysoký poplatek za směnu, který činí v případě bitcoinu 4,1% až 7,4% z dané částky nebo pevný poplatek (5,- Eur v síti bitcoinmat.sk) . V případě jiných kryptoměn dosahuje poplatek i 10% a v případě Dogecoin může činit dokonce i neuvěřitelných 21% z transakce. Směna je však jednoduchá, postačí mít u sebe kryptopeněženku nebo QR kód, případně si peněženku založit v automatu, pak stačí jen hotovost a Bitcoiny jsou odeslány téměř okamžitě. Rychlost převodu je však vždy odvislá od poplatku minerovi a požadavku na rychlost převodu, tím se může převod protáhnout i na jednu hodinu. Uskutečnění převod je možné zjistit z vyžádané SMS zprávy nebo ve virtuální peněžence. Automaty fungují obousměrně, k výměně za konvenční měnu a výběru postačí vygenerovat QR kód, vyfotit ho do své peněženky a potvrdit, peníze jsou poté odeslány. Podle toho jak na výběr spěcháte, bude odvislý poplatek za zápis do blockchainu a odměna minera. Anonymní použití Bitcoin automatu je závislé na nastaveném limitu provozovatelem. Limit je zhruba 1.000,- Eur (u nás v rozmezí 24 až 25 tisíc korun). Při takové transakci nexistuje žádná kontrola nebo registrace. V případě směny nad limit je třeba provést ověření osoby předložením průkazu. [28]

Jistou alternativou je online tržiště LocalBitcoins, kde je však možné provést směnu pouze bitcoinů. Směna probíhá dle podmínek a pod dohledem zprostředkovatele pomocí svěřeneckého účtu, ze kterého jsou bitcoiny uvolněny

---

[27] Total number of Bitcoin ATMs: Tellers in Czech Republic: 72. Coinatmradar.com [online]. [cit. 2022-03-07]. Dostupné z: https://coinatmradar.com/country/57/bitcoin-atm-czech-republic/

[28] STROUKAL, Dominik a Jan SKALICKÝ. Bitcoin a jiné kryptopeníze budoucnosti. 3. rozšířené vydání. Praha 7, U Průhonu 22: GRADA, 2021. ISBN 978-80-271-4255-2.

po uskutečněné platbě. Volba platebního způsobu, záleží si domluvě mezi prodejcem a kupícím. Tržiště je defacto inzertním portálem jako americký Craiglist nebo naše Aukro, provozovatel je jen prostředníkem a služba probíhá ve smyslu peer to peer. Na stránkách je uveřejňováno množství inzerátů s jednotlivými nabídkami. Na tržišti mohou inzerovat jen registrovaní uživatelé, ale ani to není zárukou bezpečného obchodu. Stejně jako na inzertních portálech nechává provozovatel celý průběh na samotných lidech, do dění vstupuje jen v případě vygenerování problému. Poplatek za služby jde z kapsy prodávajícího ve výši 1% za uskutečněný obchod, přičemž je na něm jaký kurz bitcoinu si zvolí. Tržiště LocalBitcoins s doménou localbitsoins.com existuje od roku 2012 a je registrováno ve Finsku, v současné době má přes jeden milion uživatelů a zaměřuje se jen na bitcoiny.[29]

2.6. Pračky bitcoinů

Jako skutečně nebezpečné lze vidět pračky bitcoinů takzvané mixéry (tumblery), které fungují na principu redistribuce pořízených bitcoinů mezi množství peněženek, čímž dojde k zamaskování původu pořízených bitcoinů, neexistuje však záruka, že uživatel takové služby neodstane bitcoin pocházející z jiného pochybného obchodu. Použití mixéru nabízí pro legalizaci výnosů z trestné činnosti jednu z možností, jak bitcoiny vyprat, není však rozhodně zárukou, že dostane bitcoiny bezpečné a s ohledem na osoby, které takové služby užívají se dá předpokládat, že jde o službu vysoce rizikovou. Uživatelé takových služeb se nerekrutují z řad fandů moderních technologií a odborníků na kryptoměny v pozitivním slova smyslu, ale spíše z řad kriminálníků a osob, kteří zprostředkovávají praní špinavých „peněz“. Jedním z rizik mixéru je i důvěryhodnost osoby, která takovou službu poskytuje. Nejenom, že zde vzniká

[29] About LocalBitcoins. LocalBitoins.com [online]. 2022 [cit. 2022-02-17]. Dostupné z: https://localbitcoins.com/about

riziko získání bitcoinů s mnohem závadnějším původem, ale existuje tu i vysoká obava z toho, zda zašle promíchané bitcoiny zpět.

2.7. Jiné formy směny a anonymita

Kryptoměny je možné získat i mnohem jednodušším způsobem. Koupí od známého, v kavárně, jako odměnu za provedenou službu, za prodej pizzy nebo třeba přes inzerát, možností je skutečně mnoho. Takovým téměř anonymním způsobem byl v minulosti i již výše uvedený LocalBitcoins, který prvotně jen zajišťoval virtuální prostor inzerci zajišťující prodej a koupi bitcoinu. V současnosti však provozuje důvěryhodnější formu provozu, kde je podmínkou uskutečnění obchodu skrze svěřenecký účet, čímž obchody na LocalBitcoins ztratily punc naprosté anonymity. Všechny směny v hotovosti by však měly dodržovat zákonné pravidla a hranici 270.000,- Kč, která limituje bezhotovostní platby. V případě směnáren i burz lze předpokládat, že k dodržování takových pravidel a hranic dojde, skutečným současným rizikem, které lze jen těžko sledovat jsou nyní právě poslední zmíněné bitcoin automaty, úplná anonymita omezena denní částkou 1.000,- Eur nebo jejího ekvivalentu 25.000,- Kč. V případě překročení povolené denní hranice je nutné použít jeden z dokladů totožnosti. Automaty Za předpokladu, že osoba provádějící výběr nebude chtít zanechat na kameře svou skutečnou podobu, může k takovému jednání použít masku, zakrytí tváře nebo bílého koně. Po provedení takové operace se taková směna stane téměř nedohledatelnou a nepostižitelnou. I když je v současné době nekontrolované prostředí ATM vysoce rizikové, lze takový způsob cestou bílého koně uskutečnit i ve směnárně.

Někteří lidé srovnávají P2P burzu s tržišti, jako je Craigslist nebo Facebook Marketplace, protože P2P burzy spojují kupující a prodávající kryptoměny. Kupující a prodávající mohou procházet kryptoreklamy nebo zveřejňovat vlastní reklamy. P2P burzy mohou také poskytnout vrstvu ochrany pro všechny účastníky transakce, a to implementací systému zpětné vazby nebo hodnocení. Představte

si toto: Na Twitteru potkáte někoho, kdo má zájem o koupi bitcoinů – a náhodou máte nějaké bitcoiny na prodej. Twitter není P2P platforma, takže je těžké navázat důvěru. Co se stane, když kupující získá bitcoiny, ale neodešle platbu? Co se stane, když kupující zašle nižší částku platby, než očekával? Podvod je největším rizikem provádění P2P obchodů bez burzy.

Binance P2P může chránit jak kupující, tak prodávající, aby ochránila transakce a snížila riziko podvodu. Kromě veřejného ratingového systému používá Binance P2P k zabezpečení kryptoměn úschovu, dokud obě strany transakci nepotvrdí. Pokud například prodáváte bitcoiny za fiat peníze, Binance si váš bitcoin uloží do úschovy. Jakmile odešlete bitcoiny a transakce bude potvrzena, Binance následně připíše peníze vám a kupujícímu, čímž zajistí bezpečnou a zabezpečenou transakci. Pokud některá ze stran není s transakcí spokojena, může podat odvolání k vyřešení problému mezi protistranami nebo požádat o zásah zákaznické podpory Binance.

2.8. Krypto peněženky

K ukládání kryptoměn stejně jako u tradičních měn je třeba peněženky. Jelikož bitcoin je defacto geniální kód, jehož existence je doložena jen jeho stopou v blockchainu je k jeho uložení třeba softwarová nebo hardwarová peněženka. Možností je vícero. Kryptoměny je možné nechat uložené přímo na vygenerované peněžence ve směnárně nebo na burze kde byla měna pořízena, toto řešení je však vhodné pro menší částky, aby bylo eliminováno riziko možného hacknutí burzy a ztráty krypta. Taková peněženka nic nestojí, je možné jich vygenerovat jakékoli množství, jedná se o adresu, kam lze peníze zasílat. Peněženku je možné vygenerovat přímo na burze nebo v bitcoin automatu, kde je měna pořizována. Je možné využít i softwarovou peněženku typu Hodly, Electrum nebo Bitcoin Knots, softwarových peněženek je mnoho. Jedná se o software, který postačí nainstalovat na počítač nebo telefon a vygenerovat novou peněženku. Některé nabízí i funkci nákupu dalších kryptoměn. Ideálním způsobem uložení je však mít je odděleně od zařízení s přístupem k internetu na externím disku nebo flash kartě,

vhodné je však zajistit takové úložiště kódem nebo na bezpečném místě. Ideálním je však pořídit si speciální zabezpečenou hardwarovou peněženku, kterou lze pořídit v řádek několika tisíc korun. Takovou nabízí například česká značka SatoshiLab, která má svůj Trezor, jedná se vlastně o speciální zařízení připomínající flashdisk. K počítači se pak připojuje, když je potřeba provést platbu. Opět i výrobců hardwarových peněženek je mnoho, je možné použít výrobky značek Ledger Nano, MetaMask a dalších. Při pořízení peněženky je však důležité uložit si bezpečnostní frázy, takzvaný seed, který slouží při ztrátě peněženky k obnově jejího obsahu. Tento seed je vhodné opět uchovávat na bezpečném místě mimo telefon nebo počítač, ideálně je kus papíru a poctivý trezor. Seed je zpravidla řetězcem 12 nebo 24 slov.

2.9. ICO, NFT, tokenizace

Technologie blockchainu, tedy veřejná účetní kniha nepřinesla jen bitcoiny, které byly jmenovatelem rychlého a pohádkového zbohatnutí. Blockchain tedy stavěl na svém kreditu veřejnosti a bezpečnosti. Nejprve dovolil rozmach dalších kryptoměn, které vcelku úspěšně kopírovaly stejný a úspěšný vývoj jako u bitcoinu. Rychlý zisk tak přilákal nové investory a zájemce moderních technologií. Ne každý je však programátor, ekonom a matematik v jednom a tak na přelomu let 2017 a 2018 vznikl projekt ICO, což je zkratka pro Initial Coin Offering, v překladu prvotní nabídka mincí. Jedná se o proces, kdy jsou prodávány nové mince dané kryptoměny, a to zpravidla ještě před tím, než tato kryptoměna vstoupí na burzu. [30] Šlo tedy vlastně o startup, který nabízel podíl při vzniku nových kryptoměn, který vycházel vlastně z předpokladu, že je nejlepší je vytvořit vlastní kryptoměnu či být alespoň u zrodu nové „měny“ přímo na počátku. Ne každý tvůrce však dokázal takovou měnu úspěšně nabídnout na již tak naplněném trhu

[30] Co to jsou ICOs?. Cryptokingdom.tech [online]. 1.3.2019 [cit. 2022-01-16]. Dostupné z: https://cryptokingdom.tech/cs/magazin/zacatecnik/co-to-jsou-icos

kryptoměn a zalistovat ji na burze. Úspěchu dosáhlo zhruba 7 z 10 kryptoměn. Taková nabídka tak trochu vykazovala prvky pyramidových podvodů, jelikož zisky končily většinou jen v kapsách tvůrců a někdy i částečně i v peněženkách prvních investorů, kteří získali svou odměnu jako součást marketingové politiky k nalákání nových investorů, kteří do startupu jako investice přinesly své skutečně hodnotné bitcoiny. Způsob a řízení platformy initial coin offering vedl v roce 2017 k jeho zákazu v Číně a Jižní Korei. [31]

Dalším takovým počinem se jeví i NFT, což je zkratka pro Non Fungible Token, tedy nezaměnitelný token. Oproti bitcoinu, který je plně zaměnitelný, jelikož jeho výměnou za jiný bitcoin zůstává jeho hodnota v ideálním případě bez těžebního poplatku neměnná. Oproti tomu je získání nezaměnitelného tokenu jako digitální informace v podobě obrázku, textu či oblíbeného příspěvku na twiteru nezaměnitelnou digitální věcí, nebo spíše nezaměnitelným zápisem v blockchainu, což je spíše zápisem digitálních vlastnických práv věci, která je veřejně přístupná na internetu.[32] Smysl vlastnictví takové digitální informace by pak byl například v případě vlastnictví fotografie či videa, které by bylo v digitálním světě veřejně dostupné ve své neúplné, zmenšené nebo kvalitativně méně hodnotné podobě, která by dokázala spojit jejího majitele s potencionálním zájemcem. Tokenizované obrázky pak lze nalézt na marketplace crypto.com/nft, Vlastnictví takové věci se zdá nelogické, nicméně takové věci lze nalézt i v konvečním světě. Umělecká díla jako je například obraz Mony Lisy, která je vystavená v galerii, je veřejně dostupná a stále existuje její obliba a potřeba ji vidět v její skutečné podobě. Stejně tak existují její napodobeniny a její podoba je všeobecně známá. Shodný prvek tak můžeme nalézt i u produktů NFT.

---

[31] CHOUDHURY, Saheli Roy. TECH China bans companies from raising money through ICOs, asks local regulators to inspect 60 major platforms. Cnbc.com [online]. 4.9.2017 [cit. 2022-01-16]. Dostupné z: https://www.cnbc.com/2017/09/04/chinese-icos-china-bans-fundraising-through-initial-coin-offerings-report-says.html

[32] STROUKAL, Dominik. Jedinečné tokeny: bublina, či inovace?. E15.cz [online]. 20.7.2021 [cit. 2022-01-15]. Dostupné z: https://www.e15.cz/nazory/dominik-stroukal-jedinecne-tokeny-bublina-ci-inovace-1382235

ICO i NFT přinesly na světlo světa i další vývojový pohled na věc, kterým je tokenizace. Tokenizace nabízí úplně nové možnosti, jak přistupovat k majetku. V současné době se přechod na tokenizaci a blockchain už nejeví jako nereálná věc, ale spíše jako budoucnost evidence vlastnictví. Tokenizovat jak pak možné cokoli, skutečné peníze, akcie, nemovitosti, lístky do kina, vše na co lze pomyslet. Dokladem o vlastnictví je pak digitální stopa v blockchainu. Smysl samotné tokenizace je v samotné decentralizaci, tedy vynechání prostředníka, zpostředkovatele, urychlení a zpřístupnění takových nabídek cestou internetu v jakoukoli dobu. Takto by skutečně mohl budoucí svět brzy vypadat, došlo by ke snížení poplatků za vyřízení hypotéky, nákupu nemovitosti. Nákup tokenů je pak možné provést za fiat měnu nebo bitcoiny. Bitcoiny jsou pseudoanonymní, jelikož existuje jejich veřejná digitální účetní evidence v blocku a je možné je vysledovat k jejich vlastníkovi. Obdobným způsob anonymity poskytují i tokenizace, ICO a NFT. Díky rychle narůstajícímu množství měn blockchainů je taková situace velmi nepřehledná. K tomuto nepřispívá ani rychle se vyvíjející se trh burz v síti internetu, který může být dostupný z různých míst planety. I když je možné, že by se tato spojení dala vypátrat, prostředí kryptoměn je pro zločince výhodné, protože transakce se ve srovnání s tradičním finančním systémem neuvěřitelně rychle pohybují. K tomu nepřispívá ani skutečnost, že nové společnosti a burzy vznikají i zanikají rychleji, než je tomu u bankovních domů, které je možné vysledovat.

Jako příklad praní špinavých peněz pomocí NFT lze uvést jeden způsob. Spekulant Karel je fanda tokenizace a pořídí si na vlně popularity obrázek na internetu, o kterém se domnívá, že jeho cena poroste podobným způsobem jako bitcoin. Sleduje vývoj trhu a rozhodne se na obrázku vydělat, mohl by ho prodat na NFT burze, kde ho před časem pořídil, ale rozhodne se vyhledat rizikovější burzu s lepší nabídkou, o které ví, že obchází regulace trhu a nespolupracuje s OČTŘ. O této burze se dozvěděl i špinavý Max, který právě wishingem získal menší část bitcoinu, kterou převedl do své peněženky a chtěl by kryptoměnu vyprat. Peněženku vytvořil jen k tomuto jedinému činu a je ochotný koupit cokoli, aby se bitcoinu zbavil. Vyjde vstříc vyšší ceně a získá NFT obrázek, jehož skutečná cena je o něco nižší, což mu nevadí, jelikož se mu podařilo bitcoin prodat a v okamžiku, kdy prodá i obrázek NFT bude jeho stopa téměř nedohledatelná.

Příklad nemá vykreslit NFT jako něco co bylo vytvořeno k praní špinavých peněz, jde jen o to ukázat na trhlinu, která toto umožňuje. Ne, že by obdobný způsob nebyl možný realizovat i pomocí konvenční měny nebo směnným způsobem. Pouze upozorňuje na rychle reagující trh a vývoj blockchainu, který se nevyskytuje jen na regionálním trhu, ale v globálním světě internetu, což samo osobě dosti ztěžuje boj proti takovém jednání.

3. Aplikace trestní odpovědnosti a dalších povinností

Aplikace trestního práva vůči kybernetické kriminalitě není samostatně vymezena, tedy neexistují speciální trestné činy uvedené v jednotlivých hlavách či skutkových podstatách trestního zákoníku, které by postihovaly přímo virtuální prostředí a jeho aspekty. Při uplatňování trestního práva je u takových útoků je vždy nutné nacházet jednotlivé znaky skutkových podstat, které lze nalézt ve zvláštní částí trestního zákoníku (dále jen TZ). Užití TZ je pak možné vždy při nalezení takové míry společenské škodlivosti, která v rámci uplatnění subsidiarity trestní represe nedovoluje užít mírnějšího předpisu. V případě naplnění zásady subsidiarity ve prospěch trestního práva lze kyberkriminalitu postihovat ve dvou odvětvích trestního práva, a to trestního práva hmotného a trestního práva procesního. Trestní právo hmotné nám pak ve své zvláštní části vyjmenovává trestné činy, které lze v případě nalezení přiléhavé skutkové podstaty užít. Zůstává však otázka působnosti trestního práva ve spojitosti s kybernetickým útokem, to je spojeno zejména se specifikací místa útoku. TZ však na takovou problematiku pamatuje a lze využít zejm. zásady v něm vymezené, a to konkrétně zásady teritoriality, registrace, personality, ochrany a univerzality a subsidiární zásadu univerzality. Z hlediska vyjmenovaných zásad a z podstaty samotné kyberkriminality, kterou lze zejména díky internetu uskutečnit z jakéhokoliv místa na planetě, pak je ve většině případů posoudit dle zásady teritoriality podle ust. § 4 TZ a to dle místa následku *„ať již zcela nebo z části*“.

Ačkoli za veškeré jednání ve virtuálním světě nelze označit jako

kyberkriminalitu a nelze toto jednání posoudit v trestněprávní rovině či v rovině správní práva, lze konstatovat, že *„v souvislosti s provozem informačních systémů, výpočetní techniky či komunikačních prostředků dochází k celé řadě jednání, která jsou jistě nežádoucí, ale nejsou postižitelná prostředky trestního práva ani prostředky správního práva trestního, přestože mohou být pro společnost značně nebezpečná. Taková jednání apriori nemohou být kvalifikována jako počítačová, informační či jakákoliv jiná kriminality – nejsou totiž kriminalitou vůbec.“* [33] Uvedené však nevylučuje občanskoprávní či správněprávní postih takového jednání.

Vymezení kryptoměn v souvislosti se stanoviskem ČNB, která kryptoměny nepovažuje za konvenční měny, shledat shodu v občanským zákoníkem, v něm lze tedy kryptoměny označit za věc ve smyslu § 489, který uvádí *„Věc v právním smyslu (dále jen „věc“) je vše, co je rozdílné od osoby a slouží potřebě lidí.“* [34] V § 489 občanského zákoníku a ustanovení následujících lze díky takto široce pojaté definici věci nalézt shodu s vlastnostmi kryptoměn potažmo bitcoinu, které stejně jako věci, jsou rozdílné od osoby a slouží k potřebě lidí. Bitcoin, stejně jako jakákoli jiná kryptoměna, tyto podmínky bezesporu splňuje. Bitcoin totiž může sloužit k potřebě lidí ve dvou rovinách, a to jednak jako směnitelná hodnota, ale hlavně jako forma investice. Investory totiž láká nejenom volatilita, ale také do určité míry anonymita díky decentralizaci blockchainu. Obecně lze tedy říct, že Bitcoin je možné označit za věc v právním smyslu. [35] Po vymezení kryptoměn v občanskoprávním formátu, které virtuální měny označilo coby věc i investiční aktivum, je tedy možné na kryptoměny hledět jako na investiční nástroj a předmět možného zisku a tím pádem na něj lze uplatňovat i daň z příjmu. V budoucnu lze

---

[33] KOLOUCH, Jan a Petr VOLEVECKÝ. *Trestněprávní ochrana před kybernetickou kriminalitou*. Praha: Policejní akademie České republiky v Praze, 2013, s. 11, [cit. 2022-2-6]. ISBN 9788072514021.

[34] *Zák. 89/2012 Sb. Občanský zákoník* [online]. Beck, 2012 [online], [cit. 2022-2-6]. Dostupné z: https://www.beck-online.cz/bo/chapterview-document.seam?documentId=onrf6mrqgezf6obzfu4a

[35] Kryptoměny a občanské právo [online]. Beck, 2020 [online], [cit. 2022-2-6]. Dostupné z: Https://www.beck-online.cz/bo/chapterview-document.seam?documentId=nrptembsgbpxe4dul4zdcx3tl4zdc&groupIndex=0&rowIndex=0

předjímat, že se vlastnictví kryptoměn stane i předmětem dědického řízení.

Na základě podřazení kryptoměn pod investiční aktivum a dle občanského zákoníku jako věc, se tedy při návratu k trestně právní rovině a trestnímu zákoníku nabízí trestnou činnost spojenou s kryptoměnami posuzovat jako majetkovou trestnou činnost, kdy se jako nejvíce přiléhavé nabízí trestné činy podvod podle § 209 tr. zákoníku, krádež podle § 205 tr. zákoníku, legalizace výnosů z trestné činnosti podle §§ 216, 217 tr. zákoníku, zkrácení daně, poplatku a podobné povinné platby podle § 240 tr. zákoníku a další trestné činy spojené s majetkovou trestnou činností. Nabízí se však i hůře uchopitelné alternativy útoků a to DDoS útoky, které blokují určitou činnost, za něž útočníci požadují výkupné, zde se pak nabízí užití skutkových podstat vydírání podle § 175 tr. zákoníku, či obecné ohrožení podle 272 tr. zákoníku, v případech kdy k takovému útoku byl ohrožen chod nemocnice.

3.1. Legalizace výnosů z trestné činnosti

Slovní spojení legalizace výnosů z trestné činnosti již samo o sobě vyjadřuje označení činnosti orientující se nelegální manipulaci s nabytými statky, v praxi označované jako praní špinavých peněz nebo pod anglickým termínem money laundering, přičemž je anglický název a jeho zkratka AML (anti money laundering) užívána v právní praxi již od platnosti prvního zákona č. 61/1996 Sb. Vývoj definice legalizace výnosů z trestné činnosti zaznamenala od svého vzniku změn a v dnešní době tak pamatuje na širší okruh „ekonomických výhod“. Fenomén legalizace výnosů z trestné činnosti, který je v současné době nejzávažnější trestnou činností, je v současném pojetí zákona definován v následující podobě:

„Legalizací výnosů z trestné činnosti se pro účely tohoto zákona rozumí jednání sledující zakrytí nezákonného původu jakékoliv ekonomické výhody vyplývající z trestné činnosti s cílem vzbudit zdání, že jde o majetkový prospěch nabytý v souladu se zákonem;“

a) *v přeměně nebo převodu majetku s vědomím, že pochází z trestné činnosti, za účelem jeho utajení nebo zastření jeho původu nebo za účelem napomáhání osobě, která se účastní páchání takové činnosti, aby unikla právním důsledkům svého jednání,*

b) *v utajení nebo zastření skutečné povahy, zdroje, umístění, pohybu majetku nebo nakládání s ním nebo změny práv vztahujících se k majetku s vědomím, že tento majetek pochází z trestné činnosti,*

c) *v nabytí, držení, použití majetku nebo nakládání s ním s vědomím, že pochází z trestné činnosti, nebo*

d) *ve zločinném spolčení osob nebo jiné formě součinnosti za účelem jednání uvedeného pod písmeny a), b) nebo c).*[36]

Cílem legalizace výnosů je tedy zastření pravého původu statku, který byl nabyt trestným činem a jeho transformaci do podoby výnosu, díky kterému dojde k přerušení stopy mezi nelegálním nabytím a předestřeným výnosem, který má vzbudit domněnku legálního nabytí. Vzhledem k tomu, že slovní spojení legalizace výnosů z trestné činnosti jako jednu z hlavních podmínek evokuje, že musí jít o majetek nabytý trestnou činností, přičemž se nemusí jednat přímo o zcizenou věc, ale může jít i odměnu za násilnou trestnou činnost, za výtěžek z obchodu s lidmi, či z prodeje jiného produktu, například v podobě návykových látek tedy drog, či alkoholu, který je podřízen dalším regulatorním opatřením, či výnosu v podobě finančních prostředků nabytých krácením daně či neoprávněně získané daně z přidané hodnoty.

„Vlastní legalizace výnosů spočívá v jednání nebo v řadě jednání, jako jsou například převody, nákupy, směny, prodeje, ukrývání, převážení, fingování obchodních dokladů apod. Majetek je v konečném důsledku prezentován jako

---

[36] *Zák. 253/2008 Sb. o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu* [online]. Beck, 2018 [cit. 2021]. Dostupné z: Https://www.beck-online.cz/bo/document-view.seam?documentId=nnptembrhbpwe2zwgyxhgys7giydaoc7gi2tgx3qmyzq

legální příjem, nabytý například prodejem movitých či nemovitých věcí, podnikáním, výhrou, děděním či darem.“[37]

Tato činnost praní špinavých peněz, jejíž název byl odvozen od jednoho a nejznámějšího způsobu legalizace výnosů, který byl provozován v USA ve 30. letech dvacátého století, ve skutečných prádelnách v době hospodářské krize a prohibice. Legalizace byla prováděna v podnicích, které zločinecké organizace jako mafie, k těmto účelům provozovala a to tak, že smíchala legální výnosy s nelegálními, čímž uměle navyšovala zisk těchto prádelen. Takovéto finanční prostředky společně zdanila a naoko tak zlegalizovala výnosy z hazardu, prodeje drog a alkoholu. Takovýmto způsobem pak došlo k zahlazení stop od nelegálních zdrojů.

Od slovního spojení praní špinavých peněz a činností těchto prádelen byly odvozeny i další termíny označující etapy jednotlivých fází legalizace výnosů z trestné činnosti a to namáčení (nebo také placement), které ve finančním světě zahrnuje shromáždění a rozmístění finančních prostředků, které probíhá zpravidla vložením větších finančních částek v bankovkách nižších nominálních hodnot, díky čemuž dochází k obtížné identifikaci původu a dohledání jejich původu. Do roku 1970 neexistovalo opatření k dohledu nad takovými operacemi, proto bylo zavedeno opatření, kterým byly sledovány vklady hotovosti ve výši 10 tisíc dolarů a výše, čímž došlo k opatření na straně potřeby praní peněz, a to na rozmělnění částek pod tuto hranici, díky čemuž si tato operace vysloužila název tzv. „smurfing“ (šmoulení – členění transakcí pod 10 tisíc dolarů, aby tak bance nevznikla oznamovací povinnost nahlášení pro podezření z praní špinavých peněz). Ke vkladu rozdrobených částek pod 10 tisíc dolarů bylo užíváno různých míst, účtů a různé časové škále, kdy byly peníze vkládány na účet postupně. Díky nastoleným opatřením docházelo k obcházení systému a zdokonalování metod praní špinavých peněz, vždy v souladu s dodržováním vnitrostátních pravidel, kdy se

---

[37] *Zák. 253/2008 Sb. o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu* – komentář [online]. Beck, 2018 [cit. 2021]. Dostupné z: Https://www.beck-online.cz/bo/document-view.seam?documentId=nnptembrhbpwe2zwgyxhgys7giydaoc7gi2tgx3qmyzq [online]. [cit. 2021].

nakonec praní špinavých peněz přesunulo do gesce sofistikovaných a specializovaných organizací, které tyto postupy provádí v souladu s právními normami a v zemích s volnějšími pravidly a s nedostatečným finančním dohledem.

Druhým převzatým termínem je namydlení (nebo také layering), kdy při této fázi dochází především k zastření původu peněz. Peníze se oddělují od nezákonného zdroje. Dochází při ní k nákupu jiných zájmových komodit v podobě dobře zobchodovatelných nemovitostí, umělecký děl, zlata, stříbra, investičního majetku a jiných komodit ve všech jeho podobách. V tomto kroku pak dochází k přeměně tzv. špinavého vkladu a pořízení čistého kapitálu. Zpravidla bývá tento krok velmi složitý a nepřehledný, přičemž zločinci jsou ochotni vyčkat a obětovat operaci 20 a ž 25 procent ze svého výnosu.

Posledním třetím krokem při praní špinavých peněz je pak ždímání (nebo také integration), který je závěrečným krokem, kdy dochází k prodeji pořízeného majetku a jeho přeměny na finanční prostředky, které jsou po takto provedeném cyklu vyprané, zbavené stigmatu špinavých peněz, díky čemuž byl zastřen jejich původ a ve formě nezávadného, legálního a často zdaněného příjmu se vracejí jejich původnímu majiteli, který je dále používá k plnění svých potřeb či investic.[38]

3.2. Nástroj legalizace trestné činnosti

Součástí legalizace výnosů se trestné činnosti je nástroj k legalizaci výnosů z trestné činnosti. Ze samotného názvu je patrná spojitost mezi oběma termíny. Spojitost nevychází z podobnosti názvů, ale z určité tematické podobnosti a mnoha společných znaků, které díky jednání tedy legalizaci směřují k získání

---

[38] *Zák. 23/2008 Sb. o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu* [online]. FAÚ, 2019 [cit. 2021-4-8]. Dostupné z: file:///C:/Users/Petr/Desktop/Diplomka/PML%20aneb%20legalizace%20v%C3%BDnos%C5%AF%20z%20trestn%C3%A9%20%C4%8Dinnost%20FAU_cz.pdf

výnosů. Definice nástroje k legalizaci výnosů z trestné činnosti tak dle stanoviska Nejvyššího soudu zní následovně:

Věcí, která byla užita ke spáchání trestného činu, můžeme rozumět takovou věc, *„pokud za použití této věci nebo s jejíž pomocí pachatel naplnil skutkovou podstatu trestného činu. Zpravidla pomocí takové věci pachatel realizoval jednání jako obligatorní znak objektivní stránky trestného činu, i když tak nemusel učinit ve vztahu k celému rozsahu jednání, resp. určitá věc mu mohla jen umožnit nebo usnadnit vlastní realizaci jednání.“* [39]

Vzhledem ke spojitosti pojmů je vhodné vnímat pojmy legalizace, nástroj a výnos trestné činnosti vnímat i vysvětlovat pospolu. S ohledem na téma této práce, tedy užití kryptoměn jako nástroje k legalizaci výnosů z trestné činnosti se tak rozumí jednání, při kterém pachatel užil kryptoměny k zastření výnosu, tedy jeho přeměny na cokoli jiného, ať již užil virtuální měny k nákupu hmotné věci nebo k převodu na jinou virtuální měnu či NFT (nezaměnitelný token), ale třeba také k vylákání možné investice jako součást jeho podvodného jednání.

Při odhlédnutí k trestnímu zákoníku lze nástroj k trestné činnosti chápat jako věc obstaranou či přechovávanou s úmyslem spáchat určitou trestnou činnost nebo byla-li k jeho spáchání určena. Užití kryptoměn se v kontextu k jejich nehmotnému stavu rozumí převážně prostředí internetu.

3.3. Výnos z trestné činnosti

Výnosem z trestné činnosti lze podle dnešní právní teorie označit jev, kdy jím je *„jakákoliv ekonomická výhoda z jednání, které vykazuje znaky trestného činu“*[40], tak jak vyplývá z dnešní podoby zákona 253/2008 Sb. o některých opatřeních proti legalizaci výnosů z trestné činnosti a o změně a doplnění souvisejících zákonů.

---

[39] usnesení Nejvyššího soudu ze dne 8.9.2016, sp. zn. 6 Tdo 1179/2016

[40] *Zák. 61/1996 Sb. o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu* [online]. 1996 [cit. 2021-4-7]. Dostupné z: https://www.zakonyprolidi.cz/cs/1996-61

V této podobě byla definice stanovena již v předchozím znění zákona č. 61/1996 Sb. Teoretické znění výnosu bylo následně zapracováno do definice legalizace výnosů, přičemž došlo k širšímu vymezení, že výnosem je jakákoli ekonomická výhoda nabytá trestnou činností a nikoli jen příjem pocházející z trestné činnosti oproti původnímu znění. Výnos včetně výkladu znění tohoto zákona pamatuje na veškerou trestnou činnost, ze které plyne jakákoli ekonomická výhoda. Toto znění pak reaguje na konvenci OSN proti mezinárodnímu organizovanému zločinu konanému ve Vídni v červenci 2020, *„Výnosy z trestné činnosti znamenají jakýkoliv majetek jako výnos z trestného činu nebo majetek získaný v souvislosti s páchání trestného činu, a to přímo či nepřímo“*[41].

Z širšího vymezení výnosu, tak lze za výnos z trestné činnosti označit nejen přímé *výnosy z trestné činnosti, ale i všechny nepřímé užitky, včetně následných reinvestic či přeměněných přímých výnosů. Výnosy z trestné činnosti tak mohou zahrnovat jakýkoli majetek, včetně majetku, který byl zcela nebo zčásti přeměněn na jiný majetek, nebo pokud byl smíšen s majetkem nabytým zákonným způsobem, až do výše odhadované hodnoty smíšených výnosů. Výnosy z trestné činnosti mohou rovněž zahrnovat příjmy nebo jiný užitek pocházející z výnosů z trestné činnosti nebo z majetku, na nějž byly takové výnosy přeměněny nebo s nímž byly smíšeny.“*[42]

Výnos je třeba chápat jako dynamický fenomén, který vzniká, trvá a zaniká“[43]. Jeho vývoj a podoba se v průběhu existence mění dle vůle a potřeb jeho disponenta, který určuje jeho podobu podle fází, ve kterých v dané chvíli a do kterých se modifikuje, jelikož je vývoj od počátku lze vnímat ve třech intervalech

---

[41] SCHEINOST, Miroslav. *Konvence OSN a další dokumenty k organizovanému zločinu*. Praha: Institut pro kriminologii a sociální prevenci, 2001. Prameny (Institut pro kriminologii a sociální prevenci). ISBN 80-86008-91-6.

[42] *SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY 2014/42/EU* [online]. Brusel: Úředním věstníku Evropské unie, 2014 [cit. 2021-8-7]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=uriserv:OJ.L_.2014.127.01.0039.01.CES

[43] DVOŘÁK, Vratislav a David ZÁMEK. *Výnos z trestné činnosti a jeho modifikace* [online]. [cit. 2021-3-20]. Dostupné z: https://eur-lex.europa.eu/legalhttps://bezpecnostni-sbory.wbs.cz/clanky/6-2011/vynos_z_trestne_cinnosti_a_jeho_modifikace.pdf-content/CS/TXT/?uri=uriserv:OJ.L_.2014.127.01.0039.01.CES

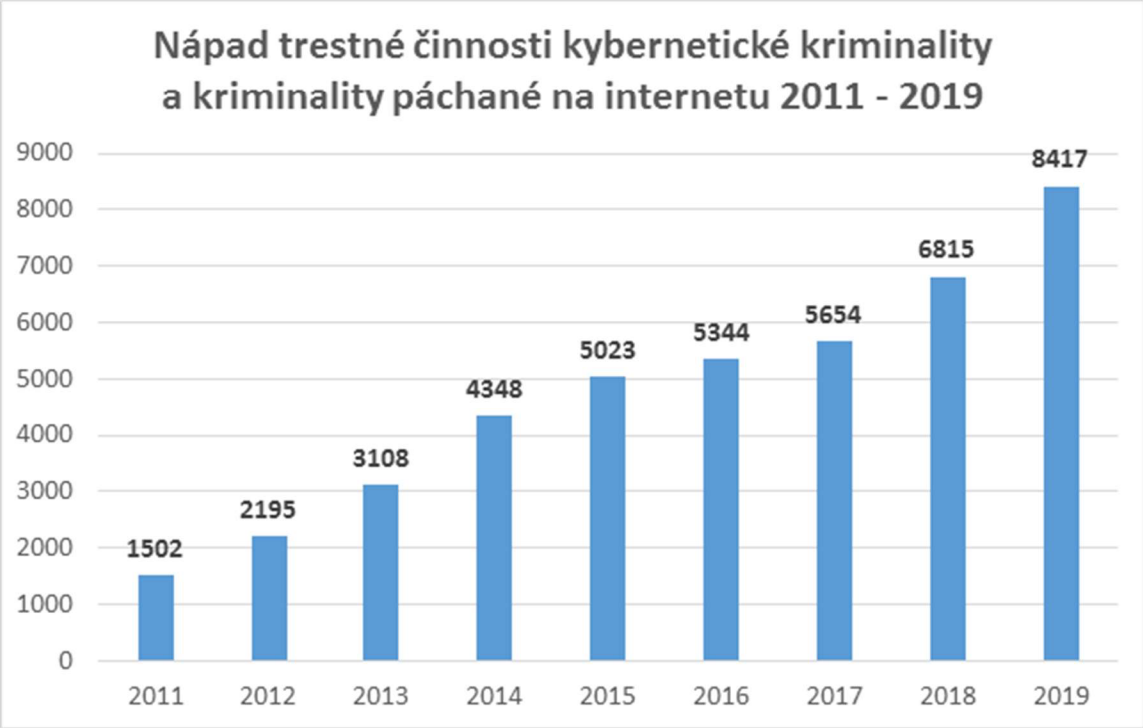
v podobě jeho vrstvení na určité místo, kde dochází k zastření pravého původu, jeho přeměny do různých podob, až do jeho opětovného vrácení do dispozice disponenta, čímž dochází k jeho integraci, přičemž díky specifičnosti kryptoměn, je lze jejich přítomnost nalézt ve všech fázích vývoje. Kryptoměna tak může být samotným nelegálním příjmem, může být přítomna při počátečním zastření svého původu až do okamžiku integrace v podobě nových elektronických peněz bez zjevně viditelných vazeb na trestnou činnost.

4. Vývoj kyberkriminality za užití kryptoměn

V České republice, zejména v posledních dvou letech došlo k rozmachu trestné činnosti spojené s kryptoměnami. K tomu přispělo sociální odloučení zapříčiněné šířením nemoci COVID-19, které bránilo v běžnému pohybu osob, příjezdu turistů i cizinců páchajících trestnou činnost. Díky omezenému pohybu, zvýšeným opatřením se trestná činnost začala přesouvat do virtuálního prostředí. Skutečný stav v číslech a grafech však nelze věrohodně doložit, jelikož v této době Policie ČR nemá atributy reflektující na kyberkriminalitu tak, aby dokázala samostatně sledovat trestnou činnost kolem virtuálních měn a typů jednotlivých útoků. Nyní lze sledovat jen kyberkriminalitu jako celek a nikoli její podmožiny. Pojem „kyberkriminalita“ v tomto systému sleduje veškerou trestnou činnost spojenou s internetem a jeho virtuálním světem a prozatím neexistuje nástroj k vykázání nárustu nových trestných činů spojených s kryptoměnami, lze však i s ohledem na nejpopulárnější bitcoin předjímat, že vede i na žebříčku kryptoměn, které byly získány jako výnos z trestné činnosti. Při dotazu jednotlivých úrovní Policie ČR, které mají přístup nebo dokonce samy zpracovávají analytické informace o trestné činnosti se mi nepodařilo získat žádný hmatatelný výsledek, ať už na úrovni Krajského ředitelství policie ČR Praha, ale ani na úrovni ÚSKPV a NCOZ. Jediným pozitivním výsledkem ke zjištění nárůstu trestné činnosti, či spíše kvantifikování zajištěných měn bylo šetření na ÚZSVM, které se zabývá následným prodejem zajištěných výnosů a nástrojů z trestné činnosti. Z jejich dosavadních informací bylo zjištěno, že evidují několik případů napříč celou

republikou, které realizovala Policie České republiky a Celní správa České republiky. Poskytnuté informace vycházejí z kryptoměn, které byly ÚZSVM předány k prodeji.

Z informací získaných od ÚZSVM tak lze uvést, že v současné době eviduje dvě desítky různých kryptoměn, které jsou prozatím pouze zajištěné dle zákona č. 279/2003 Sb. (o výkonu zajištění majetku a věcí v trestním řízení a o změně některých zákonů). Zajištěny jsou kryptoměny jako bitcoin, ethereum, monero, dogecoin, cardano, IOTA, ripple, jejichž hodnota je povětšinou v nízkých jednotkách a v případě bitcoinu dokonce ve zlomkách jednotek kryptoměny. Prozatím byly uskutečněny 3 elektronické aukce, a to vždy v roce 2021, vždy se jednalo o virtuální měnu bitcoin a všechny byly doposud zveřejněny na internetových stránkách zmíněného úřadu nabidkamajetku.cz. Všechny zajištěné kryptoměny měly pocházely z trestné činnosti a ve dvou případech byl vlastníkem stát, který je získal v rámci uloženého trestu propadnutí majetku podle § 70 tr. zákoníku, v jednom případě byl ÚZSVM pověřen k prodeji PČR v souladu se zákonem 279/2003 Sb. Již vydražené kryptoměny pocházely z trestné činnosti padělání a pozměnění platebního prostředku a nedovolené výroby a jiného nakládání s omamnými a psychotropními látkami a s jedy. Bližší informace se touto cestou ani cestou konkrétních útvarů, které kryptoměny zajistily, nepodařilo zjistit s ohledem na probíhající trestní řízení.



Graf kybernetické kriminality získaný z oficiálních stránek Policie České republiky.[44]

4.1. Operativní rozpracování nelegálních aktivit

Při odhalování trestné činnosti spojené s virtuální měnou, jejíž závěrem má být odčerpání výnosů z trestné činnosti, či spojení takové trestné činnosti s virtuálních měnou, se s ohledem na povahu kryptoměn jeví takovýto cíl jako velmi obtížný a mnohdy nesplnitelný. Důvodem je samotná myšlenka virtuálních měn, která klade důraz na zájem decentralizace spojený s jistým stupněm anonymity, díky němuž neumožňuje běžným způsobem zjistit, zda zájmová osoba je vlastníkem kryptoměn či virtuální peněženky a s tím spojené skutečné vlastnictví

[44] Kyberkriminalita. Policie.cz [online]. 2021 [cit. 2022-03-02]. Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx.

či držení virtuálních měn. Tento krok je v porovnání se zjištěním stavu na bankovním účtu velmi obtížný až přímo nesplnitelný.

Jak vyplývá z nastínění způsobu pořízení kryptoměn, je možné si je opatřit koupí několika legálními způsoby ve směnárnách, na burze, v bitcoin automatech nebo přímo od fyzické osoby, ale také krádeží virtuální peněženky či podvodem. V případě krádeže celé hardwarové peněženky se zpravidla pachatel nedostane k jejímu obsahu bez přístupového hesla a v případě takového nabytí se patrně ani nepodaří bitcoiny, či jiné mince z peněženky přečerpat do pachatelovi peněženky. Nedojde tedy ani k zápisu do blockchainu a zjištění takového stavu, takový trestný čin je pak „ryze“ běžnou krádeží.

V případě trestné činnosti, kdy je bitcoinů nebo jiných měn užito jako platidla například na darknetu k pořízení nelegální pornografie nebo jako prostředku k nákupu zakázaných látek je možné takovýto pohyb možné odhalit při sledování takového trhu, přičemž se jako nejpravděpodobnější nástroj jeví užití předstíraný převod a následné rozpracování směrem k odesilateli a zadokumentování celého skutkového děje. Při nalezení takového „obchodníka“, který přijímá virtuální měnu je pak jako další nástroj třeba užít sledování samotného obchodníka. K odčerpání výnosů z trestné činnosti je pak nutné zajistit nasazení techniky k prostorovému sledování a zjištění běžného způsobu života tak, aby došlo k zajištění nejen samotnou výpočetní techniku, peněženku s uloženou virtuální měnou nebo k zajištění seedu, aby se podařilo tuto měnu především odčerpat.

V případě zajišťování virtuální měny jako nástroje z trestné činnosti dochází u jednočinných útoků zřídkakdy. Naopak v případě vícečinných útoků je možné při takovém jednání nalézt opakované vzorce jednání, které mohou orgány činné v trestním řízení přivést k hypotéze či přímo k pachatelově chybě, kterou může být právě opakující se neobvyklá činnost či jeho chování.

U podvodného jednání na principu phishingu nebo vishingu se pak jako nástroj k odčerpávání kryptoměn nabízí zejména rychlost a připravenost reakce, tedy navedení na směnárnu, která je schopná v krátkém časovém od zjištění takový převod blokovat úseku. V případě, kdy se poškozenému podaří zjistit, že byl podveden krátce poté rozhodují vteřiny, výjimečně minuty, které rozhodují o

možnosti uskutečnit blokaci převodu. V případě již provedeného převodu je pak možné užít trasování, bohužel však v případě promyšleného útoku končí bitcoiny v peněžence držitele na území cizího státu, v mixéru nebo provedením několika zastíracích převodů, které znesnadní jeho vytrasování a spojení s útočníkem.

4.2. Trasování

Ke zjišťování toku kryptoměn slouží nástroje určené k trasování. Jedná se o software, který je možné užít ke zjištění pohybu kryptoměn v blockchainu a vytvářet různé rizikové analýzy. K tomuto jsou nejčastěji používány software Elliptic a Chainalysis Reactor. Jejich společnou náplní je boj proti praní špinavých peněz, je možné je užít k detekování rizikových operací kryptoměnami a označování či eliminování rizikových adres (peněženek), ale i vytváření analýz dle mnoha atributů. Trasování umožňuje prozkoumat, vyšetřovat a přijmout opatření jako je například zmíněné označení rizikových adres pro možné investory a swapovací služby. Policie je v současné době může užívat zejména k vystopování, tedy určení trasy převodu dokumentující směr odcizení propojení s konkrétními reálnými entitami. Jejich upotřebením je zjišťovat pohyb odcizených finančních prostředků, stejně jako legitimní činnost při zajišťování půjček a převodu NFT. Užití obou nástrojů je v současné době u policie samozřejmě podmíněno souvislostí s trestnou činností a kryptoměnami. Jejich užití je prováděno analytickými útvary krajských a městských ředitelství a útvarem OKK NCOZ

4.3. Kyberútoky

Kyberútokem je označovaná počítačová bezpečnostní událost, kterou lze chápat jako počítačový útok nebo počítačový trestný čin, tedy operaci, která

chápána jako nepovolná, neautorizovaná a nepřijatelná akce proti vědomí napadeného, jež zahrnuje počítačový systém či její síť. /toky jsou často směřovány na krádež identity, zneužití údajů, převzetí přístupu k internetovému bankovnictví a dalších útoků.[45]

4.3.1. Phishing

Takto jsou označovány útoky počítačových podvodníků, kteří se snaží získat citlivé osobní údaje, jako hesla, rodná čísla, údaje o platebních kartách, nebo čísla bankovních účtů, či přístupová hesla k bankovním účtům. K jejich šíření užívají pachatelé podvodných emailů nebo přesměrováním na falešné internetové stránky, výjimkou nejsou ani emaily napodobující adresy skutečných organizací, bankovních ústavů, nebo jiných peněžních služeb jako PayPal, E-gold, MoneyBookers, ale také jiných služeb jako je Česká pošta, kde útočník rozesílal zprávy pomocí podvržených emailových adres: infocpost23@otenetoamsaoaos.com a infocpost14@otenetoamsaoaos.com.[46] Obsahem emailu je zpravidla odkaz na internetové stránky, kde je oběť navedena ve fiktivním, ale realistickém prostředí k zadání přihlašovacích údajů, čímž sama poskytne tyto údaje třetí osobě. Pomocí takového útoku může být i přihlášení do peněženky. Nejlepší obranou v tomto případě je obezřetnost, zdravý rozum. Cílem útočníka je sběr dat a odčerpání peněžních či v tomto případě virtuálních prostředků.

---

[45]KOLOUCH, Jan a Petr VOLEVECKÝ. *Trestněprávní ochrana před kybernetickou kriminalitou*. Praha: Policejní akademie České republiky v Praze, 2013, s.14. ISBN 978-80-7251-402-1..

[46]11. 3. 2022 - Bezpečnostní upozornění na podvodné e-maily. Ceskaposta.cz [online]. [cit. 2022-03-11]. Dostupné z: https://www.ceskaposta.cz/o-ceske-poste/aktualni-podvodne-e-maily

.

4.3.2. Vishing

Většina lidí slyšela o phishingu, vishing je další formou podvodného útoku, který je vyvolán buď po návštěvě sociálních sítí kde se po kliknutí na lákavý odkaz objeví modrá obrazovka s varováním a kontaktní telefonickou linkou na helpdesk. Na telefonu poté zareaguje přátelský technik, který nabízí pomoc za poplatek, ale může jít i o snahu navést volajícího k nainstalování softwaru Anydesk umožňující dálkový přístup. Při takovém útoku existuje riziko dalších několika scénářů, vylákání přístupových kódů k internetovému bankovnictví, vydírání po odcizení citlivých údajů, nebo poskytnutí údajů o kreditní kartě k nákupu softwaru, který má vyřešit problém s počítačem. Takový útok může být mnohdy i velmi rozpačitým pokusem přesvědčit volajícího, aby postupoval podle kroků útočníka, jakým byl falešný operátor s ruským přízvukem, kterému se nepodařilo přesvědčit volajícího, aby si nainstaloval Anydesk, aby mu posléze mohl odcizit bitcoiny.[47]

4.3.3. Ransom DDos atack

Zkratka DDoS znamená „Distributed Denial of Service“, tedy kybernetický útok, spočívající v masivním zahlcení kapacit oběti, který se zaměřuje na internetové připojení, výkon serverů nebo databází prostřednictvím požadavků. Smyslem je vyřadit z provozu službu, nejčastěji směřující na webové stránky, e-shop, chod nemocnic nebo státních institucí apod. Útok není veden z jednoho místa, jelikož by se stal snadno odhalitelný, což by vedlo k rychlému odvrácení ataku útočníka. Proto je takový útok zpravidla veden z mnoha míst na světě, čímž zaměstnává správce napadeného, nebo mu zcela znemožňuje nápravu takového stavu. Odvrácení takového útoku si útočník podmiňuje splněním požadavků,

---

[47]KRÁTKÝ, Václav. Telefonní rozhovor s podvodníkem nabízející bitcoiny - požaduje přístup do internet. bankovnictví. Youtube.com [online]. 18.1.2022 [cit. 2022-03-02]. Dostupné z: https://www.youtube.com/watch?v=SCHTRRzGjSQ

.

kterými je například i výkupné v bitcoinech. Díky zahlcení kapacit oběti počítače z IP adres po celém světě je tedy útok veden jako distribuovaný.

4.4. Dokumentace pomocí případů

K uvedeným útokům je vhodné uvést i několik případů, které ukazují, že avizované je ve skutečnosti reálnou hrozbou, kterou si mnohdy ani neuvědomujeme.

4.4.1. Vývoj kyberkriminality za užití kryptoměn

Kriminalisté Odboru analytiky a kybernetické kriminality Krajského ředitelství policie Středočeského kraje ukončili po několika měsících vyšetřování ransomware útoku na benešovskou nemocnici, který se stal 11. prosince roku 2019. Útok byl veden právě zmíněným Ransom DDoS útokem, který blokoval chod nemocnice. Za jeho odstranění útočník považoval výkupné v kryptoměně. Dle zprávy došlo k zašifrování konkrétních dat v počítačích nemocnice. Útok nebyl cílený přímo na tuto konkrétní nemocnici a současně s ním došlo k napadení o dalších počítačů státní správy. Benešovská nemocnice odmítla s útočníkem komunikovat nedošlo k vyplacení výkupného. Na odstranění útoku spolupracovali středočeští kriminalisté s IT specialisty benešovské nemocnice, příslušníky NCOZ, zaměstnanci NÚKIB a ESET. Škoda způsobená tímto útokem přesáhla 59 milionů korun.[48]

---

[48]SCHNEEWEISSOVÁ, Barbora. Středočeští kriminalisté ukončili vyšetřování Ransomware útoku na benešovskou nemocnici. Policie.cz [online]. 18.8.2020 [cit. 2022-03-02]. Dostupné z: https://www.policie.cz/clanek/stredocesti-kriminaliste-ukoncili-vysetrovani-ransomware-utoku-na-benesovskou-nemocnici.aspx

4.4.2. Carlos

Případ Carlos, který byl zveřejněn v roce 2019, realizovala Národní protidrogová centrála ve spolupráci s rakouskou policií, při které odhalili rozsáhlý nelegální obchod s marihuanou, vyprodukovanou na území ČR celkem v 11 lokalitách v Moravskoslezském, Jihomoravském kraji a kraji Vysočina, kde byla marihuana pěstována a zpracovávána na sušinu. Její výroba a distribuci byla dílem dvou organizátorů, přičemž jeden měl na starosti výrobu a druhý z nich distribuoval drogy do 75 zemí světa, přičemž produkt anoncoval pomocí darknetu. Za své obchody inkasovali virtuální měnu, a to převážně bitcoiny, ale také další altcoiny jako monero nebo litecoin. Celkem bylo v tomto případě zadokumentováno 22000 realizovaných prodejů. Při realizaci operace bylo zajištěno celkem 69,8 kg sušiny marihuany určené k distribuci a mimo jiné virtuální měna ve výši 113 bitcoinů,spolu s další finanční hotovostí movitým a nemovitým majetkem ve výši 17.218.000,- Kč. Oba organizátoři byli obviněni ze zvlášť závažného zločinu nedovolené výroby a jiného nakládání s omamnými a psychotropními látkami a s jedy podle ustanovení 283 odst. 1, odst. 2 písm. a), odst. 3 písm. c) trestního zákoníku.

K samotnému případu bylo ve spolupráci s policisty, kteří na případu pracovali zjištěno, že k zajištění kryptoměn došlo v době prováděné domovní prohlídky a v souvislosti s nasazením operativně pátracích prostředků, bez nichž by k zajištění nedošlo. Současně s realizací případu byly odhaleny i další skutečnosti dokládající jednání praní špinavých peněz při výměně kryptoměn s další osobu mimo uvedený případ.[49]

.

[49] KUDLÁČKOVÁ, Barbora. Operace „CARLOS“i. Policie.cz [online]. 12.3.2019 [cit. 2022-03-02]. Dostupné z: https://www.policie.cz/clanek/operace-carlos.aspx

.

4.4.3. Phishing v praxi

Dotazem kolegy z OHK byl doložen i jeden phishingový případ z poloviny roku 2021, ke kterému došlo v Plzeňském kraji. Došlo k němu při rozesláním emailu z adresy RB.CZ@showroom.kahramanperde.com dvěma poškozeným MS a IB, s falešnou výzvou k obnovení účtu, který vzbudil v obou poškozených dojem pravosti. Ti pak na falešných stránkách zadali přihlašovací údaje, které pachatel následně užil a zmocnil se ve dvou útocích na jeden spořící a na jeden bankovní účet, vedených u Raiffeisenbank, 2 milionů korun, které přeposlal na bankovní účet u Airbank, ze kterého následně pořídil virtuální měnu bitcoin v hodnotě 0,12459178, kterou se podařilo kriminalistům zajistit dle ustanovení § 79a odst. 1 tr. řádu na účtu české směnárny bit.plus. V rámci případu bylo provedeno i trasování převodu, který zajistil útvar NCOZ pomocí Chainalysis Reactor a údajů z blockchainu. Provedeným šetřením se však nepodařilo pachatele zjistit.

5. Zhodnocení postoje regulatorních orgánů a jejich kritika

Při hodnocení postojů dohledových orgánů nezbývá než uvést, že ČNB jako kontrolní orgán v otázce kryptoměn nemá nová řešení, přístup tak dle zprávy ČNB nevyjadřuje jakým způsobem vykonávat dohled nad tokem peněz uložených do takového aktiva. Ačkoli má kryptoměna již v samotném názvu, že se jedná o platidlo, není dosud odbornou veřejností orientující se převážně na fiat měny plně akceptována. Stanovisko ČNB se tak do značné míry jeví jako vyhýbavé, kterým se rozhodli nedělat raději nic, než, aby zavedli nějaká opatření.

Navrhovaná opatření, směny v ATM provádět po přiložení jednoho z dokladů totožnosti nebo otisku ruky, sice by to vedlo k vytlačení takové služby, nebo vytlačení jejich uživatelů, ale proč by se měl zákazník takové služby bát. Při analogickém srovnání s klienty bankovních ústavů, kteří jsou v databázích finančníků již vedeni, by šlo defacto jen o narovnání rozdílů vedení evidencí dvou

obdobných produktů jako je bankovní účet spojený s identitou klienta a registrace s identitou držitele virtuální měny, což se ostatně v kontextu zákona č. 37/2021 Sb., o evidenci skutečných majitelů, jeví jako požadovaný cíl při rozvíjející se snaze bojovat proti praní špinavých peněz. Jednou z možností registrace uživatelů kryptoměn by pak bylo možné provést přímo při pořízení hardwarové peněženky.

Metody výzkumu a použité zdroje

Ke zpracování diplomové práce a jsem použil výzkumné prvky a metod analýzy, syntézy, pozorování jednotlivých jevů a jejich srovnání. Při tomto jsem užil analýzy jako nástroje myšlenkového rozkladu pro pochopení zkoumaného jevu a jeho elementárních částic. Cílem bylo poznat jejich podstatu k dalšímu užití. Oproti tomu jsem za pomoci syntézy spojil nasbírané informace opět ve funkční myšlenkový celek, který vykreslil poznané v uchopitelný informační soubor. Tímto postupem jsem pospojoval nasbírané informace a přenesl je do této práce tak, aby mohly sloužit k předání uchopitelnějších poznatků týkajících se kryptoměn a aspektů s nimi spojených. Souběžně za užití metody komparace jednotlivých článků i norem jsem porovnal a shrnul nasbírané informace tak, abych po ověření nasbíraných témat předal informace v její důvěryhodné a skutečné podobě, a to s ohledem na to, že zdrojem pro zkoumané a novodobé téma jsou v současné době převážně internetové zdroje. Metodu pozorování jsem zaměřil nejvíce na pozorování rizikových prvků, coby možných mechanismů k legalizaci výnosů z trestné činnosti. V tomto případě NFT a bitcoin automaty.

Vzhledem k tomu, že problematika kryptoměn je i přes své trvání 14 let stále novým tématem a velkým fenoménem této doby, slouží k jejímu poznání jako zdroj informací převážně internet, a to i proto, že se jedná o rychle se rozvíjející obor, který prochází řadou změn. Ačkoli existují publikace, které se danému tématu věnují, jako je například kniha ekonoma Dominika Stroukala, který pod titulem Bitcoin a jiné peníze budoucnosti vydal již třetí aktualizované vydání své knihy, a

to v období let 2015 až 2021 s cílem reagovat na nové trendy a vývoj daného oboru.

Jako zdroje své práce jsem proto užil zejména internetových článků, periodik, ale i internetových stránek domácích i zahraničních státních složek, které uvádějí v dané problematice své závěry a doporučení, ať to již byla stránky ČNB, FAÚ, BaFin, EU. Nejvíce informací jsem však čerpal ze stránek orientovaných se kolem „nadšenců“ kryptoměn, které by se díky postupné oblibě a přeměně tohoto odvětví na ekonomicky, a dnes již i politicky exponovanou část ekonomiky, dalo spíše nazvat jejími tvůrci. Tak jak jsem již uvedl, jedná se o velmi dynamické téma, ve kterém je velmi ošidné užít jako zdroj informací zdroj staršího data, zejména pokud se jedná o legislativní opatření. Regulace a vymezení problému rychle se měnícího odvětví nespí, a to co platilo včera může být již zítra minulostí. Příkladem může být například nejsilnější kryptoměnový trh, který se k virtuálním měnám vymezil zásadním způsobem.

Mezi české velké a oblíbené autory článků týkajících se kryptoměn lze uvést Dominika Stroukala a Karla Filnera, ačkoli se zabývají tématy kryptoměn velmi zdařile a jednotlivé prvky vysvětlují velmi vstřícným způsobem, je třeba mít z pohledu možného zneužití kryptoměn k trestné činnosti k jejich entuziazmu a liberálnímu přístupu střízlivý přístup a pohled na věc.

Mimo dosažitelné internetové zdroje a publikace jsem jako další zdroje užil i intranetové stránky ÚSKPV, NCOZ a internetové stránky ÚZSVM. Jak jsem uvedl, užil jsem také přímých kontaktů na příslušníky útvarů ÚSKPV, NCOZ a Celní správy ČR, kteří v této věci podnikají metodické opatření a zabývají se odčerpáváním kryptoměn z trestné činnosti. Ačkoli se mi ve většině případů nepodařilo získat konkrétní informace k vytvoření současné kazuistiky, získal jsem od nich alespoň informace o skutečném vývoji trestné činnosti na poli virtuálních měn, která se dle názoru dotázaných týká celého spektra trestné činnosti, převážně však prodeje narkotik a podvodných útoků.

Závěr

Kryptoměny v současné době získaly velikou oblibu, a to i přes punc něčeho nelegálního. Ačkoli jim ČNB neudělila status měny a označila je za investiční nástroj, je možné užít je k platbám na mnoha místech. Současně i s ohledem na riziko vysoké inflace, která postihuje měnový trh na celém světě se pojetí kryptoměn jako investičního nástroje jeví jako velmi účinné opatření. Bohužel však s oblibou virtuálních měn, potažmo bitcoinu, přišel i zájem rizikových skupin či jednotlivců coby pachatelů trestné činnosti, kteří stejně jako investoři do virtuálních aktiv nalezli možnost ke svému obohacení. K tomuto účelu se pachatelé velmi rychle přeškolili na kryptoměny, aby eliminovali dopady epidemie covidu, která omezila pohyb osob i jejich zisky z trestné činnosti, jako v jakémkoliv jiném oboru postiženého epidemií. Díky přeskupení kriminality se tak současně i podíl takto orientované zločinnosti znásobil. Přechod na novou podobu trestné činnosti, která lze díky internetu provozovat z jakéhokoli místa na světě s dostupným internetem se navíc spolu s kryptoměnami stala velmi vhodným prostředkem jako nástrojem legalizace výnosů z trestné činnosti. K takovému přístupu napomáhá možnost anonymity v případě, že k vytvoření peněženky dojde bez registrace pachatele. Díky tomu se tak pachatel stává v současné době nevystopovatelným a kryptoměny se tak stávají ideálním nástrojem trestné činnosti, ale i možným výnosem v případě jejich vyprání. Takovýto přístup požaduje i jistou dávku inteligence, kterou musí pachatel prokázat, aby se stal úspěšným. Existuje však i mnohem jednodušší způsob jakým užít bitcoin coby nástroje legalizace výnosů z TČ. Tím je přístup k bitcoin automatům. Při odcizení jakéhokoli majetku, jeho prodeji na černém trhu či pomocí inzerce, lze nabytou konvenční měnu možné ukládat do kryptoměn v automatech bez potřebné registrace. I přes omezení denním vkladem ve výši 25.000 korun na osobu na kryptopeněženku. V případě několika peněženek, které lze založit bez jakéhokoli poplatku a registrace s malým pozměněním vzhledu, aby se takovýto doveda vyhnul zájmu provozovatele auomatů se tento způsob dá snadno opakovat i bez přispění bílého koně. Takovýto způsob se jeví jako nejsnazší a nejdostupnější zejména v Praze, kde se nachází přes 40 terminálů.

Kryptoměny v současné době „volného“ přístupu regulatorních úřadů naplno využívají svého potenciálu decentralizace a volného pohybu, který je pouze v rukou jejich držitelů. Prozatím neexistuje přímý nástroj, kterým by šel takový tok virtuálních měn zvrátit mimo reálný čas uskutečněné operace či se proti jeho neoprávněnému užití pojistit. K tomuto je v současné době možné užít jen vlastní obezřetnost a informovanost, jak na úrovni jejich držitelů, orgánů činných v trestním řízení, ale i u běžných osob využívajících například internetové bankovnictví, kteří se mohou stát například obětmi například vishingu. Patrně asi jako největší problém v současné chvíli vidím možnost vytvořit nezměrné množství peněženek bez provedení registrace osoby. Liberální zastánci kryptoměn mohou jistě namítat, že kryptoměny vznikly právě z důvodu svobodného přístupu k měnám a za současného stanoviska ČNB se mohou opírat o jejich názor, že virtuální měny není třeba regulovat a je lepší ponechat vlastnímu osudu. Mě se však v současné době jeví reálná možnost regulace, která může být ovlivněna jak energetickou krizí či spojením s válečnými sankcemi vůči Rusku, které v současné chvíli podporuje i platforma Elliptic, která provozuje analytické služby v oblasti kryptoměn a jejich trasování. Ta díky svému zaměření upozornila na možnost využití kryptoměn jako nástroje k obcházení válečných sankcí. I když se zdá, že za pomoci trasování lze pohyb kryptoměn vždy vysledovat, není tomu tak, existuje riziko možných opakovaných a zastíracích převodů, které pomáhají realizovat mixéry a tumblery kryptoměn, díky čemuž dojde k natolik složitému řetězci, který se nepodaří v systému trasování odhalit a spojit s konkrétní osobou. Lze však určit směr jakým došlo například k odčerpání kryptoměny.

Ze závěru plyne, že kryptoměny jsou ideálním a snadným nástrojem k legalizaci, je však nutné užít jisté opatrnosti a obezřetnosti v tomto případě, jelikož pachatel nemůže důvěřovat žádné osobě, která se na mixování podílí, nemůže se totiž obrátit na provozovatele se žádostí o vrácení mincí nebo na policii.

V současné době policie nedisponuje žádnými statistikami, které by mohly doložit skutečný nárůst a vývoj trestné činnosti spojených s kryptoměnou. Díky současnému šetření lze s jistotou říci, že dochází k užití kryptoměn k nákupu a prodeji narkotik, ale i k ransom útokům. Současné řešení situace spatřuji jak v celosvětové registraci peněženek, což se však nedá provést bez podpory těžařů,

kteří se podílí na změně pravidel, ale také jejich tvůrců a podporovatelů. Tento krok by však neměl být funkcí restriktivní, ale spíše konsenzem, aby došlo k zajištění větší důvěry v kryptoměny, jelikož současný stav spěje k názoru více regulovat anonymizační faktory. K tomuto kroku měly přispět záminky jako dostupná dětská pornografie, která je šířena na darknetu, boj proti organizovanému zločinu, drogám a terorismu, ke kterému v současné době může přispět i vymáhání sankcí vůči ruským oligarchům. Je však možné, že díky současné válce na Ukrajině i zmíněnému problému s energiemi dojde ke skutečnému potlačení kryptoměn či minimálně těžbě, která je příliš energeticky náročná, jak k tomu došlo například v Číně.

Použitá literatura

- DVOŘÁK, Vratislav. *Výnosy z trestné činnosti*. Praha: Pro potřeby nakl. Ivan Fojt vydala Scientia, 2010. ISBN 978-80-86960-67-8.
- DVOŘÁK, Vratislav. *Ekonomické a kriminální aspekty legalizace výnosů z trestné činnosti*. Praha: Pro potřeby nakl. Ivan Fojt vydala Scientia, 2010. ISBN 978-80-86960-63-0.
- KOLOUCH, Jan a Petr VOLEVECKÝ. *Trestněprávní ochrana před kybernetickou kriminalitou*. Praha: Policejní akademie České republiky v Praze, 2013. ISBN 978-80-7251-402-1.
- STIERANKA, Jozef. *Boj proti legalizácii príjmov z trestnej činnosti vo vybraných krajinách Európskej únie*. Praha: Pro potřeby nakl. Ivan Fojt vydala Scientia, 2009. ISBN 978-80-86960-55-5.
- STROUKAL, Dominik a Jan SKALICKÝ. *Bitcoin: peníze budoucnosti: historie a ekonomie kryptoměn, stručná příručka pro úplné začátečníky*. Praha: Pro potřeby nakl. Ivan Fojt vydala Scientia, 2015. ISBN 978-808-7733-264.
- STROUKAL, Dominik a Jan SKALICKÝ. *Bitcoin a jiné kryptopeníze budoucnosti*. 3. rozšířené vydání. Praha 7, U Průhonu 22: GRADA, 2021. ISBN 978-80-271-4255-2.
- BEDNÁR, Juraj. *Kryptomeny platobná sieť internetu: Kryptomeny ako natívny platobný protkol internetu - vlastnosti, použitie, príležitosti a vízia*. ID: 20110-27181546336880022112-307093-220.
- DRAŠTÍK, Antonín. *Trestní řád: komentář*. Praha: Wolters Kluwer, 2017. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7552-600-7.
- JELÍNEK, Jiří. *Trestní zákon a trestní řád: s poznámkami a judikaturou; Zákon o soudnictví ve věcech mládeže : s poznámkami : a předpisy souvisící ... v úplném znění : podle stavu k ...* Praha: Linde, [1993]-2008. ISBN 978-80-7201-731-7.
- ŠÁMAL, Pavel. *Trestní řád: komentář*. 7., dopl. a přeprac. vyd. V Praze: C.H. Beck, 2013. Velké komentáře. ISBN 978-80-7400-465-0.

Zákonná úprava a prováděcí předpisy

Zákon č. 253/2008 Sb.: o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu. 5.6.2008. In: Sbírka zákonů. Vč. novelizací, dostupné také na https://www.beck-online.cz/bo/chapterview-document.seam?documentId=onrf6mrqga4f6mrvgmwtemq.

Metodický pokyn č. 2 FAÚ: O přístupu povinných osob k digitálním měnám. *Https://www.financnianalytickyurad.cz/download/downloads_files_cs/16 17811336_cs_zrusen.pdf* [online]. Ministerstvo financí, ze dne 16.9.2013 [cit. 2022-01-06].

Internetové zdroje

NOVOTNÝ, Radovan. Čím jsou dnes peníze kryty? Dluhem. *Mesec.cz* [online]. 3.2.2016 [cit. 2022-03-01]. Dostupné z: https://www.mesec.cz/clanky/cim-jsou-dnes-penize-kryty-dluhem/

Sdělení k účtování a vykazování digitálních měn [online]. MFČR, 2018, 15.5.2018, , 2 [cit. 2021-12-21]. Dostupné z: https://www.mfcr.cz/cs/verejny-sektor/ucetnictvi-a-ucetnictvi-statu/ucetnictvi-podnikatelu-a-neziskoveho-sek/aktuality-a-metodicka-podpora/2018/sdeleni-ministerstva-financi-k-uctovani-31864

In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2018-01-02]. Dostupné z: https://cs.wikipedia.org/wiki/Satoshi_Nakamoto

PML aneb legalizace výnosů z trestné činnosti v rukou expertů: Regulace AML [online]. FAÚ, 2019 [cit. 2021-4-10]. Dostupné z: https://www.financnianalytickyurad.cz/download/FileUploadComponent-105114954/1592488324_cs_27_29.pdf

Upozornění Ministerstva financí na rizika investičních tokenů [online]. MFČR, 2021, 29.11.2021, , 1 [cit. 2022-01-21]. Dostupné z: https://www.mfcr.cz/cs/soukromy-sektor/platebni-sluzby-a-vyporadani-obchodu/aktuality/2021/upozorneni-ministerstva-financi-na-rizik-43725

https://kryptomagazin.cz/turecko-prijima-bitcoin-a-tether-zatimco-lira-stale-klesa/

Turecko přijímá bitcoin a tether, zatímco lira stále klesá [online]. 2022 [cit. 2022-01-13]. Dostupné z: https://kryptomagazin.cz/turecko-prijima-bitcoin-a-tether-zatimco-lira-stale-klesa/

Regulace kryptoměn v Turecku, kurz Bitcoinu nad 50 tisíci dolarů [online]. 2021 [cit. 2022-01-13]. Dostupné z: https://www.tradearena.cz/rubriky/aktuality/regulace-kryptomen-v-turecku-kurz-bitcoinu-nad-50-tisici-dolaru_1063.html

Turkey's cryptocurrency law soon to be debated in Parliament'. *Dailysabah.com* [online]. 2021 [cit. 2022-01-13]. Dostupné z: https://www.dailysabah.com/business/tech/turkeys-cryptocurrency-law-soon-to-be-debated-in-parliament

STROUKAL, Dominik. Kryptoměna bitcoin se v Rusku stala veřejným nepřítelem. *Ekonomickydenik.cz* [online]. 2015 [cit. 2022-01-15]. Dostupné z: https://ekonomickydenik.cz/kryptomena-bitcoin-se-v-rusku-stala-verejnym-nepritelem/

JAVŮREK, Karel. Putin nechce zákaz těžby bitcoinu v Rusku. Je ale pro regulaci a daně spojené s těžením kryptoměn. *Connect.zive.cz* [online]. 2022 [cit. 2022-01-22]. Dostupné z: https://connect.zive.cz/clanky/putin-nechce-zakaz-tezby-bitcoinu-v-rusku-je-ale-pro-regulaci-a-dane-spojene-s-tezenim-kryptomen/sc-320-a-214658/default.aspx

Russian authorities clash on plans for crypto regulation. *Economictimes.indiatimes.com* [online]. 2022 [cit. 2022-02-19]. Dostupné z: https://connecthttps://economictimes.indiatimes.com/markets/cryptocurrency/russian-authorities-clash-on-plans-for-crypto-regulation/articleshow/89687455.cms.zive.cz/clanky/putin-nechce-zakaz-tezby-bitcoinu-v-rusku-je-ale-pro-regulaci-a-dane-spojene-s-tezenim-kryptomen/sc-320-a-214658/default.aspx

JOHN, Alun, Samuel SHEN a Tom WILSON. China's top regulators ban crypto trading and mining, sending bitcoin tumbling. *Reuters.com* [online]. 2021 [cit. 2022-02-19]. Dostupné z: https://www.reuters.com/world/china/china-central-bank-vows-crackdown-cryptocurrency-trading-2021-09-24/

Virtual Currencies. Irs.gov [online]. [cit. 2022-02-17]. Dostupné z: https://www.irs.gov/businesses/small-businesses-self-employed/virtual-currencies

QUIROZ-GUTIERREZ, Marco. El Salvador says tourism is up 30% since it made Bitcoin legal, but the country is still on the brink of economic disaster. *Reuters.com* [online]. 2022 [cit. 2022-02-23]. Dostupné z: https://fortune.com/2022/02/23/el-salvador-bitcoin-law-tourism-up-30-percent-imf-senate/

HANDAGAMA, Sandali. European Parliament Postpones Vote on Crypto Regulations Indefinitely. *Coindesk.com* [online]. 2022 [cit. 2022-02-25]. Dostupné z: https://www.coindesk.com/policy/2022/02/25/european-parliament-postpones-vote-on-crypto-regulations-indefinitely/

Virtual currency schemes – a further analysis. *Coindesk.com* [online]. 2015, únor 2015 [cit. 2021-12-24]. Dostupné z: https://ec.europa.eu/commission/presscorner/detail/en/IP_20_1684

FILLNER, Karel. Soudní dvůr EU: Bitcoinové transakce osvobozeny od DPH. *Btctip.cz* [online]. 2015, 22.10.2015 [cit. 2021-12-24]. Dostupné z: https://ec.europa.eu/commission/presscorner/detail/en/IP_20_1684

SOTO, Alonso. ECB Urges Haste on Crypto Regulation in Wake of Russian Sanctions. *Bloomberg.com* [online]. 2022, 25.2.2022 [cit. 2022-02-25]. Dostupné z: https://www.bloomberg.com/news/articles/2022-02-25/ecb-urges-haste-on-crypto-regulation-amid-russian-sanctions

Crypto Is Tool for Rich Russians Looking to Evade U.S. Sanctions. *Bloomberg.com* [online]. 2022, 24.2.2022 [cit. 2022-02-25]. Dostupné z: https://news.bloomberglaw.com/banking-law/crypto-is-potential-new-tool-for-billionaires-to-avoid-sanctions

Size of the Bitcoin blockchain from January 2009 to February 7, 2022. *Statista.com* [online]. 2022, 24.2.2022 [cit. 2022-02-15]. Dostupné z: https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/

Recenze ccShop. Investplus.cz [online]. 2018 [cit. 2022-02-17]. Dostupné z: https://investplus.cz/investice/nevyhodny-ccshop-recenze-zkusenosti-diskuze-navod-reference-je-ccshop-cz-podvod/

LocalBitcoins – Směna kryptoměn mezi lidmi. Finex.cz [online]. 2019 [cit. 2022-02-17]. Dostupné z: https://finex.cz/recenze/localbitcoins/

About LocalBitcoins. LocalBitoins.cz [online]. 2022 [cit. 2022-02-17]. Dostupné z: https://localbitcoins.com/about

Total number of Bitcoin ATMs: Tellers in Czech Republic: 72. Coinatmradar.com [online]. [cit. 2022-03-07]. Dostupné z: https://coinatmradar.com/country/57/bitcoin-atm-czech-republic/

WOLF, Karel. České „kladivo na kryptoměny“? Co má změnit chystaný zákon. Lupa.cz [online]. 13.8.2019 [cit. 2022-03-07]. Dostupné z: https://www.lupa.cz/clanky/ceske-kladivo-na-kryptomeny-co-ma-zmenit-chystany-zakon/

TESAŘ, Jaromír. Základy kryptografie a její využití pro kryptoměny. *Btctip.cz* [online]. 21.1.2021 [cit. 2022-03-08]. Dostupné z: https://btctip.cz/zaklady-kryptografie-a-jeji-vyuziti-pro-kryptomeny/

Co je kryptografická funkce hash? Ssl.com [online]. 10.11.2015 [cit. 2022-03-08]. Dostupné z: https://www.ssl.com/cs/Nej%C4%8Dast%C4%9Bj%C5%A1%C3%AD-dotazy/co-je-kryptografick%C3%A1-hashovac%C3%AD-funkce/ash

Co to jsou ICOs?. *Cryptokingdom.tech* [online]. 1.3.2019 [cit. 2022-01-16]. Dostupné z: https://cryptokingdom.tech/cs/magazin/zacatecnik/co-to-jsou-icos

CHOUDHURY, Saheli Roy. TECH China bans companies from raising money through ICOs, asks local regulators to inspect 60 major platforms. Cnbc.com [online]. 4.9.2017 [cit. 2022-01-16]. Dostupné z: https://www.cnbc.com/2017/09/04/chinese-icos-china-bans-fundraising-through-initial-coin-offerings-report-says.html

STROUKAL, Dominik. Jedinečné tokeny: bublina, či inovace?. *E15.cz* [online]. 20.7.2021 [cit. 2022-01-15]. Dostupné z: https://www.e15.cz/nazory/dominik-stroukal-jedinecne-tokeny-bublina-ci-inovace-1382235

11. 3. 2022 - Bezpečnostní upozornění na podvodné e-maily. *Ceskaposta.cz* [online]. [cit. 2022-03-11]. Dostupné z: https://www.ceskaposta.cz/o-ceske-poste/aktualni-podvodne-e-maily

KRÁTKÝ, Václav. Telefonní rozhovor s podvodníkem nabízející bitcoiny - požaduje přístup do internet. bankovnictví. *Youtube.com* [online]. 18.1.2022 [cit. 2022-03-02]. Dostupné z: https://www.youtube.com/watch?v=SCHTRRzGjSQ

SCHNEEWEISSOVÁ, Barbora. Středočeští kriminalisté ukončili vyšetřování Ransomware útoku na benešovskou nemocnici. *Policie.cz* [online]. 18.8.2020 [cit. 2022-03-02]. Dostupné z: https://www.policie.cz/clanek/stredocesti-kriminaliste-ukoncili-vysetrovani-ransomware-utoku-na-benesovskou-nemocnici.aspx

KUDLÁČKOVÁ, Barbora. Operace „CARLOS“i. Policie.cz [online]. 12.3.2019 [cit. 2022-03-02]. Dostupné z: https://www.policie.cz/clanek/operace-carlos.aspx

KHARIF, Olga. Crypto Sleuth May Have Found Tokens of Sanctioned Russians. *Bloomberg.com* [online]. [cit. 2022-03-14]. Dostupné z: https://www.bloomberg.com/news/articles/2022-03-14/crypto-sleuth-may-have-found-tokens-of-sanctioned-russians