

POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

Fakulta bezpečnostně právní

Katedra kriminální policie

**Kryptoměna jako potencionální
nástroj legalizace výnosů z trestné
činnosti**

Diplomová práce

**Cryptocurrency as a potential tool for laundering the proceeds
of crime**

Diploma thesis

VEDOUCÍ PRÁCE

Ing. Vratislav Dvořák Ph.D.

AUTOR PRÁCE

Bc. Petr Příbyl

PRAHA

2024

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 Sokolově, dne 9. února 2024

Petr Příbyl

Tímto bych chtěl poděkovat vedoucímu mé diplomové práce panu Ing. Vratislavu Dvořákovi Ph.D. za odborné vedení, vstřícný přístup a shovívavost při mém vedení. Dále bych chtěl poděkovat své rodině a kolegům za podporu a pochopení po celou dobu studia.

ANOTACE

Tato diplomová práce zpracovává problém kryptoměny jako moderního nástroje pro legalizaci výnosů z trestné činnosti. Myšlenka decentralizovaného platebního systému bez možnosti regulace ze stran státu či centrální banky k tomu nepřímo vybízí. Práce představuje historické souvislosti pro vznik Bitcoinu, princip jeho fungování a posuzuje vhodnost využití k legalizaci výnosů z trestné činnosti. Dále jsou v práci představeny projekty spadající do tématu kryptoměn ve spojení s nelegálními aktivitami. Neméně důležitou součástí diplomové práce je postup a součinnost orgánů před a po zahájení úkonů trestního řízení a zajišťování prostředků získaných nelegální činností či v návaznosti na ní.

KLÍČOVÁ SLOVA

diplomová práce * kryptoměna * legalizace výnosů z trestné činnosti * bitcoin * monero * vyšetřování * blockchain * odčerpání prostředků

ANNOTATION

This thesis deals with the problem of cryptocurrency as a modern tool for laundering the proceeds of crime. The idea of a decentralised payment system without the possibility of regulation by the state or the central bank indirectly encourages this. The thesis presents the historical background for the emergence of Bitcoin, the principle of its operation and assesses the suitability of its use for money laundering. Furthermore, the thesis presents projects falling under the topic of cryptocurrencies in connection with illegal activities. An equally important part of the thesis is the procedure and interaction of the authorities before and after the initiation of criminal proceedings and seizure of funds obtained by or in connection with illegal activities.

KEYWORDS

diploma thesis * cryptocurrency * laundering the proceeds of crime * bitcoin * monero * investigation * blockchain * withdrawal of funds

Obsah

	Úvod.....	7
1.	Peníze.....	9
1.1	Virtuální měna a její zařazení.....	9
1.2	Virtuální měny x elektronické peníze.....	10
2.	Legislativní ukotvení virtuálních měn.....	12
2.1	Zákon AML.....	12
2.2	KYC – Know your customer.....	13
2.3	MiCA – CASP.....	13
3.	Kryptoměny.....	15
3.1	Vznik kryptoměn v souvislostech.....	17
3.2	Bitcoin.....	19
3.3	Altcoiny.....	25
3.3.1	Monero.....	25
4.	DeFi.....	28
4.1	Smart contract.....	28
5.	ICO.....	29
5.1	Venture capital.....	29
5.2	BitConnect.....	30
5.3	Xixoio.....	31
5.4	A16z.....	33
6.	NFT.....	34
7.	CBDC (Central Bank Digital Currency).....	35
8.	Nákup a obchodování s kryptoměnou.....	37
8.1	Směnárný CEX vs DEX.....	37
8.2	Peer to Peer (P2P).....	39
8.3	Vexl.....	40
8.4	ATM.....	40
9.	Legalizace výnosů z trestné činnosti.....	42
9.1	Organizovaná kybernetická kriminalita.....	43
9.2	Kyberútoky.....	44
9.3	Fáze praní peněz.....	45
9.4	Mixér virtuálních měn.....	46

10.	Zahájení úkonů trestního řízení.....	47
10.1	Podpůrné operativně pátrací prostředky.....	47
10.2	FAÚ – Finanční analytický úřad.....	47
11.	Dokazování v trestním řízení.....	48
11.1	Součinnost s OČTŘ.....	49
11.2	Novinka § 7b tr. řádu.....	51
12.	Operativně pátrací prostředky v souvislosti s kryptoměnou	52
13.	Zajišťování digitálních aktiv OČTŘ.....	54
13.1	Chainalysis.....	54
13.2	Trasování virtuálních měn v ČR.....	56
13.2.1	KODEX.US	57
13.3	Odčerpávání	58
14	Případová studie: JAMES ZHONG	60
	Závěr.....	63
	Použitá literatura	66
	Zákonná úprava a prováděcí předpisy	67
	Neveřejné zdroje.....	68
	Internetové zdroje.....	68

Úvod

Parafrázováním Jana Wericha – člověk měří čas jen, aby věděl co, kdy, kde a kolik za to, může být leckomu odpovědí na smysl života. Právě kolik za to, myšleno peníze, jsou hybatelem, jak světových dějin, tak přítomnosti a samozřejmě i budoucnosti. Rozdíl ovšem je v platidlech. Zatímco v dávné historii postačovala směna materiálních věcí, povětšinou dle užitku, Babyloňané definovali ve své době revoluční principy obchodu zavedením platidla – označených, vážených kusů stříbra a společně s platbou na splátky, úrokem, kvitancí, společným obchodováním či dělením zisku, položili základ dnešní kapitalistické společnosti.

Právě zmínky z Chammurapiho zákoníku, kdy jistě není náhodou, že mezi jeho 282 články, jsou kromě otázek ohledně rodiny, násilných zločinů či společenského postavení, řešeny i otázky majetku, obchodu, cen, mezd případně půjček a jejich splácení, nám dávají připomenout, že kriminalita nezná hranic a člověk je schopný v rámci získání vlastního prospěchu různých věcí.

4000 let uplynulo a stříbro, ačkoliv je stále významnou komoditou, není dnes primárním předmětem směny. A není jím ani druhá z historicky využívaných platebních komodit – zlato, které historicky, např. během éry mezi roky 1871–1914, zvané „klasický zlatý standard“, sloužilo alespoň, když ne k přímému obchodu, jako krytí pro tištěné peníze v USA v poměru 1:20 dolar vůči unci zlata. Krize, válka a inflace daly za příčinu měnové reformě. Od krytí bylo upuštěno a nápis z bankovek amerického dolaru „REDEEMABLE IN GOLD ON DEMAND“ byl zaměněn za „IN GOD WE TRUST“. FED začal vydávat bankovky vázané na dluhopisy, tedy nekryté reálnou hodnotou a zřejmě symbolicky tento slib splácet úvěr zaštiťuje víra.

Základním platidlem je tedy fiat měna. Peníze s nuceným oběhem, vytvořené mocí úřední. Některé měny fungují nadnárodně např. EURO, jiné jako americký dolar pak může užívat více samostatných států. Rozvojem dalších vázaných technologií, jakými jsou bezhotovostní platby, ať už prostřednictvím internetového bankovníctví či platebních karet. Dali zákonodárci moc finančním institucím vytvářet peníze, prakticky stejným způsobem, jakým to dělají centrální banky, na slib splácet a evidováním tohoto slibu.

A právě kombinace centrálního měnového systému, nekrytých peněz, ovládnutí inflace a manipulace s trhy daly příčinu vzniku kryptoměn. Pod pojmem kryptoměna se drtivě většině lidí vybaví Bitcoin, který roku 2008 vytvořil jedinec či uskupení lidí říkající si Satoshi Nakamoto. Bitcoin nepředstavuje v tomto případě pouze platidlo, ale především důmyslné systémy těžby a účetnictví zvaného blockchain.

Na výhody či nevýhody bitcoinu a dalších kryptoměn, využívajících IT prostředí se zaměřuje první část této práce, především z důvodu právního ukotvení a možnosti či nutnosti vzniku regulovaného prostředí, jelikož inovace v tomto směru přináší nové možnosti využití, jakož i zneužití, především z hlediska legalizace výnosů z trestné činnosti.

Druhá část práce se zabývá teoretickým vymezením legalizace výnosů z trestné činnosti prostřednictvím internetové sítě a způsoby kryptografických zajištění při potvrzování transakcí a možností jejich následné analýzy pro účely orgánů činných v trestním řízení. Dále pak operativním postupem při odhalování tohoto druhu finanční trestné činnosti a různými úskalími, které znesnadňují či dokonce znemožňují boj proti legalizaci výnosů, právě prostřednictvím kryptoměn a podporují tak hypotézu o účelu kryptoměn jakožto prostředku v lepším případě šedé, spíše však černé ekonomiky.

V závěru jsou pak uvedeny návrhy pro zlepšení efektivity odhalování předmětné problematiky, jakož i nutnost přijetí nového podpůrného právního rámce a aktualizování současného.

1. Peníze

Rozkladem na prvočinitele, jsou penězi různá aktiva, se kterými je možno uhradit zboží, službu či dluh bez ohledu na jejich formu či druh. Nezáleží tedy na tom, zda se jedná o sofistikovaně vytištěné papírky s fyzickými ochrannými prvky či ryze digitální bitovou informaci, dokud je splněna podmínka daná zákonem o všeobecné povinnosti je přijímat.¹ A právě zde u virtuálních měn ztrácíme cestu.

1.1 Virtuální měna a její zařazení

Podíváme-li se na odbornou literaturou definované základní funkce peněz, zjistíme čtyři základní pilíře. Prvním je funkce oběživa, tedy pohybu peněz jako úhrady za zboží a obráceně. Další je možnost platby ve smyslu převodu hodnot či kapitálu, kdy nedochází k protipohybu zboží a služeb. Třetí základní funkcí peněz je vlastnost měřit hodnotu zboží nebo služeb a umožnit tak jejich porovnání, jakožto zúčtovací jednotky. Čtvrtou a poslední je funkce uchovatele hodnoty, kdy ovšem tato podmínka funguje jen v laboratorních podmínkách z důvodů současného krytí peněz a inflace. Příkladem může být bankovka v nominální hodnotě 1.000,- Kč uspořena z roku 1993 kdy, ačkoliv se jedná o stejnou bankovku, jako tehdy, její reálná hodnota v roce 2023 je díky kumulativní inflaci cca 285,- Kč.

Výsledky porovnání funkce peněz a virtuálních měn znázorňuje následující tabulka.

€	oběživo	platidlo	zúčtování	hodnota
Peníze	ano	ano	ano	ano (inflace)
Virtuální měna	ano	ano	ne	Ano/ne

Z této vyplývá, že dvě ze čtyř základních funkcí, oběživo a platidlo, jsou jak pro reálné peníze, tak pro virtuální měnu společné, ačkoliv v případě virtuálních měn se

¹ *Ecb.europa.eu. Co jsou peníze? Online. 2017, 20. 6. 2017. Dostupné z: https://www.ecb.europa.eu/ecb/educational/explainers/tell-me-more/html/what_is_money.cs.html. [citováno 2024-02-09].*

zdaleka nedá hovořit o všeobecně přijímaném prostředku. Problém nastává u zúčtovací funkce, která je ovlivněna vysokou volatilitou virtuálních měn, a je tedy pro sledování zcela nevhodná. Co se týče poslední funkce, kterou je uchovatel hodnoty, tak zde dochází ke střetu dvou protichůdných faktorů. Virtuální měny jsou obvykle nastaveny jako deflační, to znamená, že jich je či bude vytěžen určitý konečný počet (20 999 999,9769 u bitcoinu²) a díky možnosti vlastnit a platit pouze jejich frakcí, nenarážíme tu na žádné mantinely ohledně nedostatku. Otazníkem ovšem zůstává jejich hodnota, která je stejně jako ekonomika, závislá na mnoha vnitřních i vnějších faktorech, které přispívají k vysoké volatilitě, někdy i v řádu desítek procent během krátkého časového úseku.

1.2 Virtuální měny x elektronické peníze

Zařazení virtuálních měn pod kategorii elektronických peněz by se mohla zdát jako logická varianta vzhledem k možnosti využití počítačové sítě, jakožto zajištění platebního systému.

Řečí zákona o platebním styku:

„Elektronickými penězi je peněžní hodnota, která

a) představuje pohledávku vůči tomu, kdo ji vydal,

b) je uchovávána elektronicky,

c) je vydávána proti přijetí peněžních prostředků za účelem provádění platebních transakcí a

d) je přijímána jinou osobou než tím, kdo ji vydal.“³

Problém ovšem nastává již v písmeni a) paragrafového znění, kdy nepředstavují pohledávku vůči tomu, kdo ji vydal, a proto jak Česká národní banka, tak Evropský orgán pro bankovníctví virtuální měny nepovažuje za elektronické peníze. Čím tedy jsou? ČNB má ke kryptoměnám dosti rezervovaný postoj a až na několik varování ohledně podvodných jednání ve spojitosti s kryptoměnou jako

² Kurzy.cz. *Co bude s Bitcoinem po vytěžení poslední mince?* Online. 13.02.2023. Dostupné z: <https://www.kurzy.cz/zpravy/697673-co-bude-s-bitcoinem-po-vytezeni-posledni-mince/>. [citováno 2024-02-09].

³ Zákon č. 370/2017 Sb., o platebním styku § 4 odst. 1

neregulovanou složkou, lze pouze vycházet z vyjádření z roku 2017, tehdejšího viceguvernéra Mojžíra Hampla, že se chovají jako komodita a je třeba k nim tak přistupovat.⁴ Toto vyjádření ovšem nenese oporu v zákoně, leč má částečnou podporu v bodě 125 preambule k MiFID II.⁵ Ve speciálních případech však může být kryptoaktivum investičním nástrojem nebo elektronickým platidlem, tudíž jednodušší než jej někde zařazovat, je stanovit, že jde o zvláštní kategorii věcí. Zajímavostí, která stojí za zmínku určitě je, že z pohledu finanční správy ČR a z hlediska daní z příjmů jsou kryptoměny považovány za věc nehmotnou, movitou a zastupitelnou.⁶ Paradoxně tedy, ačkoliv virtuální měny – kryptoaktiva, postrádaly zákonné vymezení, víme, že se na ně vztahuje povinnost danění zisku.

⁴ HAMPL, Mojmír. *Náš postoj ke kryptoměnám? Nepomáhat, nechránit, neškodit, nevodit za Ruku.* Cnb.cz. Online. 2017, 21. 12. 2017. 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/>. [citováno 2024-02-09]

⁵ Směrnice Evropského parlamentu a Rady (EU) 2014/65 ze dne 15. května 2014 o trzích finančních nástrojů a o změně směrnic 2002/92/ES a 2011/61/EU.

⁶ Finanční správa. *Informace k daňovému posouzení transakcí s kryptoměnami.* Online. 2022. Dostupné z: https://www.financnisprava.cz/assets/cs/prilohy/d-seznam-dani/Info_kryptomeny_GFR.pdf. [citováno 2024-02-09].

2. Legislativní ukotvení virtuálních měn

2.1 Zákon AML

Z celkového pohledu zákonodárce víceméně do roku 2023 tápal nad způsobem uchopení a regulací virtuálních měn. Částečně se tímto problémem zabývá zákon č. 253/2008 Sb. o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu (anglicky AML – Anti Money Laundering), který po své novelizaci označuje virtuální měny za virtuální aktivum a zavádí do problematiky řadu opatření a regulací. Z tohoto pohledu důležité ustanovení v § 2 odst. 1 písm. l), ve kterém se jako povinná rozumí osoba poskytující služby spojené s virtuální měnou, tedy (dle § 4 odst. 8 téhož zákona) každá osoba, která v rámci předmětu své podnikatelské činnosti kupuje, prodává, uchovává, pro jiného spravuje nebo zprostředkovává nákup nebo prodej virtuální měny, případně poskytuje další služby spojené s virtuální měnou. Zároveň zde zákonodárce vymezuje povinnosti především ve vztahu převodu virtuálních měn do fiat měny, a to nastavením hranice pro směnu ve výši 1.000 eur, nad kterou podmiňuje identifikaci účastníků, jak skladatele, tak příjematele. Důkladnější kontrolu musí banky a další povinné osoby provést v případě částky převyšující 15.000 eur. Tímto je defacto na povinné kladena povinnost nutnosti kontrolních mechanismů, jelikož zavádí dále povinnost ohlásit podezřelý obchod Finančně analytickému úřadu (FAÚ). FAÚ má poté oprávnění až na dobu 72 hodin nařídit povinnému odložení platby k prověření podezřelých skutečností. Základními zásadami je v tomto případě rychlost prověření a jak nařizuje i samotný zákon povinnost mlčenlivosti o tom, že byl FAÚ upozorněn. V důsledku nařízení přineslo firmám působícím na poli kryptoměn v ČR nemalé problémy, protože jim banky odmítají vést účty.⁷

⁷ STROUKAL, Dominik. *Poslední banka ruší účty kryptofirmám. Přitom k tomu není žádný důvod.* E15.cz. Online. 4.4.2023. Dostupné z: <https://www.e15.cz/nazory-a-analyzy/posledni-banka-rusi-ucty-kryptofirmam-pritom-k-tomu-neni-zadny-duvod-1397521>. [citováno 2024-02-09].

2.2 KYC – Know your customer

Jako opora v rámci zákona AML byl dále vytvořen kontrolní mechanismus zvaný KYC, česky „Poznej svého klienta“. Tento vyžaduje po poskytovatelích finančních služeb, aby shromažďovali informace, jednak bezpečně prokazující identitu klientů a dále, aby pomohli určit míru rizika a druh klienta vůči finanční instituci, vzhledem k předpokládaným transakcím. K ověření je většinou třeba dvou dokladů totožnosti, případně v kombinaci s bankovním výpisem.

2.3 MiCA – CASP

V roce 2023 byla za českého předsednictví EU dojednána finální podoba komplexní regulace kryptoaktiv s názvem MiCA (Markets in Crypto Assets) zavádějící pojem CASP (Crypto-asset Service Provider), jakožto licencovaného poskytovatele služeb souvisejících s kryptoaktivy. Nařízení je legislativním návrhem s cílem vytvořit jednotný právní rámec pro trh s virtuálními aktivy napříč zeměmi Evropské unie, které rozšiřuje MiFID II a její obsah podrobněji zpracovává.

Licenci dle MiCA podléhá:

- a) poskytování úschovy a správy kryptoaktiv jménem zákazníků;*
- b) provozování obchodní platformy pro kryptoaktiva;*
- c) směna kryptoaktiv za peněžní prostředky;*
- d) směna kryptoaktiv za jiná kryptoaktiva;*
- e) provádění pokynů ke kryptoaktivům jménem zákazníků;*
- f) umístování kryptoaktiv;*
- g) přijímání a předávání pokynů ke kryptoaktivům jménem zákazníků;*
- h) poradenství týkajícího se kryptoaktiv;*
- i) poskytování správy portfolia kryptoaktiv;*

j) poskytování služeb převodu kryptoaktiv jménem zákazníků⁸

V účinnost směrnice nabývá již v první polovině roku 2024, kdy se předpokládá, že konec přechodného období pro kompletní implementaci a vymáhání bude přelom roku 2025/2026. Už dnes je ale jisté, že vzhledem k neustálému vývoji v rámci celého informačního odvětví, bude nutné neustále pružně přizpůsobovat i legislativu.

⁸ Nařízení evropského parlamentu a rady (EU) 2023/1114 ze dne 31. května 2023 o trzích kryptoaktiv a o změně nařízení (EU) č. 1093/2010 a (EU) č. 1095/2010 a směrnic 2013/36/EU a (EU) 2019/1937 Čl. 3 odst. 1 bod 16).

3. Kryptoměny

Z názvu práce je zřejmé, že kryptoměna a legalizace výnosů z trestné činnosti jsou stěžejními pojmy, které je vhodné řádně objasnit. Zákonem AML jsou kryptoměny definovány jako virtuální aktiva následovně:

„elektronicky uchovatelná nebo převoditelná jednotka, která je

a) způsobilá plnit platební, směnnou nebo investiční funkci, bez ohledu na to, zda má nebo nemá emitenta, pokud se nejedná o

1. cenný papír, investiční nástroj, nebo peněžní prostředek podle zákona o platebním styku,

2. jednotku podle § 3 odst. 3 písm. c) bodů 4 až 7 zákona o platebním styku, nebo

3. jednotku, kterou je prováděna platba podle § 3 odst. 3 písm. e) zákona o platebním styku, nebo

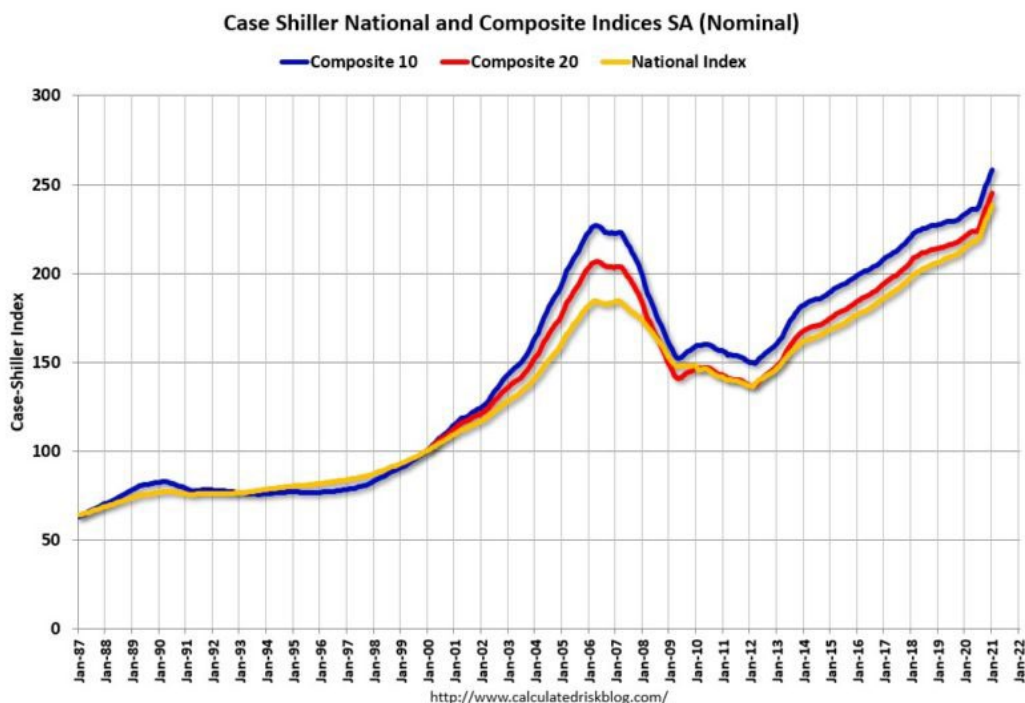
b) jednotkou podle písmene a) bodu 2 a kterou lze v konečném důsledku zaplatit pouze za úzce vymezený okruh zboží nebo služeb, který zahrnuje elektronicky uchovatelnou nebo převoditelnou jednotku podle písmene a).“⁹

⁹ Zákon 253/2008 Sb. § 4 odst. 9

Jak bylo uvedeno výše, jedná se o druh kryptoaktiva, který je decentralizovaný a není kontrolován žádnou centrální autoritou, ať už se jedná o centrální banku či vládu. Základem pro vytváření nových jednotek a samotné zajištění transakcí je kryptografie. Od tohoto je odvozen název skládající řecké kryptos (skrytý, tajný) a měna ve smyslu finančního prostředku.

3.1 Vznik kryptoměn v souvislostech

Vezmeme-li Bitcoin jako výchozí bod pro samotnou existenci životaschopný či spíše trhem akceptovatelných kryptoměn, musíme příčiny jeho vzniku zasadit do širšího kontextu. Pokud se podíváme okem statistiky na vývoj cen nemovitostí v USA začátku milénia dále, zjistíme takřka raketový růst, který dosáhl svého maxima roky 2006 a 2007. Vina byla především na straně regulátora, tedy FEDu, který díky nízkým úrokovým sazbám poskytoval „levné peníze.“ Tyto následně vytvářely tlak na růst cen a u hypoték vytvářely tzv. bublinu, která nafukovala reálnou hodnotu nemovitostí, až tato bublina splaskla. Poté následovala hypotéční krize v USA a díky provázanosti globálního bankovníctví a ekonomiky i po celém světě.



Index sledující dynamiku růstu cen nemovitostí v USA ¹⁰

¹⁰ Finlord. *Ceny nemovitostí v Usa raketově rostou*. Online. 2021, 1.4.2021. Dostupné z: <https://finlord.cz/2021/04/ceny-nemovitosti-usa-raketove-rostou/>. [citováno 2024-02-09].

Jsou tedy kryptoměny reakcí na ekonomickou krizi? Ano, na základě tří základních tezí:

- a) Ztráta důvěry ve finanční instituce – zavedení decentralizovaného systému.
- b) Manipulace s penězi – transparentní, otevřený systém – blockchain.
- c) Ochrana před inflací – jak bylo napsáno výše, kryptoměny jsou koncipovány jako deflační nástroj

3.2 Bitcoin

Pro drtivou většinu lidí je právě bitcoin synonymum pro kryptoměny. Rozhodně se jedná o nejpoblárnější a nejpoužívanější kryptoměnu s tržní kapitalizací 928,5 Miliard USD, což představuje dominanci Bitcoinu 49.67 % v poměru vůči ostatním kryptoměnám.¹¹

Jak již bylo zmíněno v úvodu, nelze na Bitcoin pohlížet pouze jako na platební prostředek. Bitcoin představuje komplexní platební, výpočetní a účetní systém fungující na principu peer to peer (P2P), který je kryptograficky zajištěn. Pro úplné pochopení je tedy vhodné rozlišovat bitcoin, jako aktivum určené k platbám a nejbliže podobné fiat penězům a Bitcoin jako prostředí. Platí tedy že bitcoin je měnová jednotka, která je podmnožinou Bitcoinu.

Princip fungování Bitcoinu

Bitcoin se stala první decentralizovanou sítí pro P2P platby a virtuální měnou, fungující jako online hotovost. Jedná se o systém s otevřeným zdrojovým kódem, umožňující jeho uživatelům jej pseudonymně využívat do doby, než je jeho adresa propojena s konkrétní osobou, především při směně na fiat měnu.

Každá transakce je zaznamenávána do veřejné elektronické účetní knihy – blockchainu, kdy tyto se automaticky propisují mezi všechny provozovatele bitcoinové sítě a tím dochází k ověřování transakcí pomocí automaticky nastaveného protokolu. Každá platba je ověřována pomocí kryptografie za pomoci dvou klíčů, veřejného a privátního. Pro lepší chápání si můžeme privátní klíč představit jako heslo a veřejný klíč jako číslo účtu. Platba je pak provedena zadáním veřejného klíče protistrany validovanou privátním klíčem odesílatele. Následně platba dostane časový otisk a je propána do mempoolu, kde čeká na zápis do vytěženého bloku. Blok je následně zapsán do blockchainu a synchronizován s aktivními uzly v rámci celé sítě. Právě v tomto procesu dochází k ověřování, zda nedošlo ke dvojí útratě prostředků a pokud dojde k validaci platby od několika nezávislých provozovatelů, je platba definitivně schválena a je navždy propána do blockchainu.

¹¹ Coingecko. *Globální grafy tržní kapitalizace kryptoměn*. Online. 2024. Dostupné z: <https://www.coingecko.com/cs/global-charts>. [citováno 2024-02-09].

Rychlost sítě a výše zároveň i výše poplatků za validaci transakcí je přímo závislá na těžařích poskytujících celé síti výpočetní výkon. Dochází tady k tzv. důkazu o vykonané práci Proof of Work, tedy přenosu hodnot z reálného světa do kybersvěta.

Hard fork a vznik Bitcoin Cash

Vzhledem k tomu, že zdrojový kód k jakékoliv aplikaci nelze udělat bez bugů i zdrojový kód Bitcoinu měl k dokonalosti daleko. Jeho tvůrce S. Nakamoto pravděpodobně předal svou pomyslnou štafetu spočívající ve správě a údržbě systému dále již v roce 2012. Přesto práce na vylepšování kódu a jeho optimalizaci neustále probíhají. Webová platforma GitHub, sloužící jako centralizovaný server zdrojových kódů různých projektů, slouží i v případě Bitcoinu, jako veřejné diskuzní fórum, umožňující zdrojový kód stáhnout, případně podávat návrhy na jeho změnu. Komunita pak konsenzem vytváří tlak na správce ohledně implementace změn. Zároveň je na platformě GitHub speciální šifrovaný kanál pro kontakt s vývojáři pro případ, že by se v kódu vyskytla kritická chyba.

Právě různé pohledy na směřování Bitcoinu ohledně vylepšení škálovatelnosti sítě, která by umožnila rychlejší potvrzování transakcí a nižší poplatky za ně, daly za příčinu rozdělení hlavní vývojové větve tzv. hard fork¹² na Bitcoin a Bitcoin Cash. Toto rozdělení pak vytvořilo dva samostatné blockchainya a držitelé bitcoinu po rozdělení obdrželi stejné množství bitcoin cash.

¹² Kryptohodler.cz. *Co je u kryptoměny fork, jaký je rozdíl mezi hard forkem a soft forkem a končí to vždy rozvětvením sítě?* Online. 5.2.2021. Dostupné z: [https://kryptohodler.cz/hodl-co-je-fork-jaky-je-rozdil-mezi-hard-forkem-a-soft-forkem-tvrdou-a-mekkou-vidlici/#Hard fork vs soft fork](https://kryptohodler.cz/hodl-co-je-fork-jaky-je-rozdil-mezi-hard-forkem-a-soft-forkem-tvrdou-a-mekkou-vidlici/#Hard%20fork%20vs%20soft%20fork). [citováno 2024-02-09].

Vlastnost	Bitcoin	Bitcoin Cash
Velikost bloku	1 MB	8 MB (dnes 32 MB)
Poplatky za transakce	Vyšší	Nižší
Doba potvrzení transakce	Pomalejší	Rychlejší
Centralizace sítě	Vyšší	Nižší (nyní vyšší)

Tabulka srovnání vlastností Bitcoin a Bitcoin Cash

I přes zdánlivě nízkou důležitost této kapitoly byla záměrně do práce zařazena, neboť, jak bude uvedeno v kapitole JAMES ZHONG níže v textu, hard fork úzce souvisel se sekundárním výnosem z trestné činnosti.

Těžba bez potu a slz

Samotná těžba zajišťující chod sítě je vlastně spektakulární matematický proces ve hře v kostky. Hashovací algoritmus je v tomto případě použit na posloupnost dat z předchozího bloku a vytvoří se vzor vyjádřený číslem (nonce). Právě toto číslo hledají těžaři, obrazně hází kostkou, dokud nedojde ke shodě. Poté systém automaticky generuje číslo nové a hra začíná nanovo. Protokol, tak jak je napsán, v sobě obsahuje též kontrolní mechanismus spouštěný zhruba každé dva týdny. Tento následně vyhodnocuje a upravuje náročnost těžby, aby odpovídala daným pravidlům. Odměnou za vykonanou práci těžařům je připsání aktuálně daného počtu bitcoinů a poplatků za validování plateb připravených pro zápis do blockchainu. Právě poplatků za provedené platby by měl být do budoucna motivací pro udržení sítě v provozu i po vytěžení posledního bitcoinu.

Halving

Důležitým procesem při těžbě je algoritmické nastavení tzv. půlení neboli halvingu, ke kterému dochází zhruba každé čtyři roky vytěžením 210000 bloků. Halvingem dojde ke snížení odměny za vytěžení bloku o polovinu. Odhady předpovídají, že příští halving bude následovat zhruba v půlce dubna roku 2024, dosažením počtu 840000 vytěžených bloků. Z historického hlediska toto vždy vedlo

k nárůstu ceny bitcoinu, jelikož jej činí vzácnějším, a to i především k předem danému počtu vytěžitelných bitcoinů.

Platidlo bitcoin

V době psaní této kapitoly činí cena jednoho bitcoinu 37.293, - USD, což odpovídá 836.708, - Kč. Naštěstí pro běžné uživatele není nutnost držet bitcoin jako celek. Bitcoin je dělitelný na 8 desetinných míst, přičemž satoshi představuje jeho nejmenší existující jednotku, tedy 1 SAT = 0,00000001 BTC. Způsob uchování bitcoinu, jakož i dalších kryptoměn je prostřednictvím peněženek. Takovouto peněženkou může být jakékoliv zařízení připojitelné k síti internet a schopné nést bitovou informaci. Ať už se jedná o softwarové či hardwarové řešení, je třeba vyvarovat se podceňováním zabezpečení takového zařízení k uchování soukromého klíče, protože rychlost, s jakou dokáže uživatel přijít o svá kryptoaktiva, je měřitelná v řádu vteřin.

Špičkou v odvětví hardwarových peněženek pro správu kryptoměn tvořící standardy v tomto odvětví jsou produkty české firmy SatoshiLabs.

Po pořízení peněženky již nic nebrání nákupu. Obchodování či směna probíhá na specializovaných burzách a směnárnách, bitcoinmatech, investicích do CFD, přímým obchodem P2P či fyzickou formou.

Casascius – fyzický bitcoin

Popularita kryptoměn kolísá, ale celkově je na vzestupné tendenci. Trendová vlna s sebou přináší řadu možností. Vzhledem k digitální povaze kryptoměn není pro řadu lidí představitelné, že soubor jedniček a nul představuje nějakou hodnotu. Právě propojení konvenčního smýšlení o představě platidla a kryptoměn stálo za vznikem fyzické bitcoinové mince společnosti Casascius. Tato na své rubové straně obsahuje hologram, ve kterém je skrytý natištěný soukromý klíč. V roce 2011, vzhledem k tomu, že bitcoin měl řádově nižší hodnotu, se prodávaly mince v nominální hodnotě 0,1 – 1.000 bitcoinů. Naneštěstí po zásahu amerického regulátora FinCEN, skončila veškerá výroba, distribuce a podnikání firmy, jelikož tato činnost podléhala obchodní licenci pro přenos peněz. Z pohledu OČTŘ a praní špinavých peněz, je toto rozhodnutí

pozitivní, protože v případě, kdy by se na prodejce nevztahoval princip KYC či zákon AML, je tento způsob potenciální bezpečností hrozbou. Na druhou stranu pomineme-li jistou zajímavou estetickou stránku, je tento způsob uchovávání krypta přinejmenším nevhodným a nebezpečným z hlediska možné krádeže.



Fyzická mince Casascius se soukromým klíčem na hologramu¹³

V současné době je drtivá většina „fyzických bitcoinů,“ prodávaných na internetu, dekorativní a s kryptoměnami mají společné než vyražené logo. Tyto mince byly především v začátcích kryptoměn nástrojem zneužívaným podvodníky, kteří využívali neznalosti poškozených a prodávali je, jako reálnou kryptoměnu či zmíněnou Casascius minci a její obdoby.

Bitcoin ETF

V současné době má k fyzické formě bitcoinu nejbližší ETF¹⁴ (Exchange Traded Funds). První ze zásadních událostí roku 2024 přišla hned 14. ledna, kdy SEC – americká Komise pro cenné papíry a burzu po dlouhých průtazích, schválila 11 bitcoinových ETF na americké burze. Ačkoliv tyto nejsou světově prvními a v roce 2023 společnost Jacobi Asset Management uvedla bitcoinové ETF pod tickerem BCOIN na burze Euronext v Amsterdamu, bylo očekávání trhu a vliv na cenu bitcoinu

¹³ News.bitcoin.com. *Casascius Bitcoin Peels: \$10M Cashed in 2023, Yet a \$1 Billion Stash Remains Unclaimed*. Online. 4.9.2023. Dostupné z: <https://cryptonews.net/news/bitcoin/22716023/>. [citováno 2024-02-10].

¹⁴ Patria.cz. *Co jsou ETF*. Online. 2024. Dostupné z: <https://www.patria.cz/fondyderivaty/etf/popis.html>. [citováno 2024-02-10].

směřováno právě v návaznosti na amerického regulátora. Za první den fungování evidovala newyorská burza transakce v objemu 4,6 miliardy USD.¹⁵

ETF představuje investorsky atraktivní a přívětivý nástroj se zachováním nízkých provozních poplatků. V případě zmíněných spotových bitcoinových ETF jsou spravovaným aktivem přímo bitcoiny vlastněné a spravované zřizující společností, která pak následně vydává akcie veřejně nakoupitelné na burze. Investor tedy přímo neovládá žádné bitcoiny a jeho výdělek se odvíjí jednak od ceny bitcoinu, tak od schopností správce aktiv obchodovat. Fyzičnost této formy je spatřována v zalistování a regulaci ze strany autority, kdy americká vláda garantuje, v případě krachu investiční společnosti, částečnou návratnost investovaných prostředků.

Seed

V úzké souvislosti s hardwarovou peněženkou a „pravým“ vlastnictvím kryptoměny, je pojem seed, seed phrase či backup seed phrase. Právě tyto zázračná „semínka“ chcete mít v případě ztráty či poruchy kryptoměnové peněženky zmíněné výše. Jedná se o 12,15 či 24 slov v přesně daném pořadí, které zajišťují hlavní klíč a zároveň zálohu pro obnovu vaší peněženky, a tedy i přístupu ke svému kryptu. Důrazně se doporučuje uchovávat seed zabezpečený a v offline prostředí.

¹⁵ GALLISTL, Vladan. *Bitcoinová ETF zažila rekordní debut na burze. Za stovky milionů korun nakupovali i Češi*. Hn.cz. Online. 2024, 15.1.2024. Dostupné z: <https://archiv.hn.cz/c1-67284460-bitcoinova-etf-zazila-rekordni-debut-na-burze-za-stovky-milionu-koron-nakupovali-i-cesi>. [paywall]. [citováno 2024-02-10].

3.3 Altcoiny

Z výše uvedeného jasně vyplývá, že kryptoměny nejsou jen Bitcoin. Ačkoliv se pro hlubší představení nabízí Ethereum, jakožto druhá nejlépe kapitalizovaná kryptoměna na světě, bude pro značnou podobnost s Bitcoinem zacíleno na Monero (XMR) s tržní kapitalizací 3 048 776 288 USD¹⁶, tedy 27. v pořadí na trhu, jelikož úzce souvisí s problémem řešeným v této práci, a to legalizací výnosů z trestné činnosti.

3.3.1 Monero

Psal se rok 2013, kdy došlo k vydání odborného článku, whitepaperu¹⁷, vývojáře pod pseudonymem Nicolas van Saberhagen, který představil koncept kryptografické metody kruhového potvrzení transakcí blockchainu za pomoci soukromého klíče člena konkrétní skupiny uživatelů. Tímto způsobem potvrzování je nemožné určit, který klíč byl použit pro potvrzení transakce a tato se stává 100% anonymní.

Na základě tohoto konceptu byla na referenčním kódu CryptoNote vytvořena kryptoměna bytecoin, kteréž kód byl následně v roce 2014 rozštěpen a došlo k vytvoření kryptoměny bitmonero, dnes již označované čistě jako monero.

Stejně jako Bitcoin je monero open source projekt a samotná komunita navrhuje, upravuje a financuje jeho vývoj. Tímto, anonymitou tvůrců a principem Proof of work si jsou obě kryptoměny podobné, leč tady veškerá podobnost končí. Na rozdíl od Bitcoinu, počet mincí monera neustále roste a algoritmicky regulována je pouze jejich emitace. Dalším rozdílem oproti Bitcoinu je dynamická velikost bloků, adaptující se dle vytíženosti sítě. Což v praxi znamená, že při větší vytíženosti sítě, blok pojme více transakcí a tím se sníží poplatky při stejné odměně pro těžáře. Bitcoin oproti tomu, má velikost jednoho bloku omezenou na 1 MB.

V lednu 2017 byla do projektu Monero implementována funkce „Ring Confidential Transactions“ (RingCT) – kruhové soukromé transakce, které krom

¹⁶ Coingecko. *Monero*. Online. 2024. Dostupné z: <https://www.coingecko.com/cs/coins/monero>. [citováno 2024-02-09].

¹⁷ VAN SABERHAGEN, Nicolas. *CryptoNote v 2.0*. getmonero.org. Online. 17.10.2013. Dostupné z: <https://www.getmonero.org/resources/research-lab/pubs/cryptonote-whitepaper.pdf>. [citováno 2024-02-10].

základního skrývání odesílatele a příjemce skrývají navíc i hodnotu transakcí. Což znamená 100 % anonymity.

Zde se je prostor navrátit se k nařízení MiCA, které bylo prezentováno výše. Společně s tímto a jako doplňující součást, byla europoslanci schválena stěžejní regulace v boji proti praní špinavých peněz a financování terorismu, zaměřená na sledování kryptoměnových transakcí, jakožto Nařízení Evropského parlamentu a Rady (EU) 2023/1113 (Transfer of Funds Regulation). Peněžní převody by tímto byly dohledatelné, jako je tomu v klasických bankách, a to minimálně při převodu kryptoaktiv na fiat měnu. Kryptosměnárny a burzy tak budou muset evidovat a prokazatelně identifikovat, jak osobu odesílatele, tak příjemce u každé transakce přesahující částku 1.000, - eur, respektive cca 23.500, - Kč, kterou zprostředkují. Při překročení těchto stanovených částek se evidence má týkat i převodu do osobní hardwarové peněženky.

Postavíme-li proti sobě kryptoměnu Monero a článek 17 předmětného nařízení ToFR, který udává že:

„Některé převody kryptoaktiv zahrnují zvláštní vysoce rizikové faktory praní peněz, financování terorismu a jiné trestné činnosti, zejména převody související s produkty, transakcemi nebo technologiemi určenými ke zvýšení anonymity, včetně privátních peněženek a anonymizačních směšovací anebo zaměňovací služeb. Aby byla zajištěna sledovatelnost těchto převodů, měl by Evropský orgán dohledu (Evropský orgán pro bankovníctví) zřízený nařízením Evropského parlamentu a Rady (EU) č. 1093/2010 (13) (dále jen „EBA“) zejména objasnit, jak mají poskytovatelé služeb souvisejících s kryptoaktivy zohledňovat rizikové faktory uvedené v příloze III směrnice (EU) 2015/849, a to i při provádění transakcí se subjekty ze zemí mimo Unii, které nejsou regulovány, registrovány ani licencovány v žádné třetí zemi, nebo s nehostovanými adresami. Pokud jsou zjištěny situace s vyšším rizikem, měl by EBA vydat obecné pokyny, v nichž upřesní, která posílená opatření náležitě péče by povinné osoby měly zvážit za účelem zmírnění těchto rizik, včetně přijetí vhodných

postupů, jako je využití analytických nástrojů technologie distribuovaného registru (dále jen „DLT“) ke zjištění původu nebo určení kryptoaktiv,“¹⁸

pak je nutno konstatovat, že principy, na kterých byla kryptoměna vytvořena a je provozována, jsou zcela neslučitelné s předmětným nařízením a pravděpodobně povedou k jejímu zákazu.

¹⁸ Nařízení evropského parlamentu a rady (EU) 2023/1113 ze dne 31. května 2023 o informacích doprovázejících převody peněžních prostředků a některých kryptoaktiv a o změně směrnice (EU) 2015/849 článek 17

4. DeFi

Myšlenka decentralizovaného financování určitě nedá spát bankéřům a makléřům, neboť se jedná o finanční systém, který je transparentní a ke svému fungování nepotřebuje prostředníka. Dokáže díky internetu fungovat globálně a stejně snadno k němu lze přistupovat. Jak bylo popsáno v kapitole o Bitcoinu je i DeFi úzce spojeno s pojmem blockchainu. Ovšem ne Bitcoinového, který se pro DeFi nehodí, nýbrž využívajícího sítě Ethereum, případně s ním kompatibilní. A využití takové aplikace? Řešení úkolů v souvislosti s půjčkami, pojištěním, investováním nebo samotná správa aktiv prostřednictvím „smart contracts.“

4.1 Smart contract

V překladu hovoříme o chytrém kontraktu, který ovšem v zásadě nemusí být nijak zvlášť chytrý. Samozřejmě se jedná o část naprogramovaného kódu, který drtivá většina lidí neovládá, ale základem je myšlenka běžných slovních úloh základní školy. Příkaz obsažený na blockchainu tak jednoduše může znít POKUD / TAK. Splnění podmínky tedy automatizuje následek neboli akce vyvolá reakci a záleží jen na představitosti programátorů, o jaké záležitosti v souvislosti s úhradou se má jednat. Ideální například pro služby typu uhrazeno mýtné, automaticky se budou zvedat závory na mýtných branách. Jasně, transparentní, neměnné a nerasmazatelné, protože se kontakt stal součástí blockchainu.

5. ICO

Initial coin offering, neboli nabídka k zakoupení emise zaváděných mincí (coin) či tokenů. Coiny jsou myšleny vlastní technologicky distribuované databáze a plně samostatné ekosystémy nezávislé na další kryptoměně. Oproti tomu token využívá již zavedené databáze a využívá je pro fungování a správu.

Historicky nejvýznamnějším příkladem ICO je Ethereum. Jeho tvůrce Vitalik Buterin, chtěl zajistit profesionální vývoj a dostatečné financování, a proto ICO Etherea mělo následující parametry:

- a) *61 000 000 coinů prodáno veřejnosti*
- b) *11 000 000 předtěženo na účet Ethereum Foundation*
- c) *Počáteční prodejní cena 2000 ETH / 1 BTC (cca 0,3 USD), postupně se cena zvyšovala*
- d) *ICO trvalo 42 dní¹⁹*

Nezisková organizace Ethereum Foundation tím získala finanční prostředky a její další chod nebyl limitován.

V ICO může být investorem jakýkoli jednotlivec, soukromý investor, a dokonce i společnost. ICO je většinou neregulované, což může ztraktivnit financování, ale přináší to obrovské riziko podvodů.

5.1 Venture capital

Venture Capital²⁰ (rizikový kapitál) je forma investice zaměřená na společnosti v rané fázi, ve které investoři poskytují finanční prostředky výměnou za procento vlastnictví. Investoři jsou obvykle zámožní podnikatelé nebo soukromé kapitálové společnosti, které mají znalosti v oboru, obchodní zkušenosti a kupní sílu. Primárním cílem financování rizikového kapitálu je zvýšit hodnotu startupu poskytováním správných odborných znalostí, mentorství a zdrojů, které pomohou společnosti uspět.

¹⁹ Alza.cz. *ICO (VŠE, CO CHCETE VĚDĚT). Co je prvotní nabídka kryptoměny?* Online. 2019, 1.1.2019. Dostupné z: <https://www.alza.cz/ico-initial-coin-offerings>. [citováno 2024-02-10].

²⁰ Czechwealth.cz. *Venture capital*. Online. 2024. Dostupné z: <https://www.czechwealth.cz/slovník-pojmu/venture-capital>. [citováno 2024-02-10].

To pomáhá společnostem VC zvýšit jejich investiční výnosy, které jsou obvykle založeny na zhodnocení nebo nárůstu hodnoty společnosti za dané období. Investice je obvykle na několik měsíců až několik let, po kterých následuje uznání zisku nebo exit. Jak ale funguje VC financování?

Mechanismus financování rizikového kapitálu funguje tak, že prostředky startupům jsou alokovány na definovanou dobu a na konci této doby dojde k exitu investice buď prodejem společnosti, fúzí, popř. akvizice, odkupy managementem nebo dokonce IPO. Zakladatel je v tomto případě povinen mít obchodní plán, finanční plán a zprávy o ocenění firmy, aby prokázal svou důvěryhodnost, udržitelnost a schopnost generovat zisk, před potenciálním investorem. Investor pak na základě důkladné analýzy poskytne projektu finanční prostředky.

Ve spojení s kryptem jsou známé příklady, kdy podobně jako u dříve zmíněných ICO dochází k předtěžení a prodeji nových coinů či tvorbě tokenů, které touto distribucí uměle získají hodnotu ve fiat měně. Firma – distributor, po dosažení určité cílové hodnoty a na ní navázaného zisku, poté prodejem veškerých aktiv z investice vystoupí. Bohužel se v tomto případě jedná o neetické jednání, však nikoliv trestné.

Bohužel u takto financovaných firem dochází k vysokému riziku čistých podvodů. Příkladem za všechny budiž project BitConnect.

5.2 BitConnect

Investování, dá-li se to tak nazvat, v tomto projektu probíhalo mezi roky 2016 a 2018 a slibovalo účastníkům denní úrok až 1 %. Interní token s tickerem BCC byl založen na technologii proof-of-stake (PoS) s pomyslnou maximální zásobou 28 milionů BCC. Bylo plánováno, že 2,6 milionu BCC bude pocházet z těžby, zatímco zbytek bude přidán v důsledku aktivit PoS staking od účastníků sítě. Koncem roku 2017 tento projekt vylákal z investorů celkově přes 2,4 miliardy USD.

Skutečnost ovšem byla taková, že se jednalo o pyramidovou hru z investování a vyplácení na základě Ponziho schématu. Právě případy typu BitConnect²¹ podlamují důvěru veřejnosti v kryptoměny a investice s nimi spojené, ačkoliv spíše než samotná

²¹ Justice.gov. BitConnect Founder Indicted in Global \$2.4 Billion Cryptocurrency Scheme. Online. 25.02.2022. Dostupné z: <https://www.justice.gov/opa/pr/bitconnect-founder-indicted-global-24-billion-cryptocurrency-scheme>. [citace 2024-02-10].

myšlenka kryptoměn, je zde na vině lidská chamtivost a hloupost, kdy v příslibu úročení překračující 30 % měsíčně nevidí podvodné jednání.

5.3 Xixoio

Aby nezůstalo jen u zahraničních kauz, příkladnou ukázkou z české kotliny je společnost Xixoio. Název možná evokuje hlavní postavu Xi Xao, z filmu Bohové musí být šílení (The Gods Must Be Crazy). Jedná se ovšem o společnost založenou v roce 2018 se sídlem v Londýně podnikatelem Richardem Watzke.

Samotná firma se na svých webových stránkách neprezentuje jako klasický emitent kryptoměny, nýbrž tokenu, který má být vázaný na aktiva, jako jsou nemovitosti, stroje či samotné firmy. Z kryptosvěta využívá zapisování tokenů, jakožto informace o vlastnictví do blockchainu, jak bylo popsáno v kapitole o DeFi. Dále představila hybridní model ICO spojený s IPO²² (Initial Public Offering) zvaný IPCO, kterým je ve své podstatě tokenovým dluhopisem firmy.

Tímto způsobem firma emitovala svůj vlastní token XIX, který bylo možné koupit, od stanovené ceny 10.000, - Kč, ovšem nešlo jej nikde prodat, neboť to zakazovaly přímo obchodní podmínky společnosti, na které při nákupu investor přistoupil a také token nebyl obchodován na žádné burze. Hodnotu defacto kompletně určoval emitent Xixoio. Získané finance měly sloužit, stejně jako v případě startupů, pro rozvoj projektu a vyvolání zájmu firem, které by prakticky tokenizovaly svůj majetek k získání dalších financí od investorů, prostřednictvím prodeje tokenů u Xixoio.

Inovace obecně k široké podpoře veřejnosti potřebují reklamu od mediálně známé tváře. Roli užitečného idiota v tomto případě sehrál Radovan Vávra, bývalý ředitel Komerční banky a Union Banky, který měl záměr, jako předseda představenstva Českého telekomunikačního operátora SimpleCell, získat prostřednictvím Xixoio nižší stovky milionů korun. Právě s tímto narativem se zúčastnil společně s Watzkem prezentací firmy.

²² Lynxbroker.cz. *IPO průvodce: Co je IPO a jaké IPO se blíží?* Online. 2024. Dostupné z: <https://www.lynxbroker.cz/investovani/burzovni-trhy/akcie/ipo/>. [citace 2024-02-10].

Ačkoliv se proti společnosti XIXOIO ohradilo spousta lidí, kdy z kryptosvěta asi nejhlásitěji ekonom Josef Tětek²³. A i přes upozornění na webu ČNB, že společnosti nebylo uděleno žádné povolení k podnikání na finančním trhu, jelikož samotné vydávání tokenů nepodléhá dohledu a investice do alternativních investičních produktů je vysoce rizikové, podařilo se této vylákat od nejméně 2931 poškozených fyzických a právnických osob finanční prostředky ve výši nejméně 339.253.008, - Kč a 571.668, - eur.

V současné době (12/2023) bylo ze strany NCOZ zahájeno trestní stíhání dvou fyzických a jedné právnické osoby pro trestný čin podvodu. V návaznosti na téma této práce je důležité zmínit, že podle zjištění kriminalistů Watzkeho manželka z peněz ze sběrného účtu společnosti, zakoupila vilu v Těptíně u Prahy za částku 36 milionů korun. Toto jednání představuje přímo učebnicový příklad způsobu legalizace výnosů z trestné činnosti, ovšem tato nemovitost a další prostředky v souhrnné hodnotě 50 milionů korun byly policií zajištěny²⁴.

²³ WOLF, Karel. *Riziko s rozumem, nebo scam? Kolem XIXOIO víří otázky i podezření*. Forbes.cz. Online. 2021, 24.11.2021. Dostupné z: <https://forbes.cz/riziko-s-rozumem-nebo-scaml-xixoio-podezreni/>. [citace 2024-02-10].

²⁴ KUČERA, Petr. *Kauza Xixoio: Policie obvinila dva lidi kvůli podvodu*. Penize.cz Online. 2023, 4.12.2023. Dostupné z: <https://www.penize.cz/investice/449188-kaucha-xixoio-policie-obvinila-dva-lidi-kvuli-podvodu>. [citace 2024-02-10].

5.4 A16z

V kategorii VC se sluší zmínit, ne snad pro jeho podvody, jedno z globálně nejvýznamnějších VC – Andreessen Horowitz, vystupující především pod názvem A16z²⁵, jakožto jakýsi fond investorů spravující portfolio čítající 35 miliard USD, s rekordní alokací prostředků v roce 2022 do WEB 3.0 a crypto start-upů ve výši 4,5 miliardy USD²⁶. Bezpochyby se jedná o kontroverzní firmu zaměřující se převážně na maximální zhodnocení svých investic, ovšem její přínos pro rozvoj v technologickém světě je už jen z hlediska vynaložených prostředků nezanedbatelný. Příkladem může být jejich portfolio, které zahrnuje finanční angažovanost ve společnostech jako jsou Airbnb, Facebook, Roblox, Wise či níže v tabulce uvedené projekty v souvislosti s kryptem.

²⁵ OKAFOR, Amina. *A16z Review*. Coinweb.com. Online. 2024. Dostupné z: <https://coinweb.com/comparison/best-crypto-vc-firms/a16z/>. [citace 2024-02-10].

²⁶ KONRAD, Alex. *A16z Crypto's Record New \$4.5 Billion Fund Doubles Down On Web3 Amid Market Crash*. Forbes.com. Online. 2022, 25.5.2022. Dostupné z: <https://www.forbes.com/sites/alexkonrad/2022/05/25/a16z-crypto-record-4th-fund-doubles-down-on-web3-amid-market-crash/>. [citováno 2024-02-10].

6. NFT

Speciální kategorií ve světě krypta je NFT neboli non-fungible token, v překladu nezaměnitelný token. Jeden bitcoin je snadno zaměnitelný za další jeden bitcoin a zřejmě právě toto vedlo programátorské „umělce“ k vytvoření jedinečného, nezaměnitelného tokenu. Tento token dokáže nést digitální informaci, u které je díky blockchainu dané její vlastnictví. Je otázkou vkusu a rozmaru každého jedince, zda tweet, meme či animovaný obrázek v sobě uchovává vnitřní hodnotu a má své místo v portfoliu. Pohlížejeíc na problematiku očima OČTŘ, je ve věci spíše zajímavý způsob a manipulovatelnost s cenotvorbou u NFT. Příkladem budiž jeden ze znuděných opičáků #8817 prodaný za rekordní cenu 819 ETH²⁷, dle tehdejšího kurzu 3,4 mil USD dnes 1,8 mil USD (prosinec 2023). Samozřejmostí je, že ze sběratelského hlediska se cena odvíjí od ochoty sběratelů za zboží zaplatit. Ovšem když běžný uživatel začne NFT vnímat jako investiční příležitost a provede si vlastní rešerši v blockchainu, může narazit na jiná díla, která svou hodnotu třeba několikrát znásobila. Vše je v blockchainu dohledatelné a například obrázek, který původně stál 0,01 ETH se mohl několikrát prodat a jeho poslední prodejní cena je 2 ETH. Výhodná investice s takovým nárůstem ceny? Může být. Ale je někde záruka, že cenu manipulativně nevyšrouboval jeden nebo více dohodnutých uživatelů za pomoci přeprodeje mezi svými peněženkami? Být posledním článkem v tomto řetězci asi nebude úplně výhodné postavení.



28

²⁷ SHARMA, Niketam. *Top 6 Most Expensive NFT Monkey (Bored Ape) Sold Ever – NFT*. Nibleappgenie.com. Online. 2023, 17.1.2023. Dostupné z: <https://www.nibleappgenie.com/blogs/top-6-most-expensive-nft-monkey-bored-ape-sold-ever/>. [citováno 2024-02-10].

²⁸ tamtéž

7. CBDC (Central Bank Digital Currency)

Ačkoliv se kryptoměny ve světě především starších politických struktur jeví výhradně jako nástroj podporující nelegální aktivity, existují i podporovatelé a řada ekonomů, kteří v nich vidí zajímavou příležitost. Rezervovaný přístup je spíše známkou toho, že politici nikdy neschválí něco, nad čím nebudou mít jistotu kontroly či vysokého vlivu. Jak toho docílit ve světě kryptoměn?

Odpovědí je CBDC neboli Central Bank Digital Currency, digitální měna centrálních bank. Teorie digitální měny centrálních bank, regulovaná centrální autoritou je v přímém opozitu k decentralizovaným kryptoměnám. Zpochybňované je i v tomto případě využití blockchainu. Hodnota digitální měny by pak byla vázána na zavedenou fiat měnu, ovšem v programovatelné verzi, která sebou může nést vážná rizika.

Vzhledem k tomu, že nejdále je s projektem centrální digitální měny Čína s digitálním jüanem, budí tato technologie velkou dávku kontroverze. Ať už z pohledu toho, zda má být Čína vzorem pro fungování západního světa, či důvody proč právě komunistická Čína má zájem na tom provozovat čistě digitální měnu s centrální autoritou.

Otázka soukromí

V případě Číny je třeba brát ve zřetel, že digitální měna přináší společně se zavedeným sociálním kreditním systémem, mocný nástroj v rukou státu. Co zahrnuje kreditní systém?

- a) *„dodržování legislativy (snížení v případě dopravních přestupků, jízdy na černo nebo kouření na zakázaných místech)*
- b) *ekonomického chování (úprava podle struktury nákupů a řádného placení účtů a daní)*
- c) *sociálního chování (úprava v závislosti od kreditu lidí, s nimiž občan komunikuje)*

d) *způsobu využívání digitálních technologií (hraní počítačových her, čas strávený na sociálních sítích, sdílení nevhodného obsahu nebo šíření fake news).*²⁹

Kombinace zmíněných faktorů vede ke ztrátě soukromí jednotlivce a programovatelné peníze v rukou státu mohou vést i k úplnému převzetí kontroly nad prostředky či omezení přístupu k některým službám či finančním produktům. Jedinou výhodou by mohlo být omezování plateb za některé služby v případě, že by digitální peníze byly poskytovány jako sociální dávky a tím účelně vynaloženy pro zamýšlené potřeby. Ovšem je otázka debaty a rozsáhlého konsenzu, zda by tímto nebyla ve větší než nezbytné míře, omezena lidská práva.

Další nebezpečí spočívá v programovatelnosti digitálních peněz ve smyslu data jejich spotřeby. Principem spotřební ekonomiky jsou peníze v neustálém oběhu, tedy jejich utrácení a návrat do oběhu, který přispívá k růstu HDP. Stanovením data spotřeby peněz, by společně s negativním úrokem, který byl již v řadě evropských zemí aplikován, k návratnosti jistě vedl. Poté opět na povrch vyvstává otázka svobodné vůle a vlastnického práva.

²⁹ CzechTrade. *Čína zavádí sociální kreditní systém. Co to znamená?* Online. 2020, 2.9.2020. Dostupné z: <https://www.businessinfo.cz/clanky/cina-zavadi-socialni-kreditni-system-co-to-znamená/>. [citováno 2024-02-10].

8. Nákup a obchodování s kryptoměnou

Globální rozšíření internetu přispělo k tomu, že jeho prostřednictvím můžete v součtu několika vteřin nakoupit různé druhy zboží či služeb. Z charakteru kryptoměn jasně vyplývá, že i tyto jdou zakoupit na internetu. Tržištěm je v tomto případě burza či směnárny.

Ačkoliv základní myšlenkou kryptosvěta je svoboda a nezávislost, aplikovatelnost v praxi těmto není úplně nakloněna, neboť už samotný nákup virtuálních měn pravděpodobně proběhne v centralizované (regulované) službě. Nebo ne?

8.1 Směnárny CEX vs DEX

Směnárny můžeme rozlišit na dvojího typu, a to na zaštitěné prostředníkem, centralizované CEX, který ji provozuje a účtuje si poměrně vyšší poplatek než směnárny decentralizované – DEX. Směnárny s prostředníkem poté podléhají registraci a stejně jako na burzy se na ně bude vztahovat zmíněná regulace MiCA. V současné době zpravidla všechny uplatňují nařízení ve smyslu AML a KYC, a tedy že registraci s ověřením totožnosti podléhají transakce přesahující částku 1.000, - Eur měsíčně v rámci jedné peněženky, respektive 10.000, - Eur s doložením původu peněz. Příkladem budiž tabulka nejstarší české krypto-směnárny Simplecoin, poskytující své služby od roku 2013.

	do 200 € za 10 dní	200 – 9999 € za 30 dní	přes 10000 € za 30 dní
Povinná registrace a identifikace		● Vyžadováno	● Vyžadováno
Fotografie 2 osobních dokladů		● Vyžadováno	● Vyžadováno
Selfie s dokladem		● Vyžadováno	● Vyžadováno
Ověřovací platba		● Vyžadováno	● Vyžadováno
Ověřovací telefonát		● Vyžadováno	● Vyžadováno
Účel transakce		● Vyžadováno	● Vyžadováno
Doložení původu příjmu		-	● Vyžadováno
Individuální limity na základě zdrojů příjmů		-	● Vyžadováno

Do hodnoty 200 € v rozmezí 10 dní můžete nakupovat bez registrace a bez nutnosti ověření osobních dokladů.

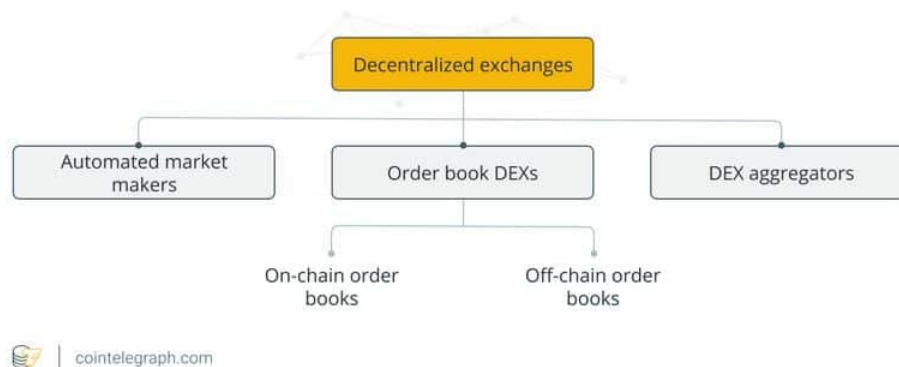
[Přejít k nákupu](#) [Registrovat](#) [Registrovat](#)

30

Druhou variantou je zmíněná DEX směnárna. Nikým neregulovaná služba, bez registrace, bez sběru citlivých dat, bez uživatelské podpory, něco jako thajský trh. Dochází zde pouze k propojování nabídky a poptávky. Prostředky obchodníků jsou vždy pod jejich kontrolou a ani v průběhu obchodu nepřechází přes prostředníka, nýbrž dochází k přímé směně. Svoboda je v tomto pro uživatele vykoupená především tím, že sebemenší chyba při převodu, je chybou fatální a dost často tou poslední.

³⁰ Simplecoin.eu. *Limity a verifikace*. Online. 2024. Dostupné z: <https://www.simplecoin.eu/cs/limits-and-verification>. [citováno 2024-02-10].

Types of decentralized exchanges



31

Decentralizované burzy (DEX) se liší především aplikovanými obchodními systémy. Jedná se o tři kategorie vypořádávání se transakcí:

- *Automatizovaní tvůrci trhu (AMM):* např. *UniSwap, SushiSwap, PancakeSwap, Curve Finance,*
- *DEXs s knihou objednávek (order bookem):* např. *Loopring, dydX, Raydium, Waves Exchange,*
- *DEX agregátory:* např. *1inch.*³²

8.2 Peer to Peer (P2P)

Právě princip p2p je pro pamětníky či zasvěcené do socialistické historie Československa až nostalgicky specifický. Fráze „Nějaký bony? Chceš bony?“ se stala kultovní, a to nejen díky kinematografii. Opustíme-li nostalgický narativ a představu šviháků postávajících před Tuzexem s vysokou morální flexibilitou, je samotný whitepaper publikovaný Satoshi Nakamotem nazvaný Bitcoin: A peer-to-peer Electronic Cash System³³, jakýmsi manifestem moderního vekslování.

³¹ Kryptomagazin.cz. *Co jsou decentralizované burzy (DEX)?* Online. 2023, 13.6.2023. Dostupné z: <https://kryptomagazin.cz/co-jsou-decentralizovane-burzy-dex/>. [citováno 2024-02-10].

³² tamtéž

³³ NAKAMOTO, Satoshi. *Bitcoin: Peer-to-Peer Systém elektronických peněz.* bitcoin.org. Online. 2009. Dostupné z: https://bitcoin.org/files/bitcoin-paper/bitcoin_cz.pdf. [citováno 2024-02-10].

P2P je založená na prosté důvěře mezi uživateli, kdy v lepších případech existuje seznam uživatelů zahrnující uživatelské skóre vycházející z předchozích hodnocení transakcí uživateli. Věrohodnost těchto hodnocení je ovšem v lepším případě pochybná a bez ověřovací autority, je zde zvýšené riziko manipulovatelnosti.

8.3 Vexl

Zlaté české ručičky a hlavičky, dozajista inspirované zmíněnou dobou, přišly s moderní aplikací, s moderním názvem a uchopily myšlenku a původní záměr v nevázanosti a nezávislosti Bitcoinu. Jak tvůrci aplikace zmiňují, hlavní výhodou je naprostá anonymita a vyhnutí se administrativě ve smyslu AML či KYC. K používání aplikace potřebujete jen zařízení s android OS či iOS s vývojářským nástrojem TestFlight³⁴ a telefonní číslo. Uživatelský profil vyplňujete na základě vlastní dobrovolnosti, tudíž může být používání aplikace zcela anonymní. Aplikace pak tvoří end to end šifrovanou sociální síť, fungující jako tržiště k propojení dvou uživatelů na základě nabídky a poptávky především na základě v telefonu uložených kontaktů a kontaktů vašich kontaktů, pro zvýšení věrohodnosti a udržení určité „vekslovací bubliny.“ Nabídka a poptávka je jediný omezující faktor aplikace. Vztaženo k tématu této práce je aplikace Vexl jeden ze způsobů nákupu kryptoměny, který prakticky znemožňuje práci OČTŘ. Jako záruka anonymního nákupu se zde používají hotovostní transakce s osobním předáním, a ačkoliv prodejci jsou označováni za tzv. „Etické veksláky,“³⁵ dokud mohou uspokojit poptávku, bude jim vždy jedno, kdo nakupuje.

8.4 ATM

Automat, který umožňuje nákup a prodej kryptoměn za hotovost. Jedná se o nejjednodušší a uživatelsky nejzajímavější způsob transakce, ne nepodobný výběru z klasického bankovního automatu. Tento luxus je ovšem vyvážen vysokým spreadem³⁶ pohybujícím se mezi 7–15 %, které slouží k pokrytí nákladů a zisku provozovatelům. V ČR došlo po masivním nárustu počtu bitcoinmatů, zejména okolo roku 2018, k částečnému ústupu, a to především ze strany nájemců, provozovatelů či

³⁴ Aplikace dostupná z <https://apps.apple.com/us/app/testflight/id899247664>

³⁵ BEDNAR, Juraj. *Etický vekslák*. Juraj.bednar.io. Online. 2020, 14.4.2020. Dostupné z: <https://juraj.bednar.io/courses/eticky-vekslak/>. [citováno 2024-02-09].

³⁶ Spread je rozdíl mezi nákupní a prodejní cenou

majitelů velkých nákupních center. Vedla je k tomu zejména řada podvodů páchaných právě prostřednictvím bitcoinů, které budou rozebrány později. Stejně jako u dříve zmíněných směnárů i zde se dle AML aplikuje zjednodušený [KYC](#) při překročení měsíčního limitu 1.000, - eur na jedné peněžence, či jejího ekvivalentu v jiné měně, respektive kompletní identifikace pak při překročení částky 10.000, - eur.

Bitcoinů jsou obecně pro svou jednoduchost považovány za největší bezpečnostní riziko a řada pronajímatelů veřejných prostor, kde jsou nejčastěji umístěny, z tohoto důvodu vypovídá provozovatelům nájemní smlouvy. Pro OČTŘ je umístění bitcoinů alespoň z části příhodné, jelikož se často jedná o monitorované prostory, a tak je tu větší pravděpodobnost využití operativně pátracích prostředků či získání důkazního materiálu.

9. Legalizace výnosů z trestné činnosti

Pojem legalizace výnosů z trestné činnosti nebo spíše praní špinavých peněz, jak jej zná drtivá většina veřejnosti a vychází tak i z překladu anglického money laundering, je závažným problémem ve společnosti. Jak už jeho název napovídá podstatou je zastřít pravý původ peněz či obdobných prostředků získaných nelegální cestou, pro jejich následné užití v reálném životě a ekonomice, bez vyvolání pozornosti ze strany úřadů. Řečí zákona č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu neboli české verze zákona AML, jak je uvedeno:

„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; uvedené jednání spočívá zejména:

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 páčání 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).“³⁷*

³⁷ Zákon č. 253/2008 Sb. § 3 odst. 1

Právníkům rozkladem předchozího paragrafového znění zjistíme, že zákonodárce nevyjadřuje v rámci subjektivní stránky jednání v úmyslu, leč je zdůrazněna jeho vědomost v původu ekonomické výhody v souvislosti s trestným činem. Trestnost legalizace výnosů z trestné činnosti je pak obsažena v § 216 respektive § 217 tr. zákoníku.

Globální pohledem je ze strany OECD odhadováno, že asi 3 % celosvětového HPD je každoročně vypráno v rámci legalizace výnosů z trestné činnosti, což činí částku 3,04 bilionu USD³⁸.

Není proto vzhledem k obrovskému objemu divu, že praní špinavých peněz je úzce spjato s pojmem organizovaného zločinu. Ze zprávy Ministerstva vnitra – Situace v oblasti organizovaného zločinu na území ČR za období 2016-2023³⁹ vyplývá, že nejčastějšími trestnými činy v ČR v souvislosti s organizovaným zločinem jsou především nedovolená výroba a jiné nakládání s omamnými a psychotropními látkami a jedy dle § 293 tr. zákoníku, krádež a podvod dle § 205 respektive § 209 tr. zákoníku a korupční trestné činy zjednání výhody při zadání veřejné zakázky, při veřejné soutěži a veřejné dražbě obsažené v § 256 tr. zákoníku. Zejména u prvních čtyř jmenovaných trestných činů je vysoký předpoklad využití virtuální měny.

9.1 Organizovaná kybernetická kriminalita

Celková kriminalita prochází dynamickým vývojem, při kterém dokáží být efektivně využívány moderní technologie. Nejinak je tomu v kyberprostředí, které si vybudovalo vlastní komplexní ekosystém. Tento lze definovat třemi základními prvky – dynamičností, profesionalizací a interaktivitou. Prvkem dynamičnosti je na mysli rychlý vznik a zánik operujících jednotek a vzájemný přesun jejich členů. Druhým klíčovým prvkem je profesionalizace projevující se především sofistikovaností kyberkriminálních aktivit se zaměřením na maximální zisk. Výjimkou není ani použití úspěšného moderního legálního modelu ve formě „as a service“,⁴⁰ při kterém je za

³⁸ Credas.com. *OECD MONEY-LAUNDERING LEADER BOARD*. Online. 2022, 25.5.2022. Dostupné z: <https://credas.com/news/oecd-money-laundering-leader-board/>. [citováno 2024-02-10].

³⁹ Ministerstvo vnitra. *VYHODNOCENÍ SITUACE V OBLASTI ORGANIZOVANÉHO ZLOČINU NA ÚZEMÍ ČR ZA OBDOBÍ 2016–2023*. Praha: Ministerstvo vnitra ČR, 2023. Dostupné pouze pro vnitřní potřeby PČR

⁴⁰ Consultancy.eu. *‘As a service’ business models: What it is and its benefits*. Online. 2022, 3.5.2022. Dostupné z: <https://www.consultancy.eu/news/7350/as-a-service-business-models-what-it-is-and-its-benefits>. [citováno 2024-02-10].

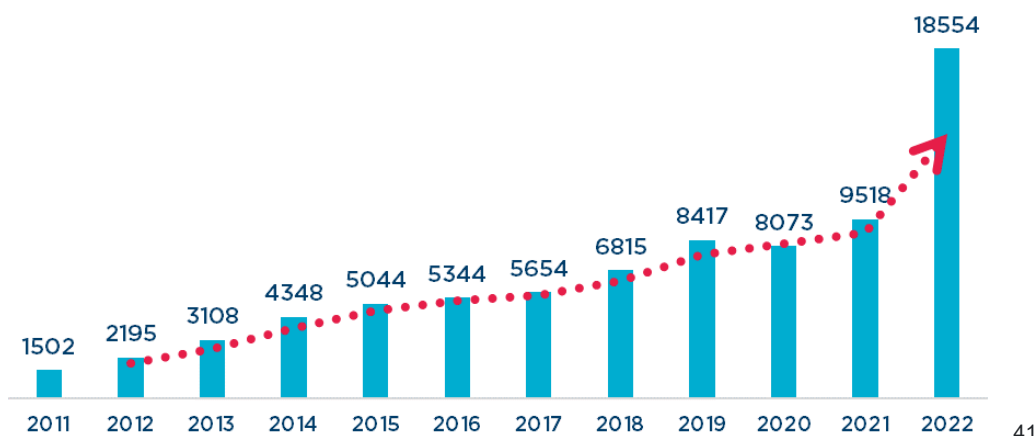
poplatek poskytována expertní služba externím dodavatelem. Osoba či firma disponující dostatečnými finančními prostředky, tak může využívat sofistikovaných nástrojů, bez nutnosti znalostí v dané problematice tzv. kriminální outsourcing. Prvek interaktivity je pak zapojen ve sdílení kriminálního know-how, jednak při fluktuaci členů skupin či vzájemnou komunikací dané komunity. Virtuální měna bývá v uvedených případech jedním z nástrojů organizovaného zločinu, vzhledem k nízké znalosti problematiky ze strany OČTŘ a složitosti stopování a následného odčerpávání těchto prostředků.

V ČR bývají kryptoměny zneužívány v souvislosti s trestnou činností v drtivé většině u investičních podvodů. Vyšetřování takovýchto trestných činů bývá značně problematické, a to nejen s ohledem na anonymitu kryptoměn, ale i kvůli pozdnímu oznámení poškozených, kteří rozpoznají podvodné jednání až s velkou prodlevou.

9.2 Kyberútoky

Pohybujeme-li se neustále v kyberprostředí, je nutné zmínit riziko kyberútoků. Z přehledu vývoje registrovaných trestných činů v kyberprostředí v ČR je patrný takřka dvojnásobný nárůst mezi roky 2021–2022 a představa, že by tomu do budoucna bylo jinak, je přinejmenším naivní.

POČTY REGISTROVANÝCH TRESTNÝCH ČINŮ PÁCHANÝCH V KYBERPROSTORU POLICIE ČR



⁴¹ Policie ČR. *Statistické přehledy kriminality za rok 2022*. Online. 2023. Dostupné z: <https://www.policie.cz/clanek/statisticke-prehledy-kriminality-za-rok-2022.aspx>. [citováno 2024-02-10].

Z veřejných sdělovacích prostředků se dozvídáme případy kybernetických útoků na kryptoburzy, kryptosměnárny či různé dokonce i státní instituce. Nejinak by tomu bylo i v případě správce digitálních peněz a oběžného systému, což by mohlo vést, jak ke ztrátě finančních prostředků, tak ke ztrátě identity, či v nejhorším případě paralyzování celého systému. Za příklad může sloužit pátek 3. 3. 2023 a několikahodinový výpadek bankovních služeb ČSOB způsobený kybernetickým útokem⁴².

9.3 Fáze praní peněz

Smyslem praní špinavých peněz je uvést nelegálně získané prostředky zpět do ekonomiky, aby bez podrobného zkoumání nevyvstaly pochyby, že se jedná o příjem z legálních zdrojů. K tomuto účelu vedou postupné na sebe navazující kroky rozdělené podle teorie do tří fází: namáčení, namydlení a ždímání. Dle Dvořáka je daleko přesnější pojmosloví: „umístění, rozmístění a integrace,⁴³ které sice tematicky nekoresponduje s představou pracího procesu ve smyslu očisty, ale o to více vystihuje podstatu samotné legalizace peněz, a které je překladem anglických pojmů: placement, layering a integration. Vztaheno k tématu této práce:

1. Umístění – převedení konvenční měny na kryptoměnu.
2. Rozmístění:
 - a) Rozdělení na několik menších částí při vytvoření řetězce převodů.
 - b) Převod na jinou kryptoměnu.
 - c) Využití mixéru virtuálních měn.
3. Integrace – prostředky se vrací do oběhu jako zdánlivě legální.

⁴² ZELENÝ, Petr. *Kvůli kyberútoky nefungovaly několik hodin některé služby ČSOB*. ČTK. Online. 2023, 3.3.2023. Dostupné z: <https://ct24.ceskatelevize.cz/domaci/3569084-kvuli-kyberutoku-nefunguji-nektere-sluzby-csob-neni-jasne-jak-dlouhy-vypadek-bude>. [citováno 2024-02-10].

⁴³ PRCHAL, Lukáš. *Od igelítek ke kryptoměnám: pachatelé praní špinavých peněz přicházejí na stále nové metody*. Ekonom.cz. Online. 2018, 9.4.2018. Dostupné z: <https://pravniuradce.ekonom.cz/c1-66103630-od-igelitek-ke-kryptomenam>. [citováno 2024-02-10].

9.4 Mixér virtuálních měn

Z každoročního reportu společnosti Chainalysis vyplývá, že již v červenci 2022 bylo prostřednictvím mixérů vypráno necelých 10 % všech kryptoměn držených nelegálními subjekty.

Základním principem mixérů je získat, pokud možno 100 % anonymizované kryptoměny tím, že dojde k promíchání různých druhů kryptoměn sdružených pod správou jednoho prostředníka – firmy, který za provizi provede několik převodů či výběrů a vkladů v náhodných částkách a tyto následně redistribuuje zpět uživatelům. Tímto způsobem se může stát, že uživatel získá část kryptoměn, které pochází z trestné činnosti a tím pádem jsou v zájmu OČTŘ.

Vzhledem k cílenému procesu zamezení vystopovatelnosti kryptoměn na poli kryptomixérů je zde, více než kde jinde, kladen důraz na kvalitní analytické nástroje. Dílčích úspěchů i v této oblasti dosahuje společnost Chainalysis se svým softwarem Reactor rozebraným v samostatné kapitole.

Používání je kryptomixérů vysoce rizikovou záležitostí pro každého uživatele, ať už z hlediska nově nabytého krypta s neznámou historií, či z hlediska důvěryhodnosti provozovatele této služby. Jakýkoliv dohled ze strany úřadů či aplikace KYC a pravidel AML je v přímém rozporu principu fungování této služby a jediná možnou regulací je v tomto případě úplný zákaz.

10. Zahájení úkonů trestního řízení

Policie České republiky je v hierarchii OČTŘ ta, která na základě vlastních poznatků, trestních oznámení a sdělení od jiných orgánů, zahajuje úkony trestního řízení dle ustanovení § 158 odst. 3 tr. řádu, plyne-li z těchto důvodné podezření, že byl spáchán trestný čin.

10.1 Podpůrné operativně pátrací prostředky

Vlastní poznatky jsou především získávány za pomoci podpůrných operativně pátracích prostředků obsažených v § 73 – § 77 zák. č. 273/2008 Sb. O Policii České republiky. K tématu této práce pak přichází v úvahu smysl využití § 73 informátor, převážně v kombinaci s § 77 zvláštní finanční prostředky.

Informátorem často bývá osoba, která se pohybuje v kriminálním prostředí a bývá obeznámena s probíhající trestnou činností např. v rámci organizace. Ačkoliv převážně za využití postupu dle § 55 odst. 2 tr. řádu. utajení totožnosti a podoby svědka může i informátor být svědkem, bylo by chybou jej takto označovat. Ačkoliv informace získané mimo trestní řízení, nejsou procesně využitelné, mohou sloužit právě jako klíčový materiál k zahájení úkonů trestního řízení, které umožňuje postupy dle trestního řádu rozebrané níže.

V souvislosti s praním špinavých peněz je nejpravděpodobnějším jiným orgánem FAÚ, Finanční správa či různé bankovní a finanční instituce.

10.2 FAÚ – Finanční analytický úřad

FAÚ je finanční zpravodajská jednotka České republiky spolupracující v celosvětové síti obdobných zpravodajců. Zároveň je v České republice hlavním gestorem opatření zaměřených na prevenci a boj proti praní špinavých peněz, financování terorismu a šíření zbraní hromadného ničení. Činnost a kompetence FAÚ jsou vymezeny zákonem AML či zákonem č. 69/2006 Sb., o provádění mezinárodních sankcí.

11. Dokazování v trestním řízení

Dá-li se ve spojitosti s justicí hovořit o moderních trendech, je jím institut spolupracujícího obviněného ve smyslu § 178a tr. řádu. OČTŘ jsou tím postaveny do pohodlnější pozice v případě obstarávání důkazů. Bohužel nežijeme v ideálním světě a většinou pokud si pachatel není jistý, že mu „teče do bot,“ spolupracuje pouze minimálně či vůbec.

Jednou ze základní zásad kybersvěta je vytvoření silného a jedinečného hesla. Nejinak je tomu v případě kryptoměn u hardwarových peněženek. Při použití 8místného hesla, které je kombinací malých písmen, velkých písmen, čísel a speciálních znaků klávesnice, se dostáváme na číslo 6.634.204.312.890.620 variant.⁴⁴ Takové heslo by pak bylo možné prolomit cca za 21 let. Ačkoliv se některé kauzy táhnou, není zdaleka možné čekat tak dlouho. Proto více než u jiných kauz, je zde důležité specializované vybavení, ať už ve smyslu lidských, tak materiálních zdrojů. Dalším aspektem je spolupráce firem, v případě, že jsou kryptoměny stále na účtu podezřelých nebo spolupráce podezřelých při výdeji, těchto hesel. U podezřelých a svědků, ovšem musíme mít na paměti zásadu zákazu sebeobviňování, lépe známou jako odmítnutí výpovědi ukotvené v článku 37 Listiny základních práv a svobod:

„(1) Každý má právo odepřít výpověď, jestliže by jí způsobil nebezpečí trestního stíhání sobě nebo osobě blízké.“⁴⁵

respektive § 100 tr. řádu, ve kterém stojí:

„Právo odepřít výpověď“

(1) Právo odepřít výpověď jako svědek má příbuzný obviněného v pokolení přímém, jeho sourozenec, osvojitel, osvojenec, manžel, partner a druh; jestliže je obviněných více a svědek je v uvedeném poměru jen k některému z nich, má právo odepřít výpověď stran jiných obviněných jen tehdy, nelze-li odloučit výpověď, která se jich týká, od výpovědi týkající se obviněného, k němuž je svědek v tomto poměru.“⁴⁶

⁴⁴ PAVELKA, Jindřich. *Heslo*. Hazardni-hry.eu. Online. 2024. Dostupné z: <https://www.hazardni-hry.eu/pravdepodobnost/heslo.html#gsc.tab=0>. [citováno 2024-02-10].

⁴⁵ Ústavní zákon č. 2/1993 Sb. ve znění ústavního zákona č. 162/1998 Sb. a ústavního zákona č. 295/2021 Sb. čl. 37

⁴⁶ Zákon č. 141/1961 Sb. Zákon o trestním řízení soudním (trestní řád) § 100

U důkazních prostředků zajištěných k prokazování nelegálních transakcí s využitím kryptoměn, bude stejně jako u jiných případů nutné dbát na dodržení zásad zákonitosti postupu, neboť se jedná o zásadní zásah do soukromí. Vzhledem k nutné analýze „řady čísel,“ je zde vysoké riziko chybovosti, proto je nasnadě více než u běžných případů, důkladná kontrola při každém úkonu. V souvislosti s charakterem virtuálních měn, které mají být jako důkazní prostředek zajištěny, přichází dle Polčáka v úvahu především:

- „a) *pevné nosiče informací – hardware,*
- a) *získání vzdáleného přístupu k datům o kryptoměně,*
- b) *získání informací od poskytovatele služeb spojených s kryptoměnou (poskytovatelů virtuálních peněženek a směnárén).“⁴⁷*

Výše uvedené instituty proto musí být využívány bezvýhradně v souladu se zásadou zdrženlivost a proporcionality a důsledného dodržení ustanovení trestního řádu.

11.1 Součinnost s OČTŘ

K bodu získávání informací od poskytovatele služeb spojených s kryptoměnou je pak v rámci procesněprávního řízení stěžejní ustanovení trestního řádu rámcově upravující – Součinnost státních orgánů, fyzických a právnických osob kdy:

(1) *Státní orgány, právnické a fyzické osoby jsou povinny bez zbytečného odkladu, a nestanoví-li zvláštní předpis jinak, i bez úplaty vyhovovat dožádáním orgánů činných v trestním řízení při plnění jejich úkolů. Státní orgány jsou dále povinny neprodleně oznamovat státnímu zástupci nebo policejním orgánům skutečnosti nasvědčující tomu, že byl spáchán trestný čin,“⁴⁸*

kteří slouží jako univerzální podpora pro práci OČTŘ ve spolupráci fyzickými i právnickými osobami, jak v ČR, tak i mimo ni. Dožádání ve smyslu uvedeného paragrafu zajišťuje OČTŘ právo žádat o spolupráci k zajištění důležitých věcí pro potřeby vyšetřování i od osob, které nejsou přímo zapojeny do trestního řízení, a to

⁴⁷ POLČÁK, Radim; PŮRY, František a HARAŠTA, Jakub. *Elektronické důkazy v trestním řízení*. Brno: Masarykova univerzita, 2015. ISBN 978-80-210-8073-7. s. 101

⁴⁸ Zákon č. 141/1961 Sb. Zákon o trestním řízení soudním (trestní řád) § 8

bez nároku na odměnu. V případě odmítnutí spolupráce může být dotyčné osobě uložena pokuta. I v tomto případě ale musí mít OČTŘ na paměti, že platí zásada zákazu sebeobviňování zmíněného dříve.

Další omezení představuje subsidiarita použití tohoto nástroje, kdy i přes jeho všeobecnou oblíbenost, lze díky své obecnosti, použít jen v případě absence speciálních postupů ve vztahu k zajišťovanému typu důkazu. V rámci policejní praxe pak bývá neefektivnější kombinace dožádání ve smyslu stanovení § 8 s např. výzvou k vydání věci ve smyslu § 78 tr. řádu.

V policejní praxi v souvislosti s hospodářskou kriminalitou je také využíván institut dožádání ve smyslu § 8 odst. 2 tr. řádu. Tento postup je možný pouze se souhlasem státního zástupce, kterému je postup a jeho rozsah navrhován, jelikož předmětem dožádání jsou informace prolamující bankovní tajemství, údaje z evidence investičních nástrojů či zaknihovaných cenných papírů. Vzhledem k virtuální povaze prostředků by mělo při získávání informací např. od kryptosměnáren, být procesně korektní využití právě druhého odstavce.

Tabulka 1: Přehled klíčových zajišťovacích institutů

	název institutu dle znění zákona	§	základní charakter	obecnost / specialita	trvání nástroje	rozhodnutí soudu
OČTŘ žádá	Dožádání	§ 8 odst. 1	žádost o informaci / součinnost	obecný nástroj	obvykle jednorázový	při mlčenlivosti dotčeného
	Nařízení vydání údajů o telekom. provozu	§ 88a	žádost o informaci	specialita k § 8 odst. 1	jednorázový	vždy
	Výzva k předložení nebo vydání věci	§ 78	žádost o věc	obecný nástroj	jednorázový	při mlčenlivosti dotčeného
OČTŘ provádí	Odnětí věci	§ 79	oprávnění k zajištění věci	obecný nástroj	jednorázový	při mlčenlivosti dotčeného
	Prohlídka (domovní / jiných prostor / osobní)	§ 82 až § 85b				
	oprávnění k prohlídce a zajišťování	obecný nástroj	jednorázový	dle druhu prohlídky		
	Sledování osob a věcí	§ 158d	oprávnění k sledování	obecný nástroj	max. 6 měsíců	při zásahu do soukromí
	Odposlech a záznam telekom. provozu	§ 88	oprávnění k odposlechu	specialita k § 158d	max. 4 měsíce	vždy

49

11.2 Novinka § 7b tr. řádu

Návratem zpět k legislativě, jelikož článek 16 a 29 Úmluvy o počítačové kriminalitě ze dne 23. listopadu 2001 č. 104/2013 Sb. m. s. známý jako „Budapeštská úmluva o počítačové kriminalitě,“ uložila státům povinnost transponovat do legislativy oprávnění určitým OČTŘ a to: „*příkázat anebo obdobně zajistit urychlené uchovávání specifických počítačových dat, včetně provozních dat, která byla uložena prostřednictvím počítačového systému, zejména pokud existují důvody pro přesvědčení, že tato počítačová data jsou zvláště ohrožená ztrátou nebo pozměněním.*“⁵⁰ Tato změna byla vložena s účinností od 1. února 2019 zákonem č. 287/2018 Sb., jako přílepek k novele trestního zákoníku. Dle dikce úmluvy se jedná o prozatímní opatření, které má za cíl v odst. 1 komukoliv nařídit, aby po dobu až 90 dní v nezměněné podobě zachoval data či znemožnil přístup k nim, resp. v odst. 2 toto nařídit správci nebo uchovateli, to vše se souhlasem státního zástupce či bez, pokud situace nesnese odkladu. Tímto se sleduje zabránění v pokračování další trestné činnosti a dá se tak označit za operativní nástroj. Je důležité si uvědomit, že tento příkaz se nevztahuje na data vzniklá po jeho vydání. Zároveň samotné ustanovení § 7b nenahrazuje vydávací či odnímací instituty obsažené v § 78 a 79 tr. ř., je pouze jakýmsi akčním mrazícím prostředkem ve formě předběžného opatření⁵¹, obdobně jako usnesení ve smyslu § 79a tr. řádu, např. ve vztahu k bankovním účtům, které je v praxi zasílané pouze se stručným odůvodněním, z důvodu úspory času, a následně doplněno o plnohodnotné odůvodnění. Jakkoliv je toto „akční“ opatření dobrou myšlenkou, platí, že chráněné dotčené zájmy jsou obvykle identické s těmi, které jsou dotčeny při využívání institutů ve smyslu §§ 88, 88a a 158d tr. řádu. Jedná se tedy spíše o splnění povinnosti transpozice částí Úmluvy, než aby se jednalo o skutečný přínos pro procesní požadavky.

⁵⁰ Sdělení č. 104/2013 Sb. m. s. Sdělení Ministerstva zahraničních věcí o sjednání Úmluvy o počítačové kriminalitě

⁵¹ Ministerstvo vnitra. *Stanovisko obp k aplikaci ustanovení § 7b trestního řádu*. Online. Praha, Ministerstvo vnitra ČR, 2019. Dostupné z: <https://www.mvcr.cz/clanek/poskytnuti-informace-metodikatykajici-se-aplikace-7b-trestniho-radu.aspx>. [citováno 2024-02-10].

12. Operativně pátrací prostředky v souvislosti s kryptoměnou

Pokud dáme do souvislosti výhody kryptoměn v kombinaci s pácháním trestné činnosti, bylo by chybou omezovat se jen na hospodářské trestné činy, jako jsou podvody či krádeže. Jak je popsáno v kapitole JAMES ZHONG, odcizené bitcoiny byly z darknet tržiště Silk road, kde docházelo k prodeji ilegálního zboží jako jsou drogy, falešné dokumenty, pornografie, umění apod. Tento široký rozsah trestné činnosti, měl právě jeden společný jmenovatel, a tím byl platební prostředek.

Z uvedeného vyplývá, že vlastní využití operativně pátracích prostředků ke zjištění a odčerpání výnosů z trestné činnosti je vzhledem k pseudonymní či anonymní povaze kryptoměn, úkolem prakticky nemožným.

Nelze ovšem vyloučit možnost, kdy v souvislosti s vyšetřováním jiných trestných činů a nasazením operativně pátracích prostředků, mezi které dle § 158b odst. 1 tr. řádu řadíme předstíraný převod, sledování osob a věcí a použití agenta, dojde k zapojení kryptoměny, jako platebního prostředku. Z uvedených se pak jako nejpravděpodobnější jeví využití sledování osob a věcí dle § 158d tr. řádu.

V případě vzdáleného přístupu k datům, volně nedostupných v síti internet, pak bude nutné využití operativně pátracího prostředku sledování osob a věcí, ve smyslu znění § 158d trestního řádu, kde je v prvním odstavci uvedeno:

„Sledováním osob a věcí (dále jen "sledování") se rozumí získávání poznatků o osobách a věcech prováděné utajovaným způsobem technickými nebo jinými prostředky. Pokud policejní orgán při sledování zjistí, že obviněný komunikuje se svým obhájcem, je povinen záznam s obsahem této komunikace zničit a poznatky, které se v této souvislosti dozvěděl, nijak nepoužít.“⁵²

se zvláštní zřetelem na odstavec 3, jelikož se jedná o zásah do záznamu uchovávaného v soukromí, který podléhá předchozímu povolení soudce.

⁵² Zákon č. 141/1961 Sb. Zákon o trestním řízení soudním (trestní řád) § 158d odst. 1

Naopak jako zcela nevhodné se jeví použití předstíraného převodu dle § 158c tr. řádu, neboť utajit v kybersvětě totožnost státními orgány ovládaných adres pro takové uskutečnění by mohlo být přinejmenším výzvou, nehledě na nutnost nasazení sil a prostředků s nejistým výsledkem.

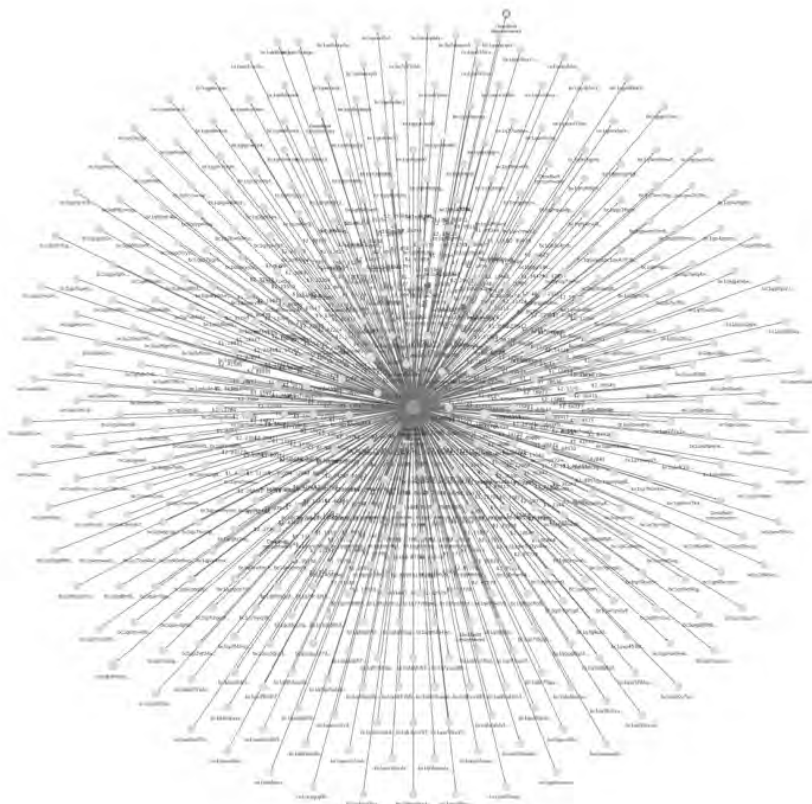
13. Zajišťování digitálních aktiv OČTŘ

Stejně jako kriminalita i justice prochází neustálým vývojem a v úzké návaznosti dochází k přechodu od tzv. inkvizičního přístupu k principu restorativní justice. Jedním z nosných pilířů tohoto principu je náhrada vzniklé újmy obětem trestných činů. Ta ve velké míře souvisí s rychlým a správným postupem OČTŘ spočívající především v zajišťování majetku a náhradní hodnoty pachatelů trestných činů. Než dojde k samotnému zajištění, je třeba řádné dohledání.

13.1 Chainalysis

Jak je blíže rozvedeno v příkladu z praxe, kapitole JAMES ZHONG, v boji proti kyberkriminalitě hrají stěžejní roli analytické nástroje pro sledování Blockchainu, tedy záznamu o pohybu prostředků z kryptopeněženek. Světovou špičkou, spolupracující s americkými či izraelskými tajnými službami, jakož i s nadnárodními bankami či fintechovými startupy, je firma Chainalysis. Právě tato firma za pomoci svého softwarového vyšetřovacího nástroje Reactor, zásadní měrou přispívá k získání důkazů při vyšetřování hackerských útoků nebo praní špinavých peněz.

Propojením softwarového nástroje Reactor na databáze firem uplatňujících proces KYC, sledováním kryptopeněženek na darknet, sociálních sítích a nelegálních aktivit v kyberprostoru, pak vzniká registr dat, přiřazující elektronické informace k fyzickým subjektům. Tento kontrolní mechanismus slouží nejen k reportu OČTŘ, ale zároveň i jako okamžitá výstraha pro uživatele chystající se provést rizikovou transakci.



Jeden z výstupů z aplikace Reaktor sledující vazby na kryptopeněženku⁵³

Kryptokomunita není v názoru na aktivitu společnosti Chainalysis jednotná. Na jednu stranu každý rozumný člověk musí ocenit přínosy firmy OČTŘ, díky kterým byla odčerpána značná část nelegálně získaných prostředků či např. uzavření darknetové stránky s dětskou pornografií – Welcome to Videos. Na druhou stranu identifikace majitelů peněženek, jde přímo proti principům vzniku kryptoměn, jako anonymního a decentralizovaného platebního systému.

Autor nicméně zastává názor, že ten, kdo nic neskrývá, se nemá čeho bát a aktivity společnosti mohou přispět k pozitivnějšímu vnímání kryptoměn ze strany široké veřejnosti.

⁵³ Chainalysis. *The 2023 Crypto Crime Report*. Online. USA, Chainalysis, 2023. Dostupné z: <https://www.chainalysis.com/blog/2023-crypto-crime-report-introduction/>. [citace 2024-02-10].

13.2 Trasování virtuálních měn v ČR

Problematika kyberkriminality až do konce roku 2022 spadala pod působnost NCOZ SKPV (Národní centrála proti organizovanému zločinu služby kriminální policie a vyšetřování). Kde dni 01. 01. 2023 došlo k nové systematizaci a vzhledem k vysoké specifičnosti byla sekce terorismu, extremismu a kybernetické kriminality vyčleněna do zcela nového, samostatného útvaru NCTEKK SKPV.

Otázka trasování virtuálních měn byla OČTŘ v ČR od roku 2020 řešena pomocí zakoupení dvouleté licence k užívání softwarového nástroje Reactor, popsaného v předchozí kapitole, se zaměřením čistě na Bitcoin a dále prostřednictvím licence k vzdálenému přístupu do webové aplikace Elliptic, kterým bylo vybaveno každé krajské ředitelství.

Vzhledem k dynamickému nárustu kriminality spojené s virtuálními měnami, přímo úměrně narostl i počet požadavků pro trasování. Z toho důvodu byly ustanoveny podmínky pro možnosti využití trasování v SW Reactor:

„1) *Řízení musí být vedeno pro úmyslný trestný čin na úseku kybernetické kriminality ve smyslu písm. l, m) PPP č. 103/2013 Sb. – zejména trestné činy podle ust. § 230, 231 a 232 tr. zák.*

2) *Řízení bude vedeno pro úmyslný trestný čin, u nějž hranice škody u jednoho skutku dosahuje částky nejméně 500.000, - Kč.*

3) *V případech, kdy trasování pomocí SW Elliptic povedou ke zjištění konkrétní směnárny, která nebude na základě žádosti policejního orgánu schopna požadovanou entitu nebo atribut (BTC adresu) identifikovat nebo nebude schopna z jiného důvodu žádosti policejního orgánu vyhovět.“⁵⁴*

Protože splnění výše uvedených podmínek není každodenní záležitostí, je obsahem doporučení i využití trasování pomocí on-line veřejných bezplatných platforem, jako například www.blockchain.com či www.walletexplorer.com. Tato „lustrace“ pak může vést k dílčím informacím, které mohou být užitečné v dalším

⁵⁴ NCOZ, *Metodický technický postup s virtuálními měnami v trestním řízení*. Praha, NCOZ, 2020. Dostupné pro vnitřní využití na intranetu PČR. [citováno 2024-02-10].

postupu v prověřování, případně vyšetřování. Kromě zajištění důkazů, zejména v elektronické podobě, je v návaznosti na dokazování v trestním řízení stěžejní náležitá důkazní interpretace zajištěného obsahu. Právě pro tyto účely je u policie zřízen specializovaný aparát, ať už v rámci jednotlivých krajských ředitelství či NCTEKK.

13.2.1 KODEX.US

Vzhledem k tomu, že drtivá většina největší kryptoburz a směnáren je registrována v USA, byla pro účely ochrany zákazníka zřízena státní online platforma na adrese app.kodexglobal.com poskytující různé právní nástroje a služby, především OČTŘ v rámci tzv. Law Enforcement Request System (LERS – systému požadavků na vymáhání práva). Klíčovou službou pro OČTŘ je samotné ověření identity vyšetřujícího, který tak získá autorizaci pro oficiální komunikaci se zapojenými subjekty. Vzhledem k tématu této práce je významné partnerství především s Binance, Coinbase Int., Coinbase US, Cross River, MoonPay či OpenSea. Tuto skutečnost je z hlediska OČTŘ důležité mít na paměti, protože všeobecná podpora uvedených subjektů, nedisponuje pravomocemi např. k zmrazení prostředků na uživatelském účtu a došlo by tak pouze k časové prodlevě. Právě prostřednictvím takto ověřené komunikace a předání základních informací o zahájení trestního řízení, společně s důkazy, jako např. výpisu z blockchainu či bankovního účtu, může být dosaženo dočasného zmrazení účtu a díky následnému doručení usnesení dle § 79a tr. řádu i k delší blokaci do doby dalšího rozhodnutí ve věci. Nedílnou součástí dožádání zahraničních subjektů musí být poučení o povinnosti zachovávat mlčenlivost o všech skutečnostech souvisejících se šetřenou záležitostí podle § 115 odst. 2 zák. č. 273/2008 Sb. a § 97 odst. 8 zák. č. 127/2005 Sb. o elektronických komunikacích.

13.3 Odčerpávání

Jak bylo zmíněno dříve, dalším rozhodujícím procesním krokem po identifikaci a zmrazení prostředků, je jejich odčerpání.

K tomuto slouží institut právně zakotvený v:

„§ 79a tr. řádu

Zajištění nástrojů trestné činnosti a výnosů z trestné činnosti

(1) Nasvědčují-li zjištěné skutečnosti tomu, že určitá věc je nástrojem trestné činnosti nebo výnosem z trestné činnosti, může předseda senátu a v přípravném řízení státní zástupce nebo policejní orgán rozhodnout o zajištění takové věci.“⁵⁵

Z předmětného usnesení pak musí být mimo jiné zřejmé, že je jím vysloven zákaz s další manipulací s virtuální měnou, ve smyslu § 79a odst. 2 tr. řádu, s poučením o případném postihu, mimo pokyn k převodu prostředků na virtuální peněženku ve správě Úřadu pro zastupování státu ve věcech majetkových (ÚZSVM) za využití § 79b odst. 2 tr. řádu.

Výše uvedené usnesení lze aplikovat výhradně na případy, kdy je obsah peněženky nástrojem či výnosem z trestné činnosti, a to i v případě, že není známa totožnost pachatele, pouze adresa virtuální měny, kdy jako zákonnou oporu najdeme v ustanovení:

„§ 77b

...

(2) Podléhá-li zajištění věc, která je součástí majetku ve svěřenském fondu nebo v podílovém fondu, zajistí se svěřenskému správci nebo obhospodařovateli podílového fondu. Není-li známo, komu věc důležitá pro trestní řízení patří, zajistí se bez uvedení osoby, jíž byla zajištěna; v opatření se uvede, kdy a kde a z jakého důvodu k zajištění věci došlo.“⁵⁶

⁵⁵ Zákon č. 141/1961 Sb. Zákon o trestním řízení soudním (trestní řád) § 79a

⁵⁶ Tamtéž § 77b odst. 2

Realizace zajištění ze strany OČTŘ je na krajské úrovni z pravidla dohlížena pověřenou styčnou osobou zařazenou na OAKK (Odbor analytiky a kybernetické kriminality) na národní pak ze strany NCTEKK. Dle získaných informací bylo v roce 2021 k dispozici celkem 21 zajišťovacích adres v gesci ÚZSVM, z toho 10 pro Bitcoin, 10 pro Litecoin a 1 pro Ethereum.

Vzhledem k nehmotné a digitální povaze kryptoměn je důležité, aby při zajištění následně došlo i k převodu aktiv na adresy pod kontrolou OČTŘ, respektive státu, neboť jak bylo zmíněno v kapitole Seed, k obnově peněženky může dojít na jakémkoliv místě, což by pravděpodobně mělo za následek opětovný převod prostředků a nutnost dalšího šetření.

Případ Jamese Zhonga patří k vůbec těm světově nejúspěšnějším počínům ze strany OČTŘ, konkrétně americké IRS:CI (Internal Revenue Service, Criminal Investigation)⁵⁷, kdy se v listopadu roku 2021 podařilo v rámci trestního řízení zabavit přes 50.000 bitcoinů⁵⁸, což v dnešním kurzu činí částku přesahující 2.000.000.000 USD.

Na jednu stranu je James Zhong „hrdina“, když se mu díky svým hackerským schopnostem povedlo v roce 2012 podvodně vylákat přes 50.000 bitcoinů z nelegálního internetového tržiště Silk road, provozovaného na Darknetu. Zhong vytvořil řetězec devíti účtů Silk Road, které byly navrženy tak, aby zakryly jeho totožnost. Poté provedl více než 140 transakcí v rychlém sledu, aby oklamal systém Silk Road pro zpracování výběrů. Například 19. září 2012 vložil Zhong do účtu na Silk Road 500 Bitcoinů. Během několika sekund poté provedl pět výběrů po 500 Bitcoiních, což mu přineslo čistý zisk 2.000 Bitcoinů. Tyto transakce celkově vedly k uvolnění přibližně 50.000 Bitcoinů ze systému Silk Road na Zhongovy účty. Zhong poté převedl tyto Bitcoiny na různé oddělené adresy, které rovněž ovládal. Tímto postupem nejenom, že dokázal odčerpat velké množství nelegálních prostředků, ale po dlouhá léta dokázal skrýt i svou totožnost, vlastnictví Bitcoinů a zároveň zamlžit jejich zdroj.

Z pohledu legalizace výnosů z trestné činnosti jsou důležité i následné tzv. sekundární výnosy, vzniklé v legální oblasti ekonomiky zákonnou aktivitou, ovšem za přispění prostředků získaných z ilegálních zdrojů. K takto vytvořeným prostředkům přišel i Zhong právě díky hard forku na Bitcoinu popsanému v předchozí kapitole. Stejně množství prostředků, které měl na své bitcoinové peněžence mu bylo připsáno v kryptoměně bitcoin cash, a ačkoliv její hodnota nedosahovala hodnoty bitcoinu, získal tak následným převodem dalších 3.500 Bitcoinů. Dalším případem sekundárních výnosů, jsou legální výnosy ze Zongovi investice ve výši přibližně 9,5

⁵⁷ Americká vládní agentura pro vyšetřování trestných činů se specializací na finance, měnu či praní špinavých peněz

⁵⁸ IRS. *Historic \$3.36 billion cryptocurrency seizure and conviction in connection with Silk Road Dark Web fraud*. Online. USA, IRS 7.11.2022. Dostupné z: <https://www.irs.gov/compliance/criminal-investigation/historic-3-point-36-billion-cryptocurrency-seizure-and-conviction-in-connection-with-silk-road-dark-web-fraud>. [citováno 2024-02-11].

milionu dolarů z prostředků získaných krádeží bitcoinů na Silk Road, do podílu ve společnosti RE&D Investments, LLC, kterou založil společně se svým přítelem ze studií informačních technologií na univerzitě v Georgii. Ani tento podíl nezůstal bez povšimnutí agentů IRS.

Celkový soupis majetku zabaveného Zhongovi v rámci trestního řízení obnáší:

- 80 % podíl ve společnosti RE&D Investments, LLC, se sídlem v Memphisu, která má významné podíly v nemovitostech,
- 661.900, - USD v hotovosti zabavených v domě Jamese Zhonga dne 9. listopadu 2021;
- čtyři stříbrné pruty o hmotnosti jedné unce a tři zlaté pruty o hmotnosti jedné unce, čtyři stříbrné pruty o hmotnosti 10 uncí a jedna zlatá mince, vše zabaveno v domě dne 9. listopadu 2021;
- 11,1160005300044 bitcoinů zabavených v domě dne 9. listopadu 2021;
- 25 mincí Casascius (fyzické bitcoiny popsané dříve) v přibližné souhrnné hodnotě 174 bitcoinů, zabavených v domě dne 9. listopadu 2021;
- 23,7112850 bitcoinů vydaných Zhongem dne 27. dubna 2022;
- 115,02532155 bitcoinů vydaných Zhongem dne 28. dubna 2022; a
- 4,57427222 bitcoinů vydaných Zhongem dne 8. června 2022.

V dané věci dále státní zástupce veřejně vyzval poškozené, aby se k propadnutému majetku v počtu 51.351,89785803 bitcoinů, u kterých lze vysledovat původ s vazbami na Silk Road, v hodnotě přibližně 3.388.817.011,90 USD v době zabavení, přihlásili úřadům. Zřejmě není překvapením, že žádný tak do dnešního dne neučinil.

Díky aplikaci procesu KYC ze strany kryptoburzy a úřady sledovanému pohybu prostředků v blockchainu na vybraných kryptopeněženkách, stačila jediná chyba Zhonga, který provedl převod bitcoinů v hodnotě, pro něj zanedbatelných 800,- USD, na registrovaný burzovní účet a OČTŘ měli v rukách klíčový důkaz k případu.

Tento případ je ukázkový příklad nevhodnosti použití pseudonymních blockchainových kryptoměn pro nelegální účely. Jak bylo již zmíněno dříve, zápis v Blockchainu je trvalý, veřejný a za pomoci analytických nástrojů zpětně dohledatelný údaj o transakcích ve své kompletní historii. Spojení fyzické osoby s konkrétní kryptopeněženkou, pak odhaluje veškeré transakční vazby.

Závěr

Stručná odpověď na otázku: „Jsou kryptoměny vhodným nástrojem pro legalizaci výnosů z trestné činnosti?“ by byla: „ano.“

Delší odpověď, zahrnující širší pohled na problematiku je poskytnuta výše. Práce je zaměřena na platební prostředky a postavení kryptoměn v tomto kontextu. Představen byl princip jejich vzniku a fungování nejpopulárnější z nich Bitcoinu, a představil vlastnosti, které jsou stěžejní v případech vyšetřování trestných činů a zároveň i prostředky, které práci OČTŘ znesnadňují, a často i znemožňují. Dále byl prezentován altcoin Monero a s ním spojené nebezpečí z pohledu OČTŘ, které představují plně anonymizované kryptoměny.

Moderní informační doba s sebou přináší řadu trendů a inovací, kterých dokáží využít různé osoby s různými záměry. Základní myšlenkou kapitalismu je dosažení zisku a zbohatnutí či nahromadění majetku, které bývá hnacím motorem a smyslem života řady lidí. Tato jednoduchá myšlenka v kombinaci s nízkou finanční gramotností následně bývá terčem podvodníků a podnikatelů operujících v šedé zóně zákona. Dále jsou v práci představeny projekty a způsoby, které pod záštitou kryptoměn, blockchainu, smart contracts a dalších technologických fines, mají za cíl jen maximalizovat zisk jejich tvůrců. Takovéto investiční podvody pak vrhají stín na celé kryptoměnové odvětví, protože neinformovaný člověk si udělá klamný obraz o funkci kryptoměn.

V práci je zmíněno téma vysoké volatility kryptoměn. Stejně jako u investičních aparátů, i zde se vlastník kryptoměn vystavuje riziku nestálosti hodnoty, kdy je na zvážení, zda toto podstupovat. Ilustrativním důkazem budiž kurz bitcoinu, který v průběhu psaní práce atakoval jak hranici 25.000, - USD, tak 47.000 USD, - za kus. Právě tato volatilita by mohla být faktorem odrazující využití kryptoměn pro kriminální účely.

V práci je dále shrnuta podstata a principy praní špinavých peněz v souvislosti s kryptoměnami a operativní postupy využívané, jak pro samotné zahájení úkonů trestního řízení, tak v jeho průběhu, včetně odčerpání prostředků.

Postoj veřejnosti by se ve vztahu ke kryptoměnám dal vyjádřit dvojí způsobem. Zastánci „tradičních hodnot“ v nich vidí jen nástroj pro páchaní trestné činnosti a jejich argumentu notně přispívala i absence legislativního rámce, která vedla k nebezpečným novým trendům kriminality zvyšující společenskou škodlivost a s tím i nebezpečnost pachatelů. Na druhou stranu „zasvěcení“ v nich spatřují nejen investiční příležitost, ale i určitý pocit svobody a nekonvenční nástroj s prokazatelnými výhodami.

Díky regulaci MiCA a ToFR by mělo dojít k posílení, jak na straně státních orgánů, tak právě důvěry ve virtuální měny v očích veřejnosti, díky větší transparentnosti. Právě tento legislativní rámec a jeho úspěšné aplikování do právního systému, dává naději orgánům činným v trestním řízení k úspěšnějšímu odhalování trestné činnosti. Ať už tím, že omezí anonymní kryptoměny, či zavede nové povinnosti osobám nakládajícím s kryptoměnami. Tímto by byla vypořádána pozitiva.

Na druhou stranu je spatřována jako forma legislativní překážky, nová podoba trestního řádu, kdy se jej prozatím nepodařilo vůbec vydat ani zásadně novelizovat, ačkoliv je ze strany OČTŘ dlouhodobě zmiňována potřeba zjednodušení, a tím i zrychlení trestního řízení do té míry, aby bylo schopné adekvátně reflektovat potřeby současného moderního světa. Ať už by šlo o použití operativně pátracích prostředků, které s využitím moderních technologií ztrácí na účinnosti či např. rozsah advokátního tajemství, které je jako institut zneužíváno pachateli trestné činnosti.

V souvislosti s legalizací výnosů z trestné činnosti je vnímáno jako obrovská chyba zrušení Elektronické evidence tržeb (EET), která opět vytvořila prostor pro mimobilanční příjmy a jejich integraci zpět do oběhu.

Do budoucna se dá předpokládat větší přesun kriminality směrem do virtuálního prostředí, a proto bude nutná i adekvátní reakce OČTŘ ve smyslu rozšíření materiálního a personální zázemí v dané oblasti, či důraz na pravidelné proškolení pracovníků a seznamování s novými trendy na tomto poli, jak z pohledu veřejnosti, tak z pohledu trestněprávního procesu.

Vyčlenění NCTEKK z NCOZ a vznik a rozšiřující se oddělení OAKK v rámci krajských ředitelství policie, je jasným signálem rozvoje koncepce policie reagující na současné potřeby. Nicméně poskytování správné a včasné analytické podpory jde

ruku v ruce s kvalitní prací při tzv. nabírání skutku na základních útvarech. Vzhledem k tomu, že na těchto místech dochází ke značné generační obměně příslušníků PČR, je zde velký prostor ke zlepšení práce právě na této „nejnižší“ úrovni. Sledování kriminalistických trendů ze strany NCTEKK či OAKK je dozajista samozřejmostí. Pružné a včasné předávání informací v rámci školení či vzniku metodického postupu již samozřejmostí nejsou. Následné seznámení s problematikou pomocí podpisové knihy ETŘ nebo dokumentu v eSiař nelze nepovažovat za plnohodnotnou a smysluplnou podporu výkonu služby. Částečně tuto podporu splňuje model vzdělávání v rámci epolis, který ovšem v současné době disponuje omezeným množstvím vzdělávacích kurzů. Nicméně pokud je dáno dikcí Zákona o služebním poměru příslušníků bezpečnostních sborů, prohlubovat svoji odbornost, a i vedoucí pracovník je povinen zabezpečovat, aby příslušníci byli pro výkon služby náležitě vyškoleni, je důležité, aby tuto činnost vedoucí orgány prioritizovaly.

Samostatnou kapitolu v práci OČTŘ pak tvoří spolupráce s okolními orgány, jako je např. v práci zmíněný FAÚ či banky. Usnadnění této spolupráce by dozajista přineslo propojení a digitalizace systémů státní správy a samosprávy, o které se v ČR dlouhé roky mluví a dochází ke zcela pozvolnému náběhu. Právě i v této oblasti by našlo uplatnění využití technologie Blockchain. Ve vztahu např. k bankám by byla třeba pohotovostní služba fungující 24/7/365, která bude mít na starosti okamžité zajišťování prostředků v zájmu OČTŘ, protože jakkoliv je doručování datovou zprávou komfortní, tak se zdaleka nejedná o akční aparát.

Závěrem by chtěl autor vyjádřit svůj apel ohledně kryptoměn a legalizace výnosů z trestné činnosti vůči veřejnosti, protože stejně jako v jiných oblastech, pouze osvěta a vzdělání se v této oblasti, může přinést pochopení problematiky, její správné používání, rozpoznávání a včasné nahlašování nelegálních aktivit.

Použitá literatura

- BORČEVSKÝ, Pavel. *Trestní právo hmotné: zvláštní část*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2023. ISBN 978-80-7380-909-6.
- 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.
- DVOŘÁK, Vratislav. *Výnosy z trestné činnosti*. Praha: Pro potřeby nakl. Ivan Fojt vydala Scientia, 2010. ISBN 978-80-86960-67-8.
- GRIVNA, Tomáš; RICHTER, Martin a ŠIMÁNOVÁ, Hana (ed.). *Vliv nových technologií na trestní právo*. Praha: Auditorium, 2022. ISBN 978-80-87284-95-7.
- 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.
- KOLOUCH, Jan a Petr VOLEVECKÝ. *Trestněprávní ochrana před kybernetickou kriminalitou*. Praha: Policejní akademie České republiky v Praze, 2013. ISBN 978-80-7251-402-1.
- POLČÁK, Radim; PÚRY, František a HARAŠTA, Jakub. *Elektronické důkazy v trestním řízení*. Brno: Masarykova univerzita, 2015. ISBN 978-80-210-8073-7.
- REVENDA, Zbyněk; MANDEL, Martin; KODERA, Jan; MUSÍLEK, Petr a DVOŘÁK, Petr. *Peněžní ekonomie a bankovníctví*. Sedmé přepracované vydání. Jesenice: Ekopress, 2023. ISBN 978-80-87865-84-2.
- 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.

- 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.
- ŠÁMAL, Pavel. *Trestní řád: komentář*. 7., dopl. a přeprac. vyd. V Praze: C.H. Beck, 2013. Velké komentáře. ISBN 978-80-7400-465-0.
- Trestněprávní revue. 2001-. Praha: C.H. Beck, 2001-. ISSN 12135313.

Zákonná úprava a prováděcí předpisy

Informace k daňovému posouzení transakcí s kryptoměnami. Finanční správa. Online. 2022 [cit. 2024-02-09]. Dostupné z: https://www.financnisprava.cz/assets/cs/prilohy/d-seznam-dani/Info_kryptomeny_GFR.pdf

Ministerstvo vnitra: Stanovisko obp k aplikaci ustanovení § 7b trestního řádu. [online]. Praha, Ministerstvo vnitra ČR, 2019 [cit. 2024-02-10]. Dostupné z: <https://www.mvcr.cz/clanek/poskytnuti-informace-metodika-tykajici-se-aplikace-7b-trestniho-radu.aspx>

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2023/1113 ze dne 31. května 2023 o informacích doprovázejících převody peněžních prostředků a některých kryptoaktiv a o změně směrnice (EU) 2015/849

Nařízení evropského parlamentu a rady (EU) 2023/1114 ze dne 31. května 2023 o trzích kryptoaktiv a o změně nařízení (EU) č. 1093/2010 a (EU) č. 1095/2010 a směrnic (EU) 2013/36

Sdělení č. 104/2013 Sb. m. s. Sdělení Ministerstva zahraničních věcí o sjednání Úmluvy o počítačové kriminalitě. 23.12.2013. In Sbírka zákonů. Vč. novelizací, dostupné také na <https://www.zakonyprolidi.cz/ms/2013-104/zneni-20190705>

Směrnice Evropského parlamentu a Rady (EU) 2014/65 ze dne 15. května 2014 o trzích finančních nástrojů a o změně směrnic 2002/92/ES a 2011/61/EU.

Ústavní zákon č. 2/1993 Sb. ve znění ústavního zákona č. 162/1998 Sb. a ústavního zákona č. 295/2021 Sb. – Listina základních lidských práv a svobod. 16.12.1992. In.

Sbírka zákonů. Vč. novelizací, dostupné také na <https://www.psp.cz/docs/laws/listina.html>

Zákon č. 253/2008 Sb.: o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu. 8.7.2008. In: Sbírka zákonů. Vč. novelizací, dostupné také na <https://www.zakonyprolidi.cz/cs/2008-253/zneni-20240120>

Zákon č. 370/2017 Sb.: o platebním styku. 13.11.2017. In: Sbírka zákonů. Vč. Novelizací, dostupné také na <https://www.zakonyprolidi.cz/cs/2017-370/zneni-20220701>

Neveřejné zdroje

Ministerstvo vnitra: VYHODNOCENÍ SITUACE V OBLASTI ORGANIZOVANÉHO ZLOČINU NA ÚZEMÍ ČR ZA OBDOBÍ 2016–2023. Praha: Ministerstvo vnitra ČR, 2023. Dostupné pouze pro vnitřní potřeby PČR.

NCOZ: Metodický technický postup s virtuálními měnami v trestním řízení. Praha, NCOZ, 2020. Dostupné pro vnitřní využití na intranetu PČR.

Internetové zdroje

Co jsou peníze? *Ecb.europa.eu*. Online. 2017, 20. 6. 2017. Dostupné z: https://www.ecb.europa.eu/ecb/educational/explainers/tell-me-more/html/what_is_money.cs.html. [citováno 2024-02-09].

Co bude s Bitcoinem po vytěžení poslední mince? *Kurzy.cz*. Online. 13.02.2023. Dostupné z: <https://www.kurzy.cz/zpravy/697673-co-bude-s-bitcoinem-po-vytezeni-posledni-mince/>. [citováno 2024-02-09].

HAMPL, Mojmír. Náš postoj ke kryptoměnám? Nepomáhat, nechránit, neškodit, nevodit za Ruku. *Cnb.cz*. Online. 2017, 21. 12. 2017. 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/>. [citováno 2024-02-09].

STROUKAL, Dominik. Poslední banka ruší účty kryptofirmám. Přitom k tomu není žádný důvod. *E15.cz*. Online. 4.4.2023. Dostupné z: <https://www.e15.cz/nazory-a-analyzy/posledni-banka-rusi-ucty-kryptofirmam-pritom-k-tomu-neni-zadny-duvod-1397521>. [citováno 2024-02-09].

Ceny nemovitostí v USA raketově rostou. *Finlord*. Online. 2021, 1.4.2021. Dostupné z: <https://finlord.cz/2021/04/ceny-nemovitosti-usa-raketove-rostou/>. [citováno 2024-02-09].

Globální grafy tržní kapitalizace kryptoměn. *Coingecko*. Online. 2024. Dostupné z: <https://www.coingecko.com/cs/global-charts>. [citováno 2024-02-09].

Co je u kryptoměny fork, jaký je rozdíl mezi hard forkem a soft forkem a končí to vždy rozvětvením sítě? *Kryptohodler.cz*. Online. 2021, 5.2.2021. Dostupné z: [https://kryptohodler.cz/hodl-co-je-fork-jaky-je-rozdil-mezi-hard-forkem-a-soft-forkem-tvrdou-a-mekkou-vidlici/#Hard fork vs soft fork](https://kryptohodler.cz/hodl-co-je-fork-jaky-je-rozdil-mezi-hard-forkem-a-soft-forkem-tvrdou-a-mekkou-vidlici/#Hard%20fork%20vs%20soft%20fork). [citováno 2024-02-09].

Casascius Bitcoin Peels: \$10M Cashed in 2023, Yet a \$1 Billion Stash Remains Unclaimed. *News.bitcoin.com*. Online. 2023, 4.9.2023. Dostupné z: <https://cryptonews.net/news/bitcoin/22716023/>. [citováno 2024-02-10].

Co jsou ETF. *Patria.cz*. Online. 2024. Dostupné z: <https://www.patria.cz/fondyderivaty/etf/popis.html>. [citováno 2024-02-10].

GALLISTL, Vladan. Bitcoinová ETF zažila rekordní debut na burze. Za stovky milionů korun nakupovali i Češi. *Hn.cz*. Online. 2024, 15.1.2024. Dostupné z: <https://archiv.hn.cz/c1-67284460-bitcoinova-etf-zazila-rekordni-debut-na-burze-za-stovky-milionu-korun-nakupovali-i-cesi>. [citováno 2024-02-10].

Monero. *Coingecko.com*. Online. 2024. Dostupné z: <https://www.coingecko.com/cs/coins/monero>. [citováno 2024-02-09].

VAN SABERHAGEN, Nicolas. CryptoNote v 2.0. *getmonero.org*. Online. 2013, 17.10.2013. Dostupné z: <https://www.getmonero.org/resources/research-lab/pubs/cryptonote-whitepaper.pdf>. [citováno 2024-02-10].

ICO (VŠE, CO CHCETE VĚDĚT). Co je prvotní nabídka kryptoměny? *alza.cz*. Online. 2019, 1.1.2019. Dostupné z: <https://www.alza.cz/ico-initial-coin-offerings>. [citováno 2024-02-10].

Venture capital. *Czechwealth.cz*. Online. 2024. Dostupné z: <https://www.czechwealth.cz/slovník-pojmu/venture-capital>. [citováno 2024-02-10].

BitConnect Founder Indicted in Global \$2.4 Billion Cryptocurrency Scheme. *Justice.gov*. Online. 2022, 25.02.2022. Dostupné z: <https://www.justice.gov/opa/pr/bitconnect-founder-indicted-global-24-billion-cryptocurrency-scheme>. [citováno 2024-02-10].

IPO průvodce: Co je IPO a jaké IPO se blíží? *Lynxbroker.cz*. Online. 2024. Dostupné z: <https://www.lynxbroker.cz/investovani/burzovni-trhy/akcie/ipo/>. [citováno 2024-02-10].

WOLF, Karel. Riziko s rozumem, nebo scam? Kolem XIXOIO víří otázky i podezření. *Forbes.cz*. Online. 2021, 24.11.2021. Dostupné z: <https://forbes.cz/riziko-s-rozumem-nebo-scam-xixoio-podezreni/>. [citováno 2024-02-10].

KUČERA, Petr. Kauza Xixoio: Policie obvinila dva lidi kvůli podvodu. *Penize.cz*. Online. 2023, 4.12.2023. Dostupné z: <https://www.penize.cz/investice/449188-kauza-xixoio-policie-obvinila-dva-lidi-kvuli-podvodu>. [citováno 2024-02-10].

OKAFOR, Amina. A16z Review. *Coinweb.com*. Online. 2024. Dostupné z: <https://coinweb.com/comparison/best-crypto-vc-firms/a16z/>. [citováno 2024-02-10].

KONRAD, Alex. A16z Crypto's Record New \$4.5 Billion Fund Doubles Down On Web3 Amid Market Crash. *Forbes.com*. Online. 2022, 25.5.2022. Dostupné z: <https://www.forbes.com/sites/alexkonrad/2022/05/25/a16z-crypto-record-4th-fund-doubles-down-on-web3-amid-market-crash/>. [citováno 2024-02-10].

SHARMA, Niketam. Top 6 Most Expensive NFT Monkey (Bored Ape) Sold Ever – NFT. *Nimbleappgenie.com*. Online. 2023, 17.1.2023. Dostupné z: <https://www.nimbleappgenie.com/blogs/top-6-most-expensive-nft-monkey-bored-ape-sold-ever/>. [citováno 2024-02-10].

Čína zavádí sociální kreditní systém. Co to znamená? *CzechTrade*. Online. 2020, 2.9.2020. Dostupné z: <https://www.businessinfo.cz/clanky/cina-zavadi-socialni-kreditni-system-co-to-znamená/>. [citováno 2024-02-10].

Limity a verifikace. *Simplecoin.eu*. Online. 2024. Dostupné z: <https://www.simplecoin.eu/cs/limits-and-verification>. [citováno 2024-02-10].

Co jsou decentralizované burzy (DEX)? *Kryptomagazin.cz*. Online. 2023, 13.6.2023. Dostupné z: <https://kryptomagazin.cz/co-jsou-decentralizovane-burzy-dex/>. [citováno 2024-02-10].

NAKAMOTO, Satoshi. Bitcoin: Peer-to-Peer Systém elektronických peněz. *bitcoin.org*. Online. 2009. Dostupné z: https://bitcoin.org/files/bitcoin-paper/bitcoin_cz.pdf. [citováno 2024-02-10].

BEDNAR, Juraj. Etický vekslák. *Juraj.bednar.io*. Online. 2020, 14.4.2020. Dostupné z: <https://juraj.bednar.io/courses/eticky-vekslak/>. [citováno 2024-02-09].

OECD MONEY-LAUNDERING LEADER BOARD. *Credas.com*. Online. 2022, 25.5.2022. Dostupné z: <https://credas.com/news/oecd-money-laundering-leader-board/>. [citováno 2024-02-10].

'As a service' business models: What it is and its benefits. *Consultancy.eu*. Online. 2022, 3.5.2022. Dostupné z: <https://www.consultancy.eu/news/7350/as-a-service-business-models-what-it-is-and-its-benefits>. [citováno 2024-02-10]

Statistické přehledy kriminality za rok 2022. Policie ČR Online. 2023. Dostupné z: <https://www.policie.cz/clanek/statisticke-prehledy-kriminality-za-rok-2022.aspx>. [citováno 2024-02-10].

ZELENÝ, Petr. Kvůli kyberútoku nefungovaly několik hodin některé služby ČSOB. ČTK. Online. 2023, 3.3.2023. Dostupné z: <https://ct24.ceskatelevize.cz/domaci/3569084-kvuli-kyberutoku-nefunguji-nektere-sluzby-csob-neni-jasne-jak-dlouhy-vypadek-bude>. [citováno 2024-02-10]

PRCHAL, Lukáš. Od igelitek ke kryptoměnám: pachatelé praní špinavých peněz přicházejí na stále nové metody. *Ekonom.cz*. Online 2018, 9.4.2018. Dostupné z: <https://pravmiradce.ekonom.cz/c1-66103630-od-igelitek-ke-kryptomenam>. [citováno 2024-02-10]

PAVELKA, Jindřich. Heslo. *Hazardni-hry.eu*. Online. 2024. Dostupné z: <https://www.hazardni-hry.eu/pravdepodobnost/heslo.html#gsc.tab=0>. [citováno 2024-02-10]

Chainalysis. The 2023 Crypto Crime Report. Online. USA, Chainalysis, 2023. Dostupné z: <https://www.chainalysis.com/blog/2023-crypto-crime-report-introduction/>. [citováno 2024-02-10].

IRS. Historic \$3.36 billion cryptocurrency seizure and conviction in connection with Silk Road Dark Web fraud. Online. IRS, 2022, 7.11.2022. Dostupné z: <https://www.irs.gov/compliance/criminal-investigation/historic-3-point-36-billion-cryptocurrency-seizure-and-conviction-in-connection-with-silk-road-dark-web-fraud>. [citováno 2024-02-11].