

**VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH
STUDIÍ, Z. Ú., ČESKÉ BUDĚJOVICE**

BAKALÁŘSKÁ PRÁCE

**KRYPTOMĚNY JAKO POTENCIONÁLNÍ
NÁSTROJ LEGALIZACE VÝNOSŮ Z TRESTNÉ
ČINNOSTI**

Autor práce: Ondřej Pisečný, DiS.

Studijní program: Bezpečnostně právní činnost

Forma studia: Kombinovaná

Vedoucí práce: RNDr. Růžena Ferebauerová

Katedra: Katedra právních oborů a bezpečnostních studií

2025

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, z. ú.
Žižkova tř. 1632/5b, 370 01 České Budějovice

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jméno a příjmení studenta: Ondřej Pisečný, DiS.

Studijní program: Bezpečnostně právní činnost

Forma studia: Kombinovaná

Místo studia: Příbram

Název bakalářské práce: Kryptoměny jako potenciální nástroj legalizace výnosů z trestné činnosti

Název bakalářské práce v anglickém jazyce: Cryptocurrency as a Potential Instrument of Money Laundering

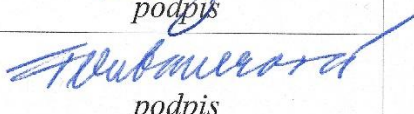
Katedra: Katedra právních oborů a bezpečnostních studií

Vedoucí bakalářské práce (jméno a příjmení, včetně titulů):

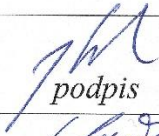
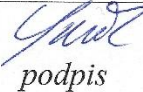
RNDr. Růžena Ferebauerová

Datum zadání bakalářské práce (měsíc, rok): listopad 2024

Cíl bakalářské práce: Hlavním cílem bakalářské práce je zhodnotit potenciál kryptoměn jako nástroje pro legalizaci výnosů z trestné činnosti a identifikovat konkrétní způsoby, jakými mohou být kryptoměny zneužívány k praní špinavých peněz. Vedlejším cílem práce je navrhnout doporučení pro zlepšení právního rámce a efektivnější odhalování a prevenci takových činností.

Student: Ondřej Pisečný, DiS.	18. 11. 2024 datum	 podpis
Vedoucí práce: RNDr. Růžena Ferebauerová	20. 11. 2024 datum	 podpis

Schvaluji zadání bakalářské práce:

Vedoucí katedry: doc. JUDr. Roman Svatoš, Ph.D.	2. 12. 2024 datum	 podpis
Prorektor pro studium a vnitřní záležitosti: doc. PhDr. Miroslav Sapík, Ph.D.	9. 12. 2024 datum	 podpis
Rektor: doc. Ing. Jiří Dušek, Ph.D.	10. 12. 2024 datum	 podpis



Prohlašuji, že jsem bakalářskou práci vypracoval(a) samostatně, na základě vlastních zjištění a s použitím odborné literatury a materiálů uvedených v seznamu použitých zdrojů.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce v elektronické podobě ve veřejně přístupné části infodisku VŠERS, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky vedoucí(ho) a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce systémem na odhalování plagiátů.

.....

Děkuji vedoucí(mu) bakalářské práce RNDr. Růženě Ferebauerové za cenné rady,
připomínky a metodické vedení práce.

ABSTRAKT

PISEČNÝ, O. *Kryptoměny jako potenciální nástroj trestné činnosti: bakalářská práce*. České Budějovice: Vysoká škola evropských a regionálních studií, 2025. 66 s.
Vedoucí bakalářské práce: RNDr. Růžena Ferebauerová.

Klíčová slova: Kryptoměna, anonymita, kybernetická kriminalita

Tato bakalářská práce se zabývá analýzou kryptoměn jako potenciálního nástroje legalizace výnosů z trestné činnosti. Hlavním cílem je identifikovat klíčové charakteristiky kryptoměn (zejména anonymity a decentralizaci), které mohou usnadňovat praní špinavých peněz, a zhodnotit, do jaké míry představují riziko pro finanční sektor a orgány činné v trestním řízení. Metodologicky se práce opírá o studium odborné literatury, analýzu stávající legislativy, mezinárodních norem a vybraných případových studií, jakož i konzultace s experty z oblasti práva a kybernetické bezpečnosti.

ABSTRACT

PISEČNÝ, O. *Cryptocurrency as a Potential Instrument of Money Laundering: Bachelor Thesis*. České Budějovice: The College of European and Regional Studies, 2025. 66 pgs. Supervisor: RNDr. Růžena Ferebauerová.

Key words: Cryptocurrency, anonymity, cybercrime

This bachelor thesis deals with the analysis of cryptocurrencies as a potential tool for laundering the proceeds of crime. The main objective is to identify the key characteristics of cryptocurrencies (in particular anonymity and decentralization) that may facilitate money laundering and to assess the extent to which they pose a risk to the financial sector and law enforcement authorities. Methodologically, the work is based on a study of the literature, analysis of existing legislation, international standards and selected case studies, as well as consultations with legal and cyber security experts.

Obsah

Úvod.....	9
1 Cíl a metodika bakalářské práce	11
2 Výnos z trestné činnosti a jeho znaky	12
3 Legalizace výnosu z trestné činnosti.....	15
4 Kryptoměny	22
4.1.1 Bitcoin.....	24
4.1.2 Vývoj hodnoty Bitcoinu	26
4.1.3 Ethereum	29
5 Vývoj kyberkriminality za užití kryptoměn.....	32
5.1.1 Konverze výnosů z trestné činnosti do kryptoměn	32
5.1.2 Obchodní operace zahrnující kryptoměny v kontextu opatření zaměřených na prevenci legalizace výnosů z trestné činnosti.....	34
6 Případy zneužití kryptoměny zaznamenané v minulosti	41
6.1.1 Silk Road.....	41
6.1.2 Liberty Reserve	45
6.1.3 Coin.mx.....	46
7 Právní regulace kryptoměn	47
7.1.1 Právní regulace kryptoměn ve světě	47
7.1.2 Regulace kryptoměn v USA	47
7.1.3 Právní regulace v Evropské unii	48
7.1.4 Právní regulace v Asii	48
7.1.5 Právní regulace kryptoměn v České republice.....	48
7.1.6 Právní status kryptoměn v ČR.....	49
7.1.7 Regulace v oblasti AML/KYC.....	49
7.1.8 Dopad evropské regulace (MiCA) na ČR	50
7.1.9 Výzvy a budoucí vývoj	50
8 Budoucí vývoj	51

8.1.1	Doporučení pro efektivnější prevenci praní špinavých peněz prostřednictvím kryptoměn	51
8.1.2	Zpřísnění a harmonizace mezinárodní regulace.....	51
8.1.3	Posílení dohledu a AML opatření	52
8.1.4	Rozvoj technologických nástrojů pro monitorování a analýzu.....	52
8.1.5	Zvýšení odpovědnosti a spolupráce soukromého sektoru.....	53
8.1.6	Vzdělávání a osvěta pro orgány činné v trestním řízení	53
Závěr		55
Seznam použitých zdrojů		58
Obrázky		66

Úvod

V polovině 20. století začaly vznikat první počítačové sítě, které postupně vedly k vytvoření moderního internetu. S rozvojem digitální komunikace se objevily i první pokusy o vytvoření elektronických platebních systémů, jež měly umožnit uživatelům provádět finanční transakce nezávisle na geografické poloze a státní příslušnosti. Tyto systémy prošly v průběhu času významným technologickým vývojem, v jehož rámci se vyprofilovaly dvě hlavní formy elektronických peněz – centralizované a decentralizované.

Kryptoměny představují specifickou kategorii decentralizovaných digitálních měn, které fungují bez nutnosti existence třetí strany, jež by spravovala a garantovala jednotlivé transakce. Absence centrální autority zároveň eliminuje možnost zásahu do měnové politiky, falšování měny či zablokování probíhajících plateb. Od vzniku bitcoinu v roce 2008 se objevilo značné množství dalších kryptoměn – webová platforma CoinMarketCap¹ v současnosti eviduje přes 11 miliónů aktivních projektů. Nicméně terminologická klasifikace těchto měn není jednoznačně ustálená, což vede k diskusím ohledně jejich přesného zařazení do kategorií kryptoměn, virtuálních měn či digitálních měn.

Obecně lze definovat digitální měnu jako prostředek směny, který sdílí řadu vlastností s fyzickými penězi (bankovkami a mincemi), avšak jeho hlavní výhodou je možnost okamžitého přenosu mezi uživateli prostřednictvím digitálního prostředí. Virtuální měny i kryptoměny spadají pod širší kategorii digitálních měn, avšak jejich využití se může lišit. Virtuální měny jsou obvykle navázány na specifická online prostředí, například herní ekosystémy, a primárně nejsou určeny k reálnému ekonomickému využití. Naproti tomu digitální měny jsou běžně používány pro transakce v reálném světě jako alternativa ke klasickým měnám. Kryptoměny se odlišují tím, že využívají kryptografické metody, decentralizovanou síťovou strukturu a systém blokových převodů k zajištění bezpečnosti a transparentnosti transakcí.² Tato práce se primárně zaměřuje na kryptoměny, přičemž hlavní důraz je kladen na bitcoin jako dosud

¹ All Currencies | Crypto-Currency Market Capitalizations [online]. [cit. 2025-02-02]. Dostupné z: <https://coinmarketcap.com/all/views/all/>

² WAGNER, A. *Digital vs. Virtual Currencies*. In: *Bitcoin Magazine* | Bitcoin and Cryptocurrency News [online]. [cit. 2025-02-02]. Dostupné z: <https://bitcoinmagazine.com/articles/digital-vs-virtual-currencies-1408735507>

nejrozšířenější a nejpoužívanější kryptoměnu. Důvodem tohoto zaměření je skutečnost, že většina dostupných nástrojů zaměřených na anonymizaci transakcí je vyvíjena právě pro bitcoin. Kromě toho se doposud zveřejněné případy legalizace výnosů z trestné činnosti prostřednictvím kryptoměn v naprosté většině týkají právě bitcoinu.

Tato bakalářská práce si klade za cíl analyzovat, zda jsou kryptoměny využitelné pro legalizaci výnosů z trestné činnosti, a pokud ano, jaké konkrétní metody pachatelé k tomuto účelu využívají. Současně se práce zaměřuje na identifikaci výhod a nevýhod, které kryptoměny přinášejí osobám zapojeným do nezákonných finančních operací, a zkoumá, zda existují účinné způsoby prevence takových praktik.

V úvodních dvou kapitolách je pozornost věnována obecnému vymezení pojmu výnos z trestné činnosti a jeho legalizaci, přičemž se práce opírá o právní rámec a teoretická východiska této problematiky. Třetí kapitola se soustředí na analýzu fungování kryptoměn, přičemž jako modelový příklad slouží bitcoin, nejrozšířenější digitální měna. Čtvrtá část se zaměřuje na metody legalizace prostřednictvím kryptoměn a způsoby, jimiž pachatelé usilují o zachování anonymity na internetu. Následující kapitola přináší konkrétní případy využití kryptoměn pro legalizaci výnosů z trestné činnosti. Vzhledem k absenci zveřejněných případů v České republice se analýza opírá výhradně o příklady ze zahraniční praxe. Závěrečná kapitola se věnuje přístupu českého právního řádu ke kryptoměnám a obsahuje návrhy možných opatření, která by mohla přispět k efektivnější regulaci této problematiky.

Vzhledem k tomu, že kryptoměny představují poměrně nový fenomén, dosud neexistuje dostatek odborné literatury, zejména v českém jazyce. Proto se tato práce do značné míry opírá o internetové zdroje, přičemž je nutné reflektovat skutečnost, že ne všechny dostupné informace lze považovat za ověřené a spolehlivé. Mezi klíčové prameny patří i zdroje z tzv. „dark webu“, což je část internetu, která není indexována běžnými vyhledávači a k jejímuž prohlížení je zapotřebí specializovaný software, například Tor. S pojmem dark web souvisí termín „clear net“, označující nezašifrované webové stránky, které jsou běžně dostupné a kde je identita uživatele zpravidla sledována prostřednictvím IP adresy.

1 Cíl a metodika bakalářské práce

Hlavním cílem bakalářské práce je zhodnotit potenciál kryptoměn jako nástroje pro legalizaci výnosů z trestné činnosti a identifikovat konkrétní způsoby, jakými mohou být kryptoměny zneužívány k praní špinavých peněz. Vedlejším cílem práce je navrhnout doporučení pro zlepšení právního rámce a efektivnější odhalování a prevenci takových činností.

Pro dosažení stanoveného cíle bude v první části zpracována odborná literatura, která poskytne teoretická východiska k problematice kryptoměn, praní špinavých peněz a jejich právní regulace. Následně bude provedena analýza relevantních legislativních rámců (národní i mezinárodní předpisy) a doporučení mezinárodních organizací (např. Financial Action Task Force – FATF). Dílčí část bude věnována případovým studiím a odborným článkům, které přiblíží aktuální trendy a praktiky v oblasti zneužívání kryptoměn. Součástí metodického postupu je i komparativní analýza dostupných nástrojů a mechanismů k odhalování, prevenci a potírání této formy trestné činnosti. V závěru budou syntetizovány získané poznatky a navržena doporučení pro legislativní úpravy i praxi v tuzemském prostředí.

2 Výnos z trestné činnosti a jeho znaky

Výnos představuje pojem s rozsáhlým významem, který se v odborné literatuře i ve specializovaných člancích vyskytuje v rozmanitých podobách. Za účelem snadnějšího porozumění je často doprovázen různými přívlastky (například legální výnos, nezákonný výnos nebo výnos z trestné činnosti). Jde o fenomén, který může vzniknout, po určitou dobu přetrvávat a následně zaniknout. Během svého „životního cyklu“ může výnos nabývat různých forem, mimo jiné i kryptoměn. Pachatelé se přitom snaží zamezit kontrolním orgánům v odhalení nezákonného původu, a proto výnosu vytvářejí fiktivní identitu. Výnos z trestné činnosti tak v průběhu transformace prochází několika stadii: od příjmu z neznámých zdrojů, přes proces legalizace, až k tzv. sekundárnímu výnosu.³

Do roku 2008 byl pojem výnosu z trestné činnosti vymezen zákonem č. 61/1996 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a o změně a doplnění souvisejících zákonů. Tento právní předpis jej charakterizoval jako veškerou ekonomickou výhodu získanou jednáním, které splňuje znaky trestného činu.⁴ Pojem „ekonomická výhoda“ představuje velmi širokou kategorii, která zahrnuje pestrou paletu možných forem obohacení. Patří sem i příjmy získané prostřednictvím krácení daňové povinnosti či zneužívání různých daňových výhod, například podvodným vylákáním nadměrného odpočtu daně z přidané hodnoty.⁵ Původní právní úpravu nahradil zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, jenž již daný termín nespecifikuje. Z definice legalizace výnosů z trestné činnosti však lze dovodit, že za výnos se pokládá „jakákoliv ekonomická výhoda vyplývající z trestné činnosti s cílem vzbudit zdání, že jde o majetkový prospěch nabytý v souladu se zákonem“.⁶ Z hlediska mezinárodního práva se lze opřít o definici uvedenou v Konvenci OSN proti mezinárodnímu organizovanému zločinu, podle níž pojem „výnos z trestné činnosti“ označuje jakýkoli majetek, jenž byl, ať už přímo či nepřímo, získán nebo nabyt v souvislosti s páčáním trestného činu.⁷ V platné trestněprávní úpravě sice

³ DVOŘÁK, V., ŠUGÁR J., MÁLEK P. a HORÁČEK P. *Výnosy z trestné činnosti*. Vyd. 1. Praha: Pro potřeby nakl. Ivan Fojt vydala Scientia, 2010. ISBN 978-80-86960-67-8, str. 46-47.

⁴ Zákon č. 61/1996 Sb. o některých opatřeních proti legalizaci výnosů z trestné činnosti a o změně a doplnění souvisejících zákonů. In: Sbírka zákonů. 20. 3. 1996.

⁵ TVRDÝ, J. *Zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a předpisy související: komentář*. 1. vyd. Praha: C.H. Beck, 2004. ISBN 80-7179-899-1. s. 48

⁶ Zákon č. 253/2008 Sb. o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu. In: Sbírka zákonů. 8. 7. 2008. ISSN 1211-1244.

⁷ SCHEINOST, M. *Konvence OSN a další dokumenty k organizovanému zločinu*. Prameny. Praha: Institut pro kriminologii a sociální prevenci, 2001. 265 s. ISBN 80-86008-91-6., s. 7.

chybí jednoznačná definice pojmu, avšak ustálený výklad vychází z toho, že za výnos v českém trestním právu se nepovažují pouze věci či jiné majetkové hodnoty získané přímo trestnou činností, nýbrž rovněž takové, které byly zcela nebo zčásti nabyté výměnou za zmíněné věci či majetkové hodnoty, případně za jejich ekvivalent tvořící odměnu za trestný čin. Na základě těchto předpisů lze následně zajistit majetek nacházející se nejen ve vlastnictví samotného obviněného, ale i dalších osob.⁸ Zásadní význam spočívá v tom, že pojem výnosu z trestné činnosti nezahrnuje pouze majetek přímo získaný spácháním trestného činu, nýbrž i veškeré hodnoty nabyté výměnou za takto získané věci či majetkové prostředky, anebo za věci a jiné majetkové hodnoty představující odměnu za trestný čin.

Výnosy z trestné činnosti lze vnímat jako dynamický jev, jenž postupně nabývá různých forem. Pokud jde o výnos z neznámých zdrojů, jeho původ, tedy konkrétní zdrojová aktivita či transakce, zůstává utajen. Charakteristickým rysem bývá značný objem výnosu, u něhož nelze doložit jeho původní historii, přičemž deklarované legální příjmy a ekonomická situace dané osoby neodpovídají skutečné výši výnosu. Zásadní rovněž je, že mezi pachatelem a trestnou činností, z níž výnos pramení, nelze prokázat přímou souvislost. V momentě, kdy pachatel zcela zamaskuje zdroj a vytvoří pro výnos fiktivní identitu, hovoříme již o zlegalizovaném výnosu z trestné činnosti. Ten následně vzbuzuje zdání, že byl získán v souladu se zákonem. Takto „očistěné“ prostředky bývají investovány buď do legální ekonomiky s cílem jejich dalšího zhodnocení, nebo jsou užívány k osobní spotřebě – například k nákupu nelegálního zboží, nemovitostí či jiných aktiv. Sekundární výnos pak představuje kapitalizovaný primární výnos, jehož zdroj sice spočívá v nezákonné aktivitě, avšak k jeho navýšení dochází prostřednictvím ekonomických procesů již v rámci legálního hospodářství.⁹

Legalizace výnosů z trestné činnosti představuje promyšlený a cíleně vedený proces, jehož cílem je zastřít nezákonný původ majetku. Skládá se z několika na sebe navazujících kroků, přičemž konkrétní metoda se vybírá podle formy, v níž se protiprávně získané prostředky nacházejí – jiný postup je nutný v případě peněz, jiný u nemovitostí či práv duševního vlastnictví. K základním přístupům patří zejména mísení nelegálních

⁸ Analýza možností odčerpávat majetek pocházející z nelegitimních zdrojů mimotrestními prostředky. In: Hospodářská komora České republiky [online]. [cit. 2025-02-02]. Dostupné z: www.komora.cz/download.aspx?dontparse=true&FileID=634, s. 13.

⁹ DVORÁK, V. a ZÁMEK D. *Výnos z trestné činnosti a jeho modifikace*. In: Bezpečnostní sbory [online]. [cit. 2025-02-02]. Dostupné z: https://bezpecnostni-sbory.wbs.cz/clanky/6-2011/vynos_z_trestne_cinnosti_a_jeho_modifikace.pdf

výnosů s legálními zdroji prostřednictvím obchodních společností ovládaných zločineckou skupinou, dále nákup a prodej zboží, bankovní operace, legalizace prostřednictvím off-shore¹⁰ jurisdikcí a rovněž využívání internetového prostředí (například online obchodů a sázkových stránek) k zakrytí původu výnosů. V posledně jmenovaných dvou případech lze navíc efektivně využít kryptoměny jako další prvek komplikující dohledání skutečného zdroje finančních prostředků.

Každý z používaných postupů lze rozčlenit do tří základních kategorií procesů – transakce, transfery a transformace. Transakce představují způsob, kterým ekonomické subjekty získávají prostředky za svou produkci, přičemž v kontextu legalizačního jednání mohou sloužit k zastření kriminální aktivity a vytvoření odlišné „identity“ nelegálně nabytého kapitálu. Transfer pak znamená přesun těchto prostředků, přičemž pachatel má na výběr mezi jejich začleněním do legálního ekonomického systému (aniž by vzbudil podezření ohledně původu) nebo přesunem do zemí, které nabízejí malou či téměř žádnou míru kontroly. Transformace spočívá ve změně samotné formy výnosu během transakčního procesu, přičemž jejím hlavním cílem je utajit původ z trestné činnosti. Vzhledem k širší možnosti podob takto získaného kapitálu může být transformace realizována i formou převodu na kryptoměny, které lze dále přesouvat mezi různými platformami a případně využít k nákupu legálního či nelegálního zboží.¹¹

¹⁰ Off-shore znamená cizí země, která umožňuje osobám a firmám, které se nachází mimo tuto zem, získat pro sebe určité výhody.

¹¹ DVOŘÁK, V. *Ekonomické a kriminální aspekty legalizace výnosů z trestné činnosti*. Vyd. 1. Praha: Scientia, 2010. ISBN 978-80-86960-63-0. s. 30 – 36..

3 Legalizace výnosu z trestné činnosti

Problematika legalizace výnosů z trestné činnosti má velmi široký záběr. Vzhledem k tomu, že tato práce se zaměřuje primárně na oblast kryptoměn, budou představeny pouze hlavní znaky dané problematiky. V odborných materiálech a médiích se však často místo termínu „legalizace výnosů z trestné činnosti“ setkáváme s pojmem „praní špinavých peněz“. Tento výraz pochází z anglického „money laundering“ či německého „Geldwäsche“ a údajně má svůj původ ve Spojených státech amerických ve 30. letech 20. století, kdy zločinecké organizace přimíchávaly zločinem získané prostředky k tržbám z veřejných prádelen. Termín „praní špinavých peněz“ je již dlouhodobě zakotven v českém právním řádu, a to od přijetí zákona č. 61/1996 Sb. Vystupuje rovněž ve Štrasburské úmluvě a běžně se používá i v trestním právu.¹² Mezi jednu z ranných definic tohoto jevu lze zařadit také výklad Alexandra Netta, odborníka na trestní právo, podle něhož „špinavé peníze“ označují finanční prostředky získané prostřednictvím trestné činnosti, zejména z obchodování s drogami. „Praní peněz“ pak představuje způsob jejich užití s cílem zakrýt skutečný původ těchto prostředků.¹³ V současné době je tato teze platná pouze zčásti, neboť nezákonné zdroje takzvaných „špinavých peněz“ přesahují oblast drogového obchodu a mohou pramenit i z celé řady jiných komodit či aktivit. Špinavé peníze představují finanční prostředky nabyté z nelegálních zdrojů, jejichž skutečný původ se pachatelé snaží zastříť prostřednictvím transakčních operací, aby vzbudili dojem, že pocházejí z legální ekonomiky. Tento jev se přitom neomezuje na hranice jediné země a má tudíž mezinárodní charakter. V důsledku toho může činnost zločineckých organizací ohrozit i demokratické zřízení státu, zejména podaří-li se jim proniknout do struktur veřejné správy.

Součástí českého právního řádu je rovněž zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu. Jeho § 3 vymezuje podstatu legalizace výnosů z trestné činnosti jako jednání, jehož cílem je zastříť nezákonný původ jakékoli ekonomické výhody plynoucí z trestné činnosti a současně

¹² TVRDÝ, J. *Zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu a předpisy související*: komentář. Vyd. 1. Praha: C. H. Beck, 2009. ISBN 978-80-7400-099-7. s. 101.

¹³ NETT, A. *Praní špinavých peněz*. 1. vyd. Brno: Masarykova univerzita, 1993. s. 3. ISBN 80-210-0630-7.

vyvolat dojem, že jde o majetkový prospěch nabytý v souladu se zákonem.¹⁴ Takové jednání lze rozpoznat zejména v následujících situacích:

a) v přeměně nebo převodu majetku s vědomím, že pochází z trestné činnosti, za účelem jeho utajení, 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, 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).¹⁵

Evropské společenství se problematikou praní špinavých peněz podrobně zabývalo a přijalo v této souvislosti několik směrnic, jež musel zohlednit i výše zmíněný zákon. Konkrétně se jedná o Směrnici Evropského parlamentu a Rady 2005/60/ES ze dne 26. října 2005, zaměřenou na předcházení zneužití finančního systému k praní peněz a financování terorismu, a dále o Směrnici Komise 2006/70/ES ze dne 1. srpna 2006. Ta stanoví prováděcí opatření ke směrnici 2005/60/ES, především ohledně vymezení pojmu „politicky exponované osoby“ a technických kritérií pro zjednodušené postupy hloubkové kontroly klienta, jakož i pro výjimku týkající se finančních činností vykonávaných pouze příležitostně nebo v omezeném rozsahu.

Zákon č. 253/2008 Sb. navazuje rovněž na některé přímo použitelné předpisy tehdejšího Evropského společenství, zejména Nařízení Evropského parlamentu a Rady (ES) č. 1889/2005 ze dne 26. října 2005, upravující kontroly peněžní hotovosti při jejím vstupu do Společenství či výstupu z něj, a Nařízení Evropského parlamentu a Rady (ES) č. 1781/2006 ze dne 15. listopadu 2006, týkající se informací o plátcích, které musejí doprovázet převody peněžních prostředků. Ačkoli jsou uvedené předpisy již neplatné, staly se základem pro přijetí následné legislativy. V současnosti patří mezi stěžejní akty v oblasti mezinárodního boje proti praní špinavých peněz Nařízení Evropského parlamentu a Rady (EU) 2015/847 a Směrnice Evropského parlamentu a Rady (EU)

¹⁴ LIŠKA, P. *Praní špinavých peněz v České republice*. 1. vydání, Praha: RADIX, spol. s r.o., 1997. ISBN 80-86031-09-8, str. 8.

¹⁵ Zákon č. 253/2008 Sb. o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu. In: Sbírka zákonů. 8. 7. 2008. ISSN 1211-1244.

2015/849. Definice legalizace výnosů z trestné činnosti, kterou tato směrnice obsahuje, zůstává obsahově totožná s vymezením obsaženým v zákoně č. 253/2008 Sb.¹⁶

Hlavním motivem, který pachatele vede k legalizaci výnosů z trestné činnosti, je snaha zapojit tyto prostředky do legální ekonomiky, aniž by hrozilo jejich odhalení či odebrání. V případě, že výnos pochází z nelegálních zdrojů, je nutné vytvořit pro něj věrohodnou „legendu“, aby nevzbudil podezření ze strany dozorových orgánů. Přírozenou nevýhodou nelegálních výnosů je fakt, že pokud zůstanou v neoficiální ekonomice, pachatel je nemůže ukládat do bank, investovat či jinak legálně zhodnocovat.

Proces legalizace výnosů z trestné činnosti se zpravidla dělí do tří základních etap, z nichž každou provázejí specifické důvody. V první etapě se pachatel snaží začlenit nelegálně nabyté prostředky do legálního hospodářského systému, přičemž využívá situací, kdy jsou kontrolní mechanismy nefunkční či nedostatečné. V důsledku trestné činnosti vzniká tzv. primární výnos, jenž může mít rozmanité formy (např. tržby, nemovitosti, obchodní podíly). Pokud orgány tento výnos zaregistrují, avšak nedokážou jej přiřadit ke konkrétní nezákonné činnosti, označí jej za výnos z neznámých zdrojů. V druhé etapě pachatel vytváří fiktivní identitu, aby zastřel původ výnosu a předešel jeho odčerpání. Dalším důvodem pro takové maskování je omezená možnost legálního nakládání s nelegálně získanými prostředky a jejich případného zhodnocení. Ve fázi třetí poté pachatel vyhledá vhodný subjekt pro kapitalizaci, čímž dosáhne navýšení výnosu. Tímto postupem vzniká tzv. sekundární výnos, který, ačkoli byl získán nezákonnou cestou, vykazuje vnější znaky legální ekonomické aktivity.¹⁷ Takto „očistěné“ prostředky pak mohou generovat další zisk. Přestože existují účinné nástroje pro odhalování legalizačních praktik, stále se diskutuje, do jaké míry se reálně uplatňují a zda jsou pachatelé schopni využívat znalosti a dovednosti k tomu, aby se těmto opatřením úspěšně vyhnuli.¹⁸

V souvislosti s legalizací výnosů z trestné činnosti dochází k řadě náročných transakčních operací vztahujících se k těmto finančním prostředkům. Tyto operace jsou označovány jako „transformační proces výnosu z trestné činnosti“ a zahrnují jak samotné

¹⁶ Legislativa AML/CFT. Ministerstvo financí České republiky [online]. [cit. 2025-02-01]. Dostupné z: https://www.mfcr.cz/assets/cs/media/Studie_2018_Podkladova-studie-online-identifikace-a-AML-CFT.pdf

¹⁷ CHMELÍK, J., HÁJEK, P. a NEČAS, S. *Úvod do hospodářské kriminality*. 1. vydání, Plzeň: Aleš Čeněk, 2005. ISBN 80-868998-13-X, str. 68.

¹⁸ DVOŘÁK, V. *Ekonomické a kriminální aspekty legalizace výnosů z trestné činnosti*. Vyd. 1. Praha: Scientia, 2010, s. 43 – 46. ISBN 978-80-86960-63-0.

nabytí primárních výnosů, tak jejich následnou legalizaci a vytvoření sekundárního výnosu v rámci legálního ekonomického systému.¹⁹ Pachatelé se v dalším kroku pokoušejí zahltit stopy vedoucí k odhalení původu výnosu, a proto výnosu vytvářejí novou „identitu“, čímž vyvolávají dojem, že je plně v souladu s právní úpravou. Následně jej investují, aby maximalizovali svůj zisk. Ekonomika se přitom dělí na tři základní sféry: legální, šedou a černou ekonomiku. Šedá ekonomika zahrnuje soubor aktivit, které sice často narážejí na běžné společenské a morální normy, avšak zpravidla se pohybují na samé hraně zákona, a tudíž je obtížné je postihnout. Může jít také o samozásobení či sousedskou výpomoc. Naproti tomu černá ekonomika představuje oblast aktivit porušujících platné právní předpisy (vnitrostátní i mezinárodní) a je zcela nelegální, což znamená, že odhalená a prokázaná činnost tohoto druhu bývá trestně sankcionována. Černá ekonomika se dále dělí na neprodukční sféru a kriminální ekonomiku. V neprodukční části nevznikají nové hodnoty; výnos zde pramení z nezákonného převádění prostředků původně pocházejících z legálního zdroje – například při nelegálním obchodování s produkty vytvořenými v rámci legitimní činnosti. V kriminální ekonomice pak dochází k produkci zboží a služeb, přičemž se uplatňují všechny základní ekonomické prvky (ekonomické aktivity, transakce a příjmy). Veškerá zdrojová kriminalita spadá do černé ekonomiky, stejně jako tzv. zlegalizovaný a sekundární výnos, který je sice na první pohled propojen s legální ekonomikou, avšak ve své podstatě zůstává součástí ekonomiky černé.²⁰

V úvodní fázi legalizace výnosů z trestné činnosti jde především o strategické rozmístění prostředků. Typicky se jedná o využití společností, které za úplatu provádějí drobné vklady do bankovních účtů (tzv. smurfing), tak aby tyto transakce nevyvolaly podezření. Následně se peníze bezhotovostně přesouvají na jeden či několik málo účtů. Dalším rozšířeným postupem je tzv. směšování tržeb, kdy dochází ke spojení příjmů z legálních aktivit s nelegálními a následnému vykázání zisku v souhrnné tržbě. Pachatelé rovněž využívají nastrčené osoby či fiktivní společnosti, které pouze předstírají legální podnikání, avšak ve skutečnosti generují veškeré příjmy z nelegálních zdrojů. Největšího efektu bývá dosaženo prostřednictvím bank, buď bez vědomí jejich zaměstnanců, nebo za jejich aktivní účasti. V některých případech pak existují instituce, jejichž hlavním cílem je právě legalizace výnosů z trestné činnosti, zatímco deklarovaná bankovní činnost

¹⁹ DVOŘÁK, V. *Ekonomické a kriminální aspekty legalizace výnosů z trestné činnosti*. Vyd. 1. Praha: Scientia, 2010, s. 11. ISBN 978-80-86960-63-0

²⁰ DVOŘÁK, V. *Ekonomické a kriminální aspekty legalizace výnosů z trestné činnosti*. Vyd. 1. Praha: Scientia, 2010, s.20. ISBN 978-80-86960-63-0.

slouží pouze jako zástěrka. Tyto subjekty se často nacházejí v tzv. daňových rájích – státech poskytujících zahraničním společnostem zvýhodněný daňový režim, včetně nízké či zcela nulové daňové povinnosti.²¹

Ve druhé fázi se pachateli jedná o zahalení nelegálního původu finančních prostředků. Toho se dosahuje převodem z jednoho účtu na druhý, ideálně do zahraničí, výběrem hotovosti a následným vložením do jiné banky, či nákupem cenných papírů, uměleckých děl nebo drahokamů. Tyto operace uskutečňují jak subjekty s reálnou podnikatelskou činností, které se dané problematice věnují, tak i čistě účelově založené, fiktivní společnosti náležející zločinecké organizaci. Hlavním cílem je znesnadnit dohledání skutečného zdroje a vytvořit tak řadu transakcí, v nichž je těžké se vyznat. Jakmile jsou prostředky „očištěny“ a jejich původ zastřen, vracejí se zpět jejich vlastníkově, který je ve třetí fázi využívá v legální ekonomice, například k nákupu či investicím do firem, nemovitostí nebo cenných papírů, případně k dalšímu zastírání původu finančních zdrojů.²²

Jednotlivé státy vytvářejí vlastní mechanismy pro potírání legalizace výnosů z trestné činnosti, přičemž na mezinárodní úrovni působí řada institucí s obdobným posláním. K nejvýznamnějším patří zejména Evropská komise, Rada Evropy, Finanční akční výbor (Financial Action Task Force, FATF) a Světová banka ve spojení s Mezinárodním měnovým fondem. Na tyto aktivity rovněž navazují další subjekty, jako například Interpol.

V rámci této problematiky zřídila Evropská komise Výbor pro prevenci praní peněz a financování terorismu, jenž se schází několikrát do roka. Rada Evropy pak v roce 1998 založila Výbor expertů pro hodnocení opatření proti praní špinavých peněz a financování terorismu (tzv. MONEYVAL), jehož činnost vychází z doporučení Finančního akčního výboru (FATF) zaměřených na tvorbu mezinárodních standardů a hodnocení jurisdikcí v oblasti boje proti praní špinavých peněz. Hlavním cílem MONEYVAL je zajistit, aby členské státy disponovaly dostatečnou infrastrukturou pro potírání praní špinavých peněz a financování terorismu. Základem jeho fungování je systém vzájemného hodnocení, v jehož rámci experti z členských zemí podnikají

²¹ Daňové ráje [online]. [cit. 2025-02-10]. Dostupné z: <http://www.danoveraje.eu>

²² DVOŘÁK, V. *Ekonomické a kriminální aspekty legalizace výnosů z trestné činnosti*. Vyd. 1. Praha: Scientia, 2010, s.

inspekce vybraného státu, kde posuzují reálnou funkčnost a efektivitu zavedených opatření.²³

Světová banka a Mezinárodní měnový fond organizují konference a semináře zaměřené na boj proti legalizaci výnosů z trestné činnosti a financování terorismu. V rámci jejich aktivit rovněž vznikají projekty, jejichž cílem je zejména finančním způsobem posílit schopnosti jednotlivých zemí v oblasti potírání praní špinavých peněz.²⁴

V České republice se na odhalování legalizace výnosů z trestné činnosti podílí především Finanční analytický útvar Ministerstva financí (dále FAÚ), Policie České republiky (zejména Útvar odhalování korupce a finanční kriminality SKPV) a tzv. povinné osoby, které mají dle zákona povinnost poskytovat FAÚ požadované informace. FAÚ se zabývá prověřováním podezřelých obchodů hlášených těmito subjekty, vykonává kontrolní činnost, podílí se na přípravě legislativy v oblasti potírání praní špinavých peněz a rovněž spolupracuje se zahraničními partnery.²⁵ Útvar odhalování korupce a finanční kriminality SKPV představuje celostátní policejní složku zaměřenou na vyšetřování nejzávažnějších forem hospodářské, finanční a korupční trestné činnosti, jejíž působnost pokrývá celé území České republiky.²⁶

V souladu s § 2 zákona č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, jsou vymezeny tzv. „povinné osoby“ a jejich příslušná práva a povinnosti. Mezi tyto povinné osoby patří především úvěrové instituce, jako jsou banky, spořitelny a úvěrní družstva či instituce elektronických peněz. Dále sem náleží finanční instituce, pokud současně nejsou institucemi úvěrovými, auditori, daňoví poradci a účetní, osoby oprávněné k obchodování s nemovitostmi či k jejich zprostředkování a řada dalších subjektů. Klíčové povinnosti povinných osob zahrnují zejména identifikaci klientů, informační povinnost a archivaci údajů. Identifikace klienta je vyžadována v situacích, kdy objem obchodu převyšuje 1 000 eur (bez ohledu na to, zda se jedná o jednorázovou platbu či splátky), popřípadě jde-li o

²³ Moneyval. Nejvyšší státní zastupitelství [online]. [cit. 2025-02-10]. Dostupné z: <https://www.nsz.cz/index.php/cs/mezinarodni-spoluprace/dali-organizace/moneyval>

²⁴ Mezinárodní spolupráce - Boj proti praní peněz a financování terorismu. Ministerstvo financí České republiky [online]. [cit. 2025-02-10]. Dostupné z: <https://www.mfcr.cz/cs/zahranicni-sektor/mezinarodni-spoluprace/mezinarodni-institute/mezinarodni-spoluprace-boj-proti-prani11642>

²⁵ Základní informace. Ministerstvo financí České republiky [online]. [cit. 2025-02-10]. Dostupné z: <https://www.mfcr.cz/cs/zahranicni-sektor/ochrana-financnich-zajmu/boj-proti-prani-penez-afinancovani-tero/zakladni-informace>

²⁶ Útvar odhalování korupce a finanční kriminality SKPV. Policie České republiky [online]. [cit. 2025-02-10]. Dostupné z: <https://policie.gov.cz/clanek/uokfk-skpv-utvar-odhalovani-korupce-a-financni-kriminality-skpv.aspx>

podezřelý obchod. V případě fyzické osoby se ověřují údaje typu jména a příjmení, rodného čísla, pohlaví, místa narození, trvalého či jiného pobytu a státní příslušnosti. U právnické osoby se zjišťuje název firmy, identifikační číslo a osoby tvořící statutární orgán. Pokud hodnota transakce přesáhne 15 000 eur, musí povinná osoba provést hloubkovou kontrolu klienta, která zahrnuje například zjištění účelu obchodu, průběžné sledování obchodního vztahu a přezkoumání zdrojů finančních prostředků.²⁷

²⁷ Zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu

4 Kryptoměny

Kryptoměny lze charakterizovat jako specifický prostředek směny, obdobný konvenčním měnám, avšak primárně určený k digitálnímu přenosu informací. Bezpečnost transakcí a regulace nově vytvořených „mincí“ se opírá o kryptografické postupy. Samotný pojem „kryptoměna“ představuje český ekvivalent anglického „cryptocurrency“, složeného z výrazů „crypto“ (kryptografie) a „currency“ (měna). První kryptoměnou svého druhu byl bitcoin, uvedený na trh v roce 2009. V současné době ovšem existují již stovky dalších kryptoměn.

V nejjednodušší podobě lze kryptoměnu definovat jako digitální měnu, která je elektronicky vytvářena a uchovávána, přičemž slouží k provádění transakcí v prostředí internetu. V odborné i populární praxi bývá taktéž označována jako „virtuální měna“. Jakub Jedlinský uvádí: „Kryptoměnou rozumím jakoukoli soustavu jednotek, které jsou kvantifikovatelným vyjádřením hodnoty, pro svůj přenos využívají technologie blockchainu a jejím nosičem je string získaný hashovací funkcí.“²⁸ Blockchain lze definovat jako databázi uchovávající všechny uskutečněné transakce od počátku fungování dané sítě. Tato databáze je replikována na neomezeném množství uzlů (počítačů obsahujících úplnou kopii blockchainu), čímž je zajištěna decentralizace i autenticita záznamů – případný neautorizovaný zásah do jedné kopie nemůže ovlivnit ty zbývající.²⁹ Takto vzniká decentralizovaná síť sloužící k přenosu dat, přičemž její správu neřídí jeden konkrétní subjekt, ale série počítačových mechanismů, které zajišťují pravidelnou aktualizaci blockchainu na všech uzlech. V této souvislosti hraje klíčovou roli tzv. „hash“ (též string), tedy řetězec znaků generovaný hashovací funkcí, jenž je jednoznačný pro každou transakci. Příslušná hashovací funkce funguje jako šifrovací nástroj, umožňující mimo jiné dopočítat nové hashe na základě předchozích i z adres peněženek, na něž směřovaly transakce. Z ekonomického pohledu je podstatné, že uzly sítě poskytují svou výpočetní kapacitu k vyřešení rovnic, jejichž výsledkem je vznik nového bloku, a tedy nového stavu blockchainu. Každý uzel má přitom zpětnou možnost

²⁸ JEDLINSKÝ, J. *Jsou kryptoměny bublinou nebo mají význam pro světové hospodářství?* In: HUJOVÁ, G. ed. *Zkušenosti s virtuálními měnami - Bitcoin měna budoucnosti?*: sborník z konference: Praha, 26. března 2014. Praha: Vysoká škola manažerské informatiky, ekonomiky a práva, 2014, s. 44

²⁹ STROUKAL, D. a SKALICKÝ, J. *Bitcoin: peníze budoucnosti: historie a ekonomie kryptoměn, stručná příručka pro úplné začátečníky*. Praha: Ludwig von Mises Institut CZ, 2015. ISBN 978-80-87733-26-4, str. 20-21.

ověřit správnost výpočtů a tím potvrdit, že například peněženka ABC obsahuje určité množství měny XYZ.³⁰

Ve srovnání s fiat měnami (tj. oficiálními národními měnami s nuceným oběhem, emitovanými v souvislosti se vznikem dluhu) nabízejí kryptoměny několik významných předností. Zatímco státní peníze lze považovat za zadlužené a často nedostačující pro potřeby reálné ekonomiky, kryptoměny jsou přístupné komukoli a působí jako doplňující forma oběhiva. Jejich stěžejním rysem je motivace k úsporám a snaha zefektivnit a urychlit platební styk, přičemž transakce nejsou zatíženy poplatky. Kryptoměny fungují decentralizovaně, tedy bez centrální autority, a zároveň umožňují částečnou anonymitu – všechny platby jsou zajištěny kryptograficky, přičemž soukromé peněženky sestávají z numerických kódů, veřejných a soukromých klíčů. Naproti tomu fiat měny nemusejí prokazovat svou hodnotu, důvěryhodnost ani stabilitu, neboť tyto atributy jim garantuje zákon. Stát rovněž vytváří poptávku po měně tím, že v ní vybírá daně. Kryptoměny jsou ovšem často spojovány s legalizací výnosů z trestné činnosti, jelikož zatímco objem prostředků držených ve virtuálních peněženkách lze v principu vysledovat, identifikace konkrétních držitelů bývá mnohem obtížnější.

Většina kryptoměn je koncipována tak, aby se jejich emise postupně snižovala, jak je tomu například u bitcoinu, jehož maximální počet je stanoven na 21 milionů mincí. Tím se výrazně odlišují od státních měn, které mohou být finančními institucemi libovolně dotvářeny, což následně vede k inflaci. Základy, na nichž spočívá většina kryptoměn, vypracoval Satoshi Nakamoto. Ačkoli v současnosti existují stovky různých kryptoměn, zpravidla se odvozují ze dvou typů protokolů – proof-of-work či proof-of-stake. Udržování systému zajišťuje komunita těžařů (tzv. „minerů“), tj. uživatelů poskytujících svůj výpočetní výkon pro validaci a zpracování transakcí (tzv. bitcoin mining). Kryptoměny, které vznikly odvozením od bitcoinu, se označují jako altcoiny a snaží se zdokonalit původní bitcoinový protokol. V dubnu 2011 byl uveden první altcoin s názvem Namecoin, jehož cílem bylo především snižování internetové cenzury. V říjnu téhož roku se objevil Litecoin, který umožnil širokému okruhu uživatelů těžit tuto kryptoměnu bez specializovaného hardwaru typu ASIC, běžně užívaného u bitcoinu. Mediální pozornost si Litecoin získal koncem roku 2013, kdy dosáhl tržní kapitalizace o hodnotě jedné miliardy amerických dolarů. Ripplecoin, který byl vyvinut roku 2011,

³⁰ JEDLINSKÝ, J. *Jsou kryptoměny bublinou nebo mají význam pro světové hospodářství?* In: HUJOVÁ, G., ed. *Zkušenosti s virtuálními měnami - Bitcoin měna budoucnosti?: sborník*

vychází ze stejného protokolu jako bitcoin, odlišuje se však v samotném platebním systému. Přestože bitcoin není v absolutních číslech nejcennější kryptoměnou, zůstává nejrozšířenější a nejznámější, přičemž se řadí k lídrům trhu spolu s Ethereum, Ripplecoinem a Litecoinem. Těžební výkonnost kryptoměn je vyjadřována v počtu hashů za sekundu, přičemž každý nově vyřešený blok generuje také nový hash. Z hlediska bezpečnosti kryptoměn lze zdůraznit dva klíčové aspekty. První spočívá v technické náročnosti získání správného hash, druhým je tzv. „51% útok“, při němž by těžář s většinovým podílem výpočetního výkonu v síti teoreticky mohl blockchain ovládnout a například zvrátit své vlastní transakce či blokovat transakce jiných uživatelů. Ani v tomto případě však jeho možnosti zůstávají omezené. Kryptoměny jsou navíc méně zranitelné případným státním zabavením, bývají proto označovány jako „pseudo-anonymní“. Některé z nich navíc obsahují funkce vedoucí k dosažení téměř úplné anonymity. Existuje rovněž řada internetových platforem a služeb, které slouží ke sledování a analyzování kryptoměn. CoinMarketCap poskytuje přehled o aktuálních tržních lidech, cenových hladinách, dostupném objemu a obchodovaném množství. Komunitní platforma Reddit umožňuje uživatelům diskutovat, sdílet zkušenosti a sledovat aktuální trendy. Web CryptoCoinCharts nabízí údaje o výměnách, možnostech arbitráže a seznamu různých kryptoměn, zatímco CryptoCoinsNews monitoruje změny v jejich hodnotách za posledních 24 hodin, týden či měsíc. Nástroj CoinWarz pak pomáhá těžářům zjistit, která kryptoměna je v daném okamžiku nejvýnosnější pro těžbu, a současně poskytuje historická data ohledně vývoje ziskovosti těžby.³¹

4.1.1 Bitcoin

Bitcoin se řadí k nejstarším kryptoměnám, jeho počátky spadají do roku 2008. Koncem listopadu téhož roku obdržela skupina kryptografů a programátorů e-mail od uživatele vystupujícího pod pseudonymem Satoshi Nakamoto (jehož skutečná identita dosud nebyla objasněna), který je informoval o vytvoření nové kryptoměny pojmenované bitcoin a vyzval je k účasti na jejím dalším vývoji. Podle Nakamotova sdělení se jedná o online směnný systém využívající šifrování, který dvěma stranám umožňuje obchodovat s virtuálními „žetony“ s určitou hodnotou, a to bez nutnosti sdílet osobní údaje či využívat služby zprostředkujícího subjektu (např. platební karty). Transakce se uskutečňuje prostřednictvím privátního, tedy tajného, kódu k ověření klíče, jenž zajišťuje držbu

³¹ GRAYDON, C. *What is Cryptocurrency?* In: CCN: Bitcoin, Blockchain, FinTech; Cryptocurrency News[online]. [cit. 2025-02-02]. Dostupné z: <https://www.cryptocoinsnews.com/cryptocurrency/>

digitální měny. Možnost vstupu do sítě má díky tomuto principu prakticky každý, kdo vlastní či spravuje vhodný počítač.

Klíčovou výhodou bitcoinu se stala jeho naprostá nezávislost na centrální autoritě a využití matematických algoritmů, které by mělo bránit jakýmkoliv manipulacím. Nakamoto zároveň spustil webové stránky projektu a vytvořil počáteční bitcoinový blok. V počáteční fázi vygeneroval několik bitcoinů, jež však postrádaly faktickou hodnotu, pokud by se k síti nikdo další nepřidal. Pro etablování bitcoinu bylo nezbytné stanovit jeho cenu, která se komunitním konsenzem ustálila na přibližně 1 dolar za 1,3 bitcoinu. Bitcoinová komunita rovněž zřídila diskusní fórum, na kterém Nakamoto 12. prosince 2010 odeslal svou poslední zprávu a poté přerušil veškerou veřejnou komunikaci. Několika vývojářům zůstal k dispozici až do dubna 2011. V té době se cena za jeden bitcoin pohybovala kolem 0,14 centů, avšak postupně stoupala.³²

Zásadní zlom v praktickém užití bitcoinu nastal, když programátor Laszlo Hanyecz, v době, kdy měl příslušné fórum pouhých 230 členů, nabídl 10 000 bitcoinů (ekvivalent 41 dolarů) výměnou za dvě pizzy. Zpočátku nedošlo k žádné odezvě, protože bitcoin se dosud nepoužíval v reálném platebním styku. Po několika dnech souhlasil muž z Anglie, který pizzy objednal a zaplatil v dolarech; Hanyecz mu na oplátku zaslal bitcoiny. Šlo tak o první praktické využití bitcoinu jako platidla. Roku 2013 začali výhody nabízené kryptoměnami zaznamenávat i obchodníci, neboť díky nezávislosti na bankách a nižším transakčním poplatkům mohou kryptoměny představovat atraktivní nástroj i pro maloobchod.

Navzdory nepochybným přínosům s sebou bitcoin nese i určité nevýhody. Pokud při konvenční platbě kartou dojde k chybné transakci či odcizení karty, klient má možnost platbu pozastavit či kartu zablokovat. U bitcoinu takový postup není realizovatelný: jednou odeslané prostředky nelze stornovat či vrátit a ztráta privátního klíče zpravidla znamená nenávratnou ztrátu všech mincí. Přesto existují bezpečnostní nástroje, například funkce „virtuálního trezoru“ umožňující časovou prodlevu a upozornění majitele, pokud dojde k odebrání prostředků. Mezi klíčové riziko patří tzv. problém „dvojití útraty“ (double-spending), při němž by jedna osoba mohla stejnou digitální měnu poslat dvěma stranám zároveň. Satoshi Nakamoto toto nebezpečí vyřešil uplatněním decentralizovaného systému, kde transakce zaznamenává veřejně přístupná hlavní účetní

³² LÁNSKÝ, J. *Kryptoměny*. Praha: C.H. Beck, 2018. ISBN 978-80-7400-722-4, str. 57.

kniha (blockchain). Blockchain slouží jako jádro celého systému, ve kterém se všechny transakce evidují transparentně. Držitel privátního klíče může v síti uskutečňovat platby a každá nová operace se automaticky ukládá do blockchainu. Jakmile transakce nepřetržitě probíhají, blockchain se nadále rozšiřuje, a je tak možné sledovat veškeré příjmy a výdaje časově zařazené do bloků. Tím je eliminováno riziko podvodných převodů, neboť žádný uživatel nemůže jedny a tytéž bitcoiny utratit vícekrát.³³

V raných fázích bitcoinové sítě bylo pro těžáře relativně snadné získávat nové mince, avšak s rostoucí oblibou bitcoinu se jejich těžba stala náročnější. V současnosti se používají mimořádně výkonné počítačové systémy s vysokou energetickou náročností, což výrazně zvyšuje provozní náklady. Bitcoin má řadu zastánců i odpůrců: kritici poukazují především na chybějící vnitřní hodnotu a nazývají jej „bublinou“. Někteří v něm spatřují ráj pro spekulanty, zatímco jiní důvěřují jeho dalšímu potenciálnímu růstu. Za úspěšným vývojem bitcoinu zčásti stojí i skupina mladých talentovaných vývojářů, kteří projevíli nespokojenost se stávajícím finančním systémem. Ačkoli lze obecnou myšlenku bitcoinu pochopit poměrně snadno, vysvětlit konkrétní důvody prudkého vzestupu jeho tržní hodnoty je obtížnější. Přesto, že bitcoin v sobě nese povahu rizikového kapitálu (během jednoho pololetí jeho cena klesla z 1 151 dolarů na méně než 500 dolarů za minci), neustále přibývá nových uživatelů, kteří věří, že bitcoin se teprve nachází na počátku své cesty k úspěchu.³⁴

4.1.2 Vývoj hodnoty Bitcoinu

V roce 2009 se Bitcoin nacházel ve své rané fázi vývoje a veškeré transakce probíhaly pouze mezi úzkým okruhem nadšenců. Až v říjnu téhož roku byla zveřejněna první oficiální směnná hodnota, podle níž bylo možné za jeden dolar získat 1 309 bitcoinů. Po zbytek roku se pak cena bitcoinu pohybovala v řádu zlomků centu. V jarních měsících roku 2010 došlo k první reálné směně, kdy Laszlo Hanyecz za bitcoiny nakoupil zboží, a tím stanovil hodnotu bitcoinu na úroveň nižší než 0,01 USD.

S cílem rozšířit okruh uživatelů a zpřístupnit obchodování byla spuštěna první kryptoměnová burza Mt. Gox. Objem transakcí začal následně narůstat a v listopadu

³³ VIGNA, P. a CASEY, M. *The Age of Cryptocurrency*. In: *The Investing Podcast* [online]. [cit. 2025-02-02]. Dostupné z: <https://archive.org/details/ageofcryptocurre0000vign/>

³⁴ VIGNA, P. a CASEY, M. *The Age of Cryptocurrency*. In: *The Investing Podcast* [online]. [cit. 2025-02-02]. Dostupné z: <https://archive.org/details/ageofcryptocurre0000vign/>

2010, kdy bylo vytěženo již přibližně čtyři miliony bitcoinů, vzrostla cena jedné mince na 50 centů. V únoru 2011 zahájilo činnost internetové tržiště Silk Road, umožňující nákupy a prodeje výhradně za bitcoiny, přičemž cena bitcoinu poprvé dosáhla hodnoty jednoho dolaru. Tato událost přilákala nové uživatele a spekulanty, což vedlo k prudkému nárůstu ceny na 31 dolarů za minci v červnu téhož roku. Následné hackerské útoky na burzu Mt. Gox však otřásl důvěrou investorů a hodnota bitcoinu se propadla až ke dvěma dolarům za kus.³⁵

V následujících měsících cena stagnovala, dokud v červenci 2012 nedosáhla hodnoty sedmi dolarů. Bitcoin si postupně získával pozornost větších společností, jako například Wordpress či Reddit, a k jeho dalšímu zviditelnění přispěla finanční krize na Kypru, neboť banky omezily výběry hotovosti z účtů, zatímco u bitcoinu takové opatření není možné provést. Reakcí na rostoucí zájem uživatelů bylo první regulační nařízení amerického ministerstva financí, které bitcoin neoznačilo za nelegální měnu, čímž povzbudilo další investory a zvýšilo cenu bitcoinu.³⁶

Následně vznikla například směnárna BitInstant, usnadňující rychlý nákup kryptoměny. V dubnu 2013 se cena bitcoinu vyšplhala na 266 dolarů, avšak během pouhých šesti hodin klesla na polovinu. Pokles pokračoval až k hodnotě 70 dolarů, odkud se cena zvolna vrátila ke 100 dolarům. Postupem času se objevily nové projekty, například Coinbase, nabízející uživatelům online peněženky, a BitPay coby platební brána pro obchodníky přijímající bitcoiny. V letních měsících 2013 podpořili rostoucí hodnotu bitcoinu také investoři z Číny, čímž cena v listopadu daného roku stoupla až k 350 dolarům. Na samém konci roku 2013 bitcoin dokonce překonal hranici 1 000 dolarů.³⁷

Počátek roku 2014 však nepřál dalšímu rozmachu. Zatčení osob spojených se směnárnou BitInstant a rostoucí obavy o solventnost Mt. Gox vyústily v odhalení rozsáhlého hackerského útoku na tuto burzu a ztrátu bitcoinů v hodnotě téměř půl milionu dolarů, což vedlo k jejímu krachu. Cena bitcoinu se tehdy propadla na 500 dolarů, krátce vystoupala na 600 a poté klesla k 370 dolarům. Během roku 2015 se hodnota bitcoinu

³⁵ Royal, J. Ph.D. *Bitcoin's price history: From its 2009 launch to its 2025 heights* [online]. [cit. 2025-02-27]. Dostupné z: <https://www.bankrate.com/investing/bitcoin-price-history>

³⁶ Wikipedia.org *History of bitcoin* [online]. [cit. 2025-02-27]. Dostupné z: https://en.wikipedia.org/wiki/History_of_bitcoin

³⁷ Rooney, B. *Bitcoin prices top \$1,000* [online]. [cit. 2025-02-27]. Dostupné z: <https://money.cnn.com/2013/11/27/investing/bitcoin-1000/>

držela v rozpětí 200–300 dolarů, až koncem září začala opět mírně stoupat. V prosinci překonala hranici 450 dolarů za minci a následně vykazovala drobné výkyvy.³⁸

Od roku 2016 prošel bitcoin dalším bouřlivým vývojem, který zahrnoval nárůsty i prudké poklesy jeho tržní hodnoty. Na přelomu let 2016 a 2017 se cena držela v řádu několika stovek dolarů, avšak v průběhu roku 2017 postupně rostla a v prosinci téhož roku dosáhla přibližně 20 000 USD za bitcoin. Tento nárůst byl připisován mimo jiné rostoucímu zájmu drobných investorů a počínajícímu vstupu institucionálních hráčů do kryptoměnového sektoru. V následujícím roce 2018 však přišel výrazný propad, kdy se hodnota bitcoinu ustálila zhruba mezi 3 000 a 4 000 USD. Během roku 2019 se cena začala znovu postupně zvyšovat a na počátku roku 2020, navzdory nejistotám spojeným s pandemií COVID-19, setrvala kolem hranice 7 000 až 9 000 USD. Následné období bylo ve znamení několika faktorů podporujících další růst – k již existujícímu zájmu retailových investorů se přidaly větší institucionální investice a širší akceptace bitcoinu jako uchovatele hodnoty.³⁹

V roce 2020 se zároveň uskutečnila tzv. třetí „půlení“ (halving), kdy se odměna pro těžaře za vytěžený blok opět snížila na polovinu. Tento mechanismus je obecně spojován s potenciálním růstem ceny, neboť omezuje rychlost emise nových mincí. Na konci roku 2020 a především v prvním pololetí 2021 dosáhl bitcoin dalších historických maxim, přičemž v listopadu 2021 krátce překonal hranici 68 000 USD za minci. Přesto však během roku 2022 prošel zásadní korekcí, kdy se jeho hodnota vlivem globálních makroekonomických tlaků, geopolitických nejistot a několika otřesů na kryptoměnových trzích (včetně krachu některých burz a projektů) propadla ke hranici 16 000 USD.⁴⁰

³⁸ Wikipedia.org *Mt. Gox* [online]. [cit. 2025-02-27]. Dostupné z: https://en.wikipedia.org/wiki/Mt._Gox

³⁹ Edwards, J. *Bitcoin's Price History* [online]. [cit. 2025-02-27]. Dostupné z: <https://www.investopedia.com/articles/forex/121815/bitcoins-price-history.asp>

⁴⁰ *The 2024 Bitcoin Halving: Analyzing Past Trends to Predict the Next Big Crypto Surge* [online]. [cit. 2025-02-27]. Dostupné z: <https://www.bitpay.com/blog/analyzing-past-btc-halvings>

Obrázek č. 1 Vývoj hodnoty Bitcoin od roku 2016 do 2025 v USD⁴¹



V průběhu roku 2023 vykazoval bitcoin částečné zotavení, přičemž investoři opět začali spekulovat na možný obrat trendu. Těžištěm pozornosti se stala nadcházející událost tzv. čtvrtého půlení (předpokládána na jaře roku 2024), kdy se opět sníží odměna za vytěžení bloku. Přestože se část trhu domnívá, že halving by mohl opět podnítit růst ceny bitcoinu, zůstává výhled do konce roku 2024 nejistý a do značné míry závisí na faktorech, jako je regulace kryptoměn, světová ekonomická situace či technologické inovace v oblasti blockchainu. Z historického hlediska lze však konstatovat, že bitcoin i přes četné výkyvy nadále přitahuje zájem širokého spektra uživatelů – od drobných investorů až po velké finanční instituce – a jeho cenový vývoj od roku 2016 až k roku 2024 tak demonstruje setrvalou dynamiku a rostoucí institucionální význam této nejznámější kryptoměny.⁴²

4.1.3 Ethereum

Ethereum, jehož základní jednotkou je Ether (ETH), bylo uvedeno na trh v roce 2015 a jeho vznik byl inspirován Bitcoinem. Klíčovým rozdílem oproti Bitcoinu je technická architektura sítě, která výrazně rozšiřuje možnosti blockchainové technologie. Zatímco Bitcoin slouží primárně jako platební systém, v jehož blockchainu jsou

⁴¹ Google finance. [online]. <https://www.google.com/finance/quote/BTC-USD?window=MAX>. 2025. Dostupné z: <https://www.google.com/finance/quote/BTC-USD?window=MAX>. [cit. 2025-02-09]

⁴² Cochintu, C. *The next bitcoin (BTC) halving* [online]. [cit. 2025-02-27]. Dostupné z: <https://capex.com/en/academy/bitcoin-halving-2024>

zaznamenávány výhradně finanční transakce, Ethereum představuje komplexní platformu umožňující tvorbu decentralizovaných aplikací (DApps), programů a chytrých kontraktů (smart contracts). Chytrý kontrakt je autonomní program uložený v blockchainu, který vykonává předem definované podmínky bez nutnosti zásahu třetích stran. Tento mechanismus zajišťuje transparentnost a nezměnitelnost pravidel, čímž eliminuje potřebu prostředníků.

V rámci transakční rychlosti Ethereum vykazuje výrazně kratší dobu potvrzení, přibližně 12 sekund, zatímco transakce v síti Bitcoin trvají průměrně více než 10 minut. Další zásadní odlišností oproti Bitcoinu je absence pevně stanoveného maximálního množství Etheru, přičemž nové jednotky této kryptoměny jsou generovány průběžně. Historicky nejvyšší hodnoty dosáhl Ether na konci roku 2017, kdy jeho cena činila přibližně 1 400 USD. Aktuálně se hodnota této kryptoměny pohybuje okolo 2 650 USD. Z hlediska celkové tržní kapitalizace, která dosahuje přibližně 24,5 miliard USD, si Ethereum udržuje pozici druhé nejvýznamnější kryptoměny na trhu.⁴³

Ethereum prošlo v průběhu let významným technologickým i ekonomickým vývojem, který výrazně ovlivnil jeho postavení na trhu kryptoměn. Mezi klíčové milníky patří přechod na konsensuální mechanismus Proof of Stake (PoS) v rámci aktualizace Ethereum 2.0, která byla zahájena v roce 2020 a vyvrcholila tzv. The Merge v září 2022. Tento přechod odstranil potřebu těžby prostřednictvím Proof of Work (PoW) a výrazně snížil energetickou náročnost sítě, což zvýšilo její udržitelnost a efektivitu.

⁴³ Ethereum: *Home of Ethereum* [online]. [cit. 4.2.2020]. Dostupné z: <https://www.ethereum.org>

Obrázek č. 2 Vývoj hodnoty Bitcoin od roku 2016 do 2025 v USD⁴⁴



⁴⁴Google finance. [online] <https://www.google.com/>. 2025. Dostupné z: <https://www.google.com/finance/quote/ETH-USD?window=MAX>. [cit. 2025-02-09]

5 Vývoj kyberkriminality za užití kryptoměn

Kryptoměny představují relativně nový a dosud ne zcela zmapovaný fenomén, proto je poměrně obtížné předložit ucelený výčet možností, jak jich lze využít k legalizaci výnosů z trestné činnosti. V podmínkách České republiky dosud není znám žádný publikovaný případ, v němž by kryptoměny v této souvislosti sehrály roli, zatímco ve světě bylo odhaleno jen několik ojedinělých kauz. První krok vždy spočívá v získání finančních prostředků z nelegálních zdrojů, případně jinou protiprávní cestou – například prostřednictvím fiktivních e-shopů, phishingu, ransomware programů nebo přímé hotovosti („kufríku plného peněz“). S výjimkou využití bitcoinmatu je pokaždé zapotřebí bankovní účet, z něhož se provede směna peněz za kryptoměnu. Přestože níže uvedené přístupy nejsou vyčerpávající, ilustrují alespoň některé způsoby, jak by pachatelé mohli postupovat. V zájmu jednoduchosti se přitom soustředíme na bitcoin, neboť ten v českém prostředí nabízí nejvíce příležitostí pro praktickou manipulaci.⁴⁵

5.1.1 Konverze výnosů z trestné činnosti do kryptoměn

Konverze výnosů z trestné činnosti do kryptoměn může být realizována prostřednictvím internetových směnár a burz. K tomu postačí využít službu, která umožňuje směnu bez nutnosti registrace. Uživatel zadá požadovanou částku ke směně, uvede svou e-mailovou adresu a adresu kryptoměnové peněženky. Následně obdrží pokyny k provedení platby. Některé směnárny však mohou stanovit limity na maximální výši transakce. Například platforma SimpleCoin umožňuje nákup kryptoměn bez registrace a ověření identity do výše 200 € během 10 dnů. Pro transakce v rozmezí 200 € až 9 999 € za 30 dní je vyžadována registrace a ověření totožnosti. Při překročení částky 10 000 € za 30 dní je navíc nutné doložit původ finančních prostředků.⁴⁶

Kryptoměny lze získat nejen prostřednictvím směnár a burz, ale také přímou transakcí mezi jednotlivci. K vyhledávání nejbližších nabídek na základě geografické polohy slouží například globální platforma LocalBitcoins.com. Tento způsob nákupu však obvykle vyžaduje bankovní účet, skrze který se transakce realizuje. Aby se pachatel vyhnul přímé identifikaci spojené s vlastním bankovním účtem, může založit nový účet

⁴⁵ KOLOUCH, J. a BAŠTA, P. *CyberSecurity*. CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2019. ISBN 978-80-88168-31-7., s. 83.

⁴⁶ Cena je platná ke dni 2. února 2025. SimpleCoin - snadný nákup Bitcoinů [online]. [cit. 2025-02-02]. Dostupné z: <https://simplecoin.cz>

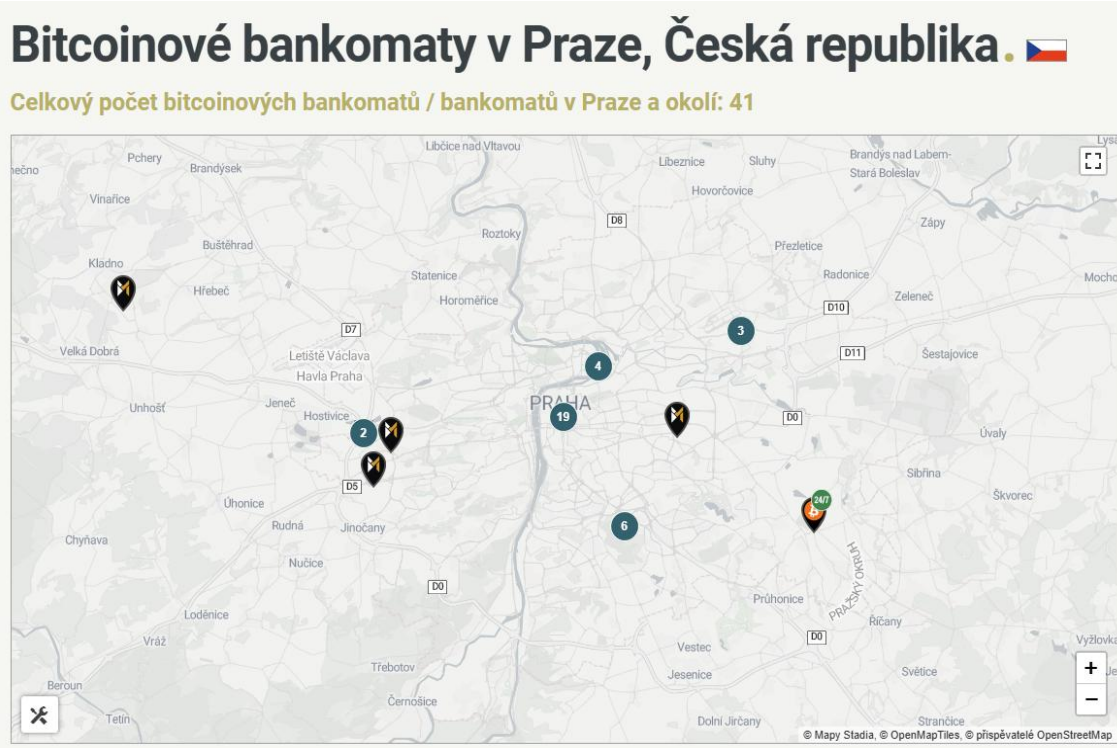
na základě padělaných dokladů totožnosti. Další metodou konverze finančních prostředků na kryptoměnu je využití tzv. bílých koní. V tomto případě pachatel vyhledává jedince ze sociálně znevýhodněných skupin, například osoby bez domova nebo jedince s nižší úrovní vzdělání. Ti jsou následně motivováni finanční odměnou nebo vydíráním k tomu, aby si v bance založili účet, na který pachatel následně převede peníze. Ty jsou posléze směněny za kryptoměnu a odeslány na adresu peněženky ovládané pachatelem.

Pokud se pachatel rozhodne vyhnout směně prostřednictvím bankovního účtu, nabízí se několik alternativních metod. Jednou z možností je založení vlastní směnárny, která může sloužit jako prostředek legalizace výnosů z trestné činnosti – ať už krátkodobě, nebo jako dlouhodobě fungující podnik. Historickým příkladem je směnárna Liberty Reserve (podrobněji viz kapitola 5.2), která umožňovala legalizaci nezákonných výnosů po dobu sedmi let, než byla její činnost ukončena. Dalším příkladem je případ Silk Road, jenž ilustruje jiný přístup. Obchodník Robert Faiella nakupoval bitcoiny ve velkém množství a následně je prodával zákazníkům bez požadavku na jejich identifikaci. Tito zákazníci poté bitcoiny využívali k nákupům na anonymním internetovém tržišti Silk Road (blíže viz kapitola 5.1). Tento postup byl nejen diskrétní, ale zároveň relativně jednoduchý, což z něj činilo atraktivní metodu pro anonymní transakce.

Další variantou nákupu kryptoměn, konkrétně bitcoinu, je využití specializovaných automatů, tzv. bitcoinmatů. Tyto zařízení umožňují hotovostní transakce, přičemž maximální limit jednorázového vkladu činí 25 000 Kč. Pokud uživatel disponuje bitcoinovou peněženkou s QR kódem, naskenuje jej do bitcoinmatu, čímž vloží adresu své peněženky. Následně vloží požadovanou částku v hotovosti, za kterou mu budou připsány bitcoiny. V případě, že uživatel peněženku nemá, může si ji vytvořit přímo na bitcoinmatu. Přístroj v takovém případě vygeneruje a vytiskne papírovou bitcoinovou peněženku s QR kódem, který uživatel následně naskenuje a pokračuje ve standardním procesu. Tato nově vytvořená bitcoinová peněženka může být rovněž zaslána na e-mailovou adresu uživatele. Přístup k informacím o peněžence je zabezpečen heslem, které je uživateli zobrazeno při zadávání e-mailové adresy a umožňuje mu přístup k uloženým údajům. Mezi hlavní nevýhody této metody patří relativně nízký počet dostupných bitcoinmatů a omezená maximální částka, kterou lze jednorázově směnit. Ke květnu 2020 bylo celosvětově v provozu přibližně 7040 bitcoinmatů. Na území České

republiky je k lednu 2025 evidováno celkem 95 zmiňovaných bitcoinmatů, avšak jejich počet se vzhledem k jejich popularitě neustále zvyšuje.⁴⁷

Obrázek č. 3 Přehledová mapa bitcoinmatů na území města Prahy⁴⁸



5.1.2 Obchodní operace zahrnující kryptoměny v kontextu opatření zaměřených na prevenci legalizace výnosů z trestné činnosti

Existuje několik klíčových metod analýzy blockchainových transakcí, jejichž znalost je zásadní pro odhalování nelegálních aktivit. Mezi hlavní faktory usnadňující trasování transakcí patří opakované používání stejné adresy, analýza adresy pro vrácení prostředků a sdružování vstupů před provedením rozsáhlejší transakce. Obvyklým postupem při platbách v bitcoinech je využití jedné adresy, avšak není technicky problémem generovat novou adresu pro každou jednotlivou transakci. V rámci blockchainu, lze poté jednoduše zpětně dohledat veškeré transakce vztahující se ke konkrétní adrese, což umožňuje celá řada specializovaných blockchainových prohlížečů. Další metodou analýzy je zaměření se na tzv. adresu vrácení prostředků. V rámci

⁴⁷ Nákup a prodej prostřednictvím bitcoinmatu - hotovost. WBTCB [online]. [cit. 2025-02-02]. Dostupné z: <https://www.wbtc.com/cz/sluzby/nakup-a-prodej-prostrednictvim-bitcoinmatuhotovost> Bitcoin ATM Industry Statistics / Charts [online]. [cit. 2025-02-02]. Dostupné z: <https://coinatmradar.com/charts/FILLNER>, Karel

⁴⁸ Bitcoinové bankomaty v Praze, Česká republika. Online. <https://coinatmradar.com>. 2025. Dostupné z: <https://coinatmradar.com/city/129/bitcoin-atm-prague/>. [cit. 2025-02-09]

bitcoinových transakcí dochází k odeslání celého zůstatku dostupného na dané adrese, přičemž výstupy se rozdělí mezi částku určenou příjemci a zbytek, který se vrací zpět původnímu vlastníkov. Pokud například odesílatel z adresy s jedním bitcoinem provede platbu ve výši 0,006 bitcoinu, celý zůstatek je v rámci transakce odeslán a systém rozdělí výstupy na částku určenou příjemci (0,006 bitcoinu) a vrácený zůstatek (0,994 bitcoinu). Při analýze transakcí lze tedy předpokládat, že jeden z výstupů patří zpět odesílateli, čímž lze určit vzory chování uživatele. Třetí metodou sledování transakcí je analýza sdružování prostředků před provedením větší platby. Pokud uživatel nemá dostatečné množství kryptoměny na jedné adrese, je nucen seskupit prostředky z několika jiných adres. Tento postup signalizuje, že pokud transakce obsahuje více vstupů, pravděpodobně všechny patří stejnému odesílateli. Tato technika umožňuje efektivněji sledovat pohyb finančních prostředků a usnadňuje identifikaci subjektů zapojených do podezřelých transakcí.⁴⁹

Pro pachatele představuje značnou výhodu skutečnost, že transakční poplatky v rámci kryptoměnových sítí jsou velmi nízké. Rovněž disponuje možností vytvoření neomezeného počtu peněženkových adres, mezi nimiž může finanční prostředky opakovaně převádět, čímž vytváří složitou síť transakcí, která je obtížně sledovatelná. Kromě přímého vlastnictví kryptoměnových adres může pachatel využít služeb rozsáhlých kryptoměnových burz, které umožňují směnu různých digitálních měn. Vzhledem k tomu, že tyto burzy zpracovávají obrovské množství transakcí na denní bázi, významně se tím snižuje pravděpodobnost identifikace skutečného vlastníka finančních prostředků. Dalším faktorem, jenž přispívá k zachování anonymity pachatelů, je skutečnost, že internetové burzy a směnárny obchodující s kryptoměnami nejsou v České republice zařazeny mezi tzv. povinné osoby ve smyslu zákona č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu. V důsledku toho se na ně nevztahují povinnosti týkající se identifikace klientů ani další regulační opatření stanovená tímto zákonem, což zvyšuje míru anonymity uživatelů využívajících tyto služby.

Kromě již uvedených metod existují specializované nástroje, které umožňují zastřít původ bitcoinů a tím zvýšit anonymitu transakcí. Mezi nejčastěji používané patří tzv. mixéry (coin mixers) a tumblery (coin tumblers). Při využívání těchto služeb je zásadní, aby uživatel nepoužíval stejnou adresu peněženky pro odeslání i přijetí

⁴⁹ JEKIELEK, M. *Advokát radí: Bitcoin a právo*. In: OnBusiness: Ekonomika, podnikání, investice [online]. [cit. 2025-02-05]. Dostupné z: <http://onbusiness.cz/advokat-radi-bitcoin-a-pravo2229>

kryptoměny, ale aby byly jednotlivé adresy odlišné. Mixéry fungují na principu slučování bitcoinů pocházejících z různých adres. Uživatel odešle bitcoiny na centrální adresu mixéru, kde dojde k jejich smíchání s dalšími prostředky, často pocházejícími přímo z rezerv mixéru. Následně jsou smíšené prostředky zaslány zpět uživateli, čímž vzniká složitá síť transakcí, která je prakticky nepropojitelná s původní adresou a velmi obtížně dohledatelná. Služby coin tumblers fungují na podobném principu, avšak kromě míchání kryptoměn mezi různými peněženkami provádějí dodatečné kroky pro zvýšení anonymity. Tumbler transakce rozkládá na menší částky, odesílá je ke kontrole a simuluje další převody, čímž vytváří dojem přirozeného pohybu mincí v blockchainu. Výsledkem je, že bitcoiny vrácené uživateli prošly řadou transakcí, byly několikrát sloučeny a opět odděleny, což zásadně komplikuje jejich zpětné trasování. Vyhledání těchto anonymizačních služeb je poměrně snadné – při zadání příslušného dotazu do vyhledávače Google se zobrazí řada dostupných platform nabízejících anonymizaci bitcoinových transakcí. Většina těchto služeb se prezentuje jako nástroje pro ochranu soukromí uživatelů, avšak vzhledem k jejich povaze bývají rovněž využívány k legalizaci výnosů z trestné činnosti a jiným nelegálním účelům.⁵⁰

Některé kryptoměnové peněženky integrují anonymizační funkce přímo do svého systému a automaticky poskytují vyšší úroveň soukromí. Příkladem je Hidden Wallet, která uživatelům zajišťuje zvýšenou anonymitu kombinací tumblerů, mixérů a zároveň provozem v rámci sítě Tor. Podle oficiálního vyjádření Hidden Wallet nepodléhá žádné státní regulaci a neuchovává informace o svých uživateli. Díky využití sítě Tor je navíc technicky nemožné identifikovat jednotlivé uživatele na základě jejich IP adresy. Tvůrci této peněženky deklarují, že spojení bitcoinu a sítě Tor představuje optimální kombinaci, neboť propojuje nejpokročilejší digitální měnu s vysoce efektivní šifrovací technologií.⁵¹

Jedním z anonymizačních nástrojů určených k obfuskování původu bitcoinů je služba CleanCoin, která umožňuje jejich „očistění“ prostřednictvím výměny za jiné mince pocházející z široké škály nezávislých zdrojů. CleanCoin disponuje rozsáhlou zásobou bitcoinů získaných z tisíců různých transakcí a peněžekových adres. Při využití této služby jsou uživatelem odeslané bitcoiny nahrazeny jinými, čímž dochází k narušení přímého propojení mezi původním a novým vlastnictvím. Tento proces výrazně

⁵⁰ GORALE, A. *How to Launder Stolen Bitcoins*. In: CCN: Bitcoin, Blockchain, FinTech, & Cryptocurrency News [online]. [cit. 2025-02-09]. Dostupné z: <https://www.cryptocoinsnews.com/laundry-stolen-bitcoins/>

⁵¹ Hidden Wallet | Tor Anonymous Hidden Bitcoin Wallet [online]. [cit. 2025-02-10]. Dostupné z: <http://nql7pv7k32nnqor2.onion/>

komplikuje jakýkoli pokus o zpětné trasování transakcí a identifikaci uživatele. Jakmile je cílová adresa zadána a potvrzena, systém automaticky vybere vhodný blok bitcoinů k převodu na příjemce. Celý proces je řízen algoritmicky a běžně trvá přibližně jednu hodinu. Pokud není možné transakci provést zcela automatizovaně, dochází k manuálnímu zpracování, které může v některých případech prodloužit dobu realizace až na 24 hodin.⁵²

Některé anonymizační služby lze dohledat prostřednictvím běžných vyhledávačů, zatímco jiné jsou dostupné pouze skrze specializované softwarové systémy, jejichž principy budou podrobněji vysvětleny v následujících kapitolách. Služba Washbit je přístupná oběma způsoby – pro uživatele běžného internetu je dostupná na adrese <https://washbit.org>, zatímco v síti Tor je provozována na adrese washbitcom2qv6wa.onion. Washbit funguje na principu rozsáhlé sítě peněženek, mezi nimiž neustále probíhají drobné transakce. Tato síť se skládá z několika nezávislých skupin peněženek, které spolu nejsou propojeny. Při využití služby uživatel nejprve odešle své bitcoiny na adresu Washbitu, kde jsou následně převedeny do jednoho ze samostatných souborů peněženek. Po dokončení anonymizačního procesu jsou uživateli zpět vyplaceny prostředky pocházející z jiné skupiny peněženek, čímž je eliminována možnost přímého propojení mezi původní a novou transakcí. Služba deklaruje, že disponuje dostatečným množstvím bitcoinů pro efektivní míchání, konkrétně více než 1 000 BTC. Maximální doporučená hodnota jedné transakce činí 200 BTC, zatímco minimální částka pro použití služby je stanovena na 0,01 BTC. Pro zajištění vyšší míry anonymity je doporučeno, aby uživatel zadal minimálně pět různých cílových adres, což umožňuje rozložení transakce na menší částky a tím snižuje možnost jejího zpětného vysledování. Za využití těchto služeb je účtován poplatek, který se aktuálně pohybuje v rozmezí 0,9 % až 1 % z celkové transakce. Provozovatelé Washbitu se zaměřují na bezpečnost a aktivně se brání jak vzdáleným, tak lokálním kybernetickým útokům. Zároveň motivují uživatele k identifikaci možných zranitelností systému – pokud je uživatelem odhalena bezpečnostní chyba a následně nahlášena správci, poskytovatel vyplácí menší finanční odměnu. V zájmu ochrany soukromí Washbit neuchovává žádné informace o uživateli a zadané peněženkové adresy jsou automaticky odstraněny ze systému po 24 hodinách.⁵³

⁵² CleanCoin - Low-Fee Bitcoin Mixing/Tumbling/Laundry Service [online]. [cit. 2025-02-10]. Dostupné z: <http://cleancondgja34b.onion/>

⁵³ WashBit [online]. [cit. 2025-02-10]. Dostupné z: <https://washbit.org>

Kromě výše uvedených služeb mají pachatelé k dispozici i další metody, jak skrýt svou identitu v online prostředí. Každý uživatel internetu za sebou zanechává digitální stopu, která zahrnuje IP adresu, informace o délce návštěvy webových stránek, poskytovatele internetového připojení a další metadata. K eliminaci těchto identifikačních prvků existuje řada anonymizačních a pseudoanonymizačních nástrojů, jejichž účelem je minimalizovat sledovatelnost uživatele. Nicméně žádný z těchto nástrojů neposkytuje absolutní anonymitu. Pseudoanonymita spočívá v tom, že veškeré online aktivity uživatele lze teoreticky dohledat, pokud se pohybuje pod určitým pseudonymem. Avšak tento pseudonym nelze snadno přímo propojit s konkrétní fyzickou osobou, což poskytuje určitou míru ochrany identity. Níže jsou podrobněji popsány tři různé anonymizační a pseudoanonymizační systémy, které jsou často využívány k zajištění vyššího stupně soukromí v online prostředí – Tor, I2P a Vuvuzela.

Tor (The Onion Router) je softwarový systém určený pro anonymní komunikaci, který využívá technologii tzv. onion routingu (doslova „cibulového šifrování“). Tento princip byl vyvinut v polovině 90. let ve Spojených státech jako mechanismus pro zajištění soukromí při přenosu informací. Onion routing funguje na principu vrstveného šifrování, kde jsou jednotlivé zprávy postupně obalovány v několika vrstvách šifrování, podobně jako struktura cibule. Při přenosu mezi uzly sítě je každá zpráva vždy dešifrována pouze jedním klíčem na konkrétním uzlu, než je odeslána dál. Výsledkem je, že žádný jednotlivý uzel nezná celý komunikační řetězec – vidí pouze předchozí a následující bod, nikoli konečného příjemce ani odesílatele. Systém Tor byl oficiálně spuštěn v roce 2002 s cílem poskytnout uživatelům vyšší úroveň anonymity při používání internetu. Původně nesl název The Onion Routing, z něhož vznikla současná zkratka Tor. Síť je provozována dobrovolníky, kteří spravují servery a umožňují tok dat mezi uživateli. Tor se stal důležitým nástrojem pro ochranu soukromí nejen jednotlivců, ale i organizací, především v případech, kdy čelí represím kvůli svému politickému přesvědčení nebo potřebují zveřejňovat citlivé informace, které by mohly být v běžném online prostředí cenzurovány. Pokud je systém používán správně, efektivně znemožňuje sledování uživatelů a minimalizuje jejich digitální stopu. Tor rovněž nachází využití v oblasti ochrany obětí trestných činů, zejména těch souvisejících s porušováním osobní integrity a mravnostní kriminalitou, jelikož umožňuje bezpečnou a anonymní komunikaci. Pro přístup k síti Tor je nezbytné využití specializovaného softwaru. Jeho konfigurace může být pro běžného uživatele poměrně složitá, proto byl vyvinut Tor Browser, což je

upravený webový prohlížeč s přednastaveným přístupem k síti Tor, který lze snadno nainstalovat a spustit bez pokročilého technického nastavení.⁵⁴

I2P (The Invisible Internet Project) je pseudoanonymizační síť, která byla spuštěna v roce 2003 a slouží jako prostředek pro anonymní komunikaci a přenos dat. Síť je tvořena soustavou směrovačů, které disponují množstvím příchozích a odchozích tras, tzv. **tunelů**. Každý jednotlivý směrovač je identifikován kryptografickým klíčem, jenž se v pravidelných intervalech mění, čímž je zajištěna vyšší úroveň soukromí. Komunikace v rámci sítě I2P probíhá prostřednictvím směrovačů a tunelů, přičemž uživatel využívá vlastní směrovač pro odesílání i příjem dat. Zprávy jsou odesílány skrze odchozí tunely odesílatele, zatímco příjem probíhá prostřednictvím jednoho z příchozích tunelů příjemce. Směrovač při doručování zprávy využívá decentralizovanou databázi, ve které vyhledává optimální trasu pro přenos dat. Tato databáze se pravidelně aktualizuje, aby reflektovala změny v síti a zajistila plynulost komunikace. I2P poskytuje podobné možnosti využití jako klasický Internet – umožňuje uživatelům vytvářet webové stránky, sdílet soubory nebo bezpečně komunikovat. Přímý přístup k veřejnému Internetu však není automaticky zajištěn. Pro propojení s běžnými webovými stránkami a dalšími internetovými službami musí uživatelé využívat přeposílací proxy servery (tzv. outproxy), které umožňují směrování provozu mezi anonymní sítí I2P a standardním Internetem.⁵⁵

Systém **Vuvuzela** byl poprvé představen na konci června 2015 v rámci symposia Privacy Enhancing Technologies konaného ve Filadelfii. Tento projekt vyvinul výzkumný tým v Massachusetts s cílem eliminovat možnost sledování uživatelů prostřednictvím metadat. Vuvuzela k dosažení tohoto cíle využívá techniku vytváření šumu, čímž znemožňuje třetím stranám analyzovat komunikaci na základě síťového provozu. V současnosti je systém určen výhradně pro odesílání zpráv a neumožňuje přímou interakci mezi uživateli. Místo toho využívá e-mailové schránky a řetězec serverů ke zprostředkování komunikace. Dva uživatelé si nejprve zvolí sdílenou e-mailovou schránku, přes kterou budou vzájemně komunikovat. Odeslaná zpráva nejprve projde prvním serverem, který k ní přidá další vrstvu šifrování a uloží ji do určené e-mailové schránky. Následně je zpráva doručována příjemci prostřednictvím dalšího serveru. Pro

⁵⁴ Tor Project: Overview. *Tor Project: Anonymity Online* [online]. [cit. 2025-02-10]. Dostupné z: <https://www.torproject.org/about/overview.html.en>

⁵⁵ A Gentle Introduction to How I2P Works. *I2P Anonymous Network* [online]. [cit. 2025-02-10]. Dostupné z: <https://geti2p.net/en/docs/how/intro>

každou novou zprávu uživatelé vybírají novou schránku, což zvyšuje bezpečnost komunikace. Aby se minimalizovala možnost sledování pomocí analýzy síťového provozu, dochází v rámci systému Vuvuzela k neustálému promíchávání zpráv, čímž se mění jejich pořadí. Kromě skutečných zpráv servery v pravidelných intervalech generují a odesílají fiktivní zprávy do náhodných schránek, a to i v případě, že uživatel není aktuálně aktivní. Tento mechanismus znemožňuje potenciálním pozorovatelům provádět analýzu objemu přenesených dat a získávat statistické informace o frekvenci komunikace konkrétního uživatele. Testování systému proběhlo na virtuálních serverech Amazon EC2, přičemž průměrná doba doručení zprávy činila přibližně 44 sekund. Ačkoli je Vuvuzela v současné fázi určena pouze pro odesílání textových zpráv, lze předpokládat, že se její funkcionality v budoucnu rozšíří i na další formy zabezpečené komunikace.⁵⁶

⁵⁶ Vuvuzela: *Scalable Private Messaging Resistant to Traffic Analysis*. In: *PoPETs/PETS* [online]. [cit. 2025-02-27]. Dostupné z: <https://petsymposium.org/2015/papers/vandenhooff-vuvuzela-hotpets2015.pdf>

6 Případy zneužití kryptoměny zaznamenané v minulosti

Jedním z prvních a patrně nejznámějších příkladů je platforma Silk Road, která se specializovala na nelegální obchodování prostřednictvím darknetu. Na obdobném principu přitom funguje značná část online tržišť nabízejících nezákonné komodity. Liberty Reserve, jež vyvinula vlastní virtuální měnu, dokázala až do svého odhalení legalizovat rozsáhlé finanční částky. Dále lze zmínit službu Coin.mx, která ilustruje značnou míru vynalézavosti pachatelů působících v této oblasti. Mezi nejnovější případy spojené s legalizací výnosů z trestné činnosti patří zatčení deseti osob v Nizozemsku. Tyto osoby jsou podezřelé z toho, že zprostředkovaly převod 15–20 milionů eur pocházejících z online obchodů s drogami. Údajně pomáhaly drogovým dealerům směňovat bitcoiny, přijaté od zákazníků, přičemž na sebe upozornily pravidelnými vklady vysokých hotovostních částek na bankovní účty a jejich následnými rychlými výběry. V rámci vyšetřování, probíhajícího ve spolupráci s úřady ve Spojených státech, Austrálii, Litvě a Maroku, byly zabaveny luxusní vozy, finanční hotovost, zablokovány bankovní účty a zajištěno blíže nespecifikované množství bitcoinů. Probíhající šetření by mělo objasnit přesný mechanismus, jímž pachatelé legalizaci nelegálních výnosů prováděli.⁵⁷

6.1.1 Silk Road

Silk Road představovala internetové tržiště typické pro nelegální obchod s omamnými látkami. Tato platforma, začleněná do tzv. dark webu, byla provozována prostřednictvím anonymizační služby Tor, což uživatelům umožňovalo minimalizovat riziko odhalení při prohlížení a obchodování. Provoz Silk Road byl zahájen v únoru 2011, přičemž zpočátku systém nabízel omezené množství prodejních účtů dostupných pouze formou aukce. Později byl zaveden fixní poplatek za založení nového účtu. Již v březnu 2013 bylo na platformě evidováno 10 000 produktů, z nichž přibližně 70 % tvořily drogy.⁵⁸ V říjnu 2014 se na stránkách nacházelo 13 756 nabídek na drogy rozdělených do kategorií, jako jsou stimulanty, léky na předpis, prekursor, opiáty, extáze či konopí. Kromě nelegálního zboží byly však dostupné i běžné předměty, například oblečení, umění, knihy nebo cigarety. K prvnímu zatčení spojenému se Silk Road došlo v únoru

⁵⁷ STERLING, T. *Dutch arrest 10 men suspected of using Bitcoin to launder money*. In: Business & Financial News, Breaking US & International News | Reuters.com [online]. [cit. 2025-02-01]. Dostupné z: <https://www.reuters.com/article/us-netherlands-crime-bitcoinidUSKCN0UY0V8>

⁵⁸ KOLOUCH, J. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-8-088168-15-7, str. 49-50.

2013, kdy australský obchodník zaslal drogy odhalené úřady, které následným vyšetřováním zjistily jeho napojení na Silk Road. V říjnu téhož roku Federální úřad pro vyšetřování (FBI) tržiště uzavřel a zatkl jeho zakladatele Rosse Williama Ulbrichta. Ten byl obviněn mimo jiné z praní špinavých peněz, pašování drog a spolčení za účelem narušení počítačového zabezpečení. Nakonec byl odsouzen k doživotnímu vězení bez možnosti podmíněčného propuštění. Kromě Ulbrichta bylo v souvislosti s fungováním Silk Road obviněno a odsouzeno několik dalších osob. Australan Peter Nash se přiznal k obchodování s drogami a k praní špinavých peněz. Dále byli zatčeni Charlie Shrem, výkonný ředitel BitInstant, a Robert Faiella. Shrem se dostal do hledáčku vyšetřovatelů kvůli spolupráci s Faiellou, který pořídil velké množství bitcoinů a prodával je uživatelům Silk Road, čímž jim umožňoval nelegální transakce. V kontextu americké legislativy mají přitom finanční instituce povinnost hlásit úřadům jakoukoli podezřelou aktivitu, jež by mohla signalizovat praní špinavých peněz.⁵⁹

Nicolas Christin z Carnegie Mellon University v Pensylvánii uskutečnil anonymizovanou analýzu Silk Road, přičemž sbíral data po dobu osmi měsíců.⁶⁰ V jeho studii byly zahrnuty i každodenní tržní transakce v intervalu 3. února až 24. července 2012, díky čemuž získal komplexní přehled o prodávaném sortimentu, příjmech prodejců i ziscích provozovatelů. Analýza prokázala, že trh se využíval převážně k obchodování s kontrolovanými látkami a narkotiky. Většina nabídek byla aktivní po dobu kratší než tři týdny. Podle Christinových zjištění se celkové měsíční příjmy prodejců pohybovaly nad hranicí 1,2 milionu dolarů, zatímco samotní provozovatelé tržiště vydělávali přibližně 92000 dolarů měsíčně.

Silk Road nefungoval jako klasický internetový obchod, nýbrž poskytoval infrastrukturu pro vzájemné transakce mezi prodávajícími a nakupujícími. Platforma zároveň zabezpečovala online převody plateb. Prodejci na Silk Road museli dodržovat přísná omezení týkající se nabízeného sortimentu. Z interních pravidel například vyplývalo, že je zakázáno inzerovat zboží či služby s cílem poškodit nebo podvést zákazníka, jako jsou kradené předměty nebo data, padělané peníze, kreditní karty, vražedné zakázky či jakékoli druhy zbraní. Rovněž bylo explicitně zapovězeno nabízet cokoliv spojeného s pedofilií. Zbraně a munice se na Silk Road směly prodávat pouze do

⁵⁹ Silk Road (marketplace). Wikipedia, the free encyclopedia [online]. [cit. 2025-02-02]. Dostupné z: [https://en.wikipedia.org/wiki/Silk_Road_\(marketplace\)#cite_note-nytlife-14](https://en.wikipedia.org/wiki/Silk_Road_(marketplace)#cite_note-nytlife-14)

⁶⁰ CHRISTIN, N. *Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace* [online]. [cit. 2025-02-02]. Dostupné z: <https://www.andrew.cmu.edu/user/nicolasc/publications/Christin-WWW13.pdf>

4. března 2012, poté byly přesunuty na sesterský portál The Armory, ukončený v srpnu 2012 z důvodu nedostatečného zájmu. Nabídka se dělila na veřejné a tajné položky; Silk Road navíc podporoval samostatné stránky přístupné jen speciálním uživatelům s příslušným URL odkazem.

Proces obchodu lze demonstrovat na příkladu: Bob (B) si zvolil prodejce Sarah (S) a Tor zajišťoval anonymitu komunikace, zatímco Silk Road, vyžadující anonymní platební systém, pracoval výhradně s bitcoiny. Bob tak nejprve získal bitcoiny ve směnárně a umístil platbu do úschovy na Silk Road, což operátorům umožnilo vypočítat provizi a řešit případné neshody. Pokud se některý účastník trhu provinil proti stanoveným pravidlům, následovalo zablokování účtu. Sarah k doručení objednaného zboží potřebovala Bobovu fyzickou adresu, avšak pro zachování anonymity se nakupujícím doporučovalo uvádět jinou než skutečnou adresu. Po označení balíčku za odeslaný byla Bobova adresa z databáze odstraněna. Jakmile Bob zásilku převzal, schválil platbu a mohl poskytnout zpětnou vazbu Sarah. K ještě větší anonymizaci plateb Silk Road využíval prostředníky (P1, P2), kteří stáli mezi Bobem a Sarah (B – P1 – P2 – S). Vysokou spolehlivost prodejců potvrzuje statistika, podle níž 97,8 % získalo hodnocení čtyř až pěti bodů z pěti.

Celkově Silk Road nabízel kolem 220 kategorií zboží, přičemž nejvíce inzerátů se týkalo konopných produktů, následovaly další narkotika a léky na předpis. Podstatná část položek byla dostupná kratší dobu než tři týdny, přičemž více než čtvrtina z nich zmizela během pouhých tří dnů. Lze předpokládat buď skutečnou krátkodobost nabídek, nebo takzvaný "relisting", kdy prodejci stejný produkt znovu zveřejnili pod odlišným názvem, aby se objevoval v jiných částech tržiště.

Christin se zaměřil na geografické rozmístění jednotlivých položek nabízených na tržišti a zjistil, že hlavními zdroji nabídky byly Spojené státy americké (43,83 %), následované kategorií s neurčeným původem (16,29 %), dále pak Velká Británie, Nizozemsko a Kanada. Přestože by se mohlo zdát riskantní distribuovat zboží mezinárodně z důvodu hraničních kontrol, praxe ukázala, že prodávající s dobrou reputací často vyžadují platbu předem nebo využívají úschovu na Silk Road. Rovněž je obvyklé, že se prodávají menší objemy (například několik gramů marihuany), což komplikuje identifikaci odesílatele. Navíc mnozí prodejci volí profesionální způsoby balení a někteří dokonce nabízejí částečné odškodnění v případě zadržení zásilky. Z hlediska objemu prodeje v bitcoinech došlo nejprve k nárůstu z přibližně 6 000 BTC za den na 9 500 BTC

za den, přičemž následně poklesl na 7 000 BTC za den (kolem ledna 2012). Ve finančním vyjádření přesahovala průměrná měsíční hodnota prodeje 1,22 milionu dolarů, což ročně představovalo zhruba 15 milionů dolarů. Provozovatelé tržiště vybírali provizi z každé transakce; původní sazba činila 6,23 %, avšak v lednu 2012 došlo k zavedení odstupňovaného poplatkového systému po vzoru eBay. Provize rostla od zhruba 2 200 dolarů denně v březnu 2012 k přibližně 4 000 dolarům v červenci 2012. Přestože v důsledku posilování bitcoinu mohlo dojít k poklesu jeho objemů, v dolarovém vyjádření se celková hodnota transakcí, a tím i provize pro provozovatele, zvýšila. Christin odhadl, že měsíčně mohli provozovatelé dosáhnout příjmů přibližně 92 000 dolarů, tedy kolem 1,1 milionu dolarů ročně.⁶¹

Senátor Spojených států Charles Schumer označil Silk Road za „nestydatější než cokoli jiného v dobách klidu“⁶², což symbolizuje obecnou obavu a nejistotu, jež panuje mezi politickými představiteli v souvislosti s anonymními internetovými platformami. Nástup uživatelsky přívětivých anonymizačních nástrojů, například Tor Browser Bundle, významně zjednodušil přístup k anonymnímu prohlížení internetu i pro jedince s omezenými technickými dovednostmi. Provoz anonymních online tržišť však naráží na legislativní předpisy požadující identifikaci obchodníků i nakupujících, a proto se tyto trhy často specializují na nelegální sortiment, jako je pornografie, zbraně či omamné látky. Mezi jejich populární představitele patří AlphaBay, Dream Market nebo Valhalla. Analýza Silk Road přináší vhled do fungování podobných černých trhů, kterých se na internetu vyskytuje značné množství. V lednu 2015 se objevila nová verze pod názvem Silk Road Reloaded, jež se v několika ohledech zásadně odlišuje od svých předchůdců. Především neběží v síti Tor, ale na méně rozšířené anonymní síti nazývané Invisible Internet Project (I2P), kterou od roku 2003 vyvíjí anonymní skupina programátorů. Zatímco původní Silk Road umožňoval platby pouze v bitcoinech, Silk Road Reloaded rozšířil platební možnosti na několik různých kryptoměn, přičemž výsledná transakce je převedena na bitcoiny podle aktuálního směnného kurzu.

⁶¹ CHRISTIN, N. *Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace* [online]. [cit. 2025-02-03]. Dostupné z: <https://www.andrew.cmu.edu/user/nicolasc/publications/Christin-WWW13.pdf>

⁶² CHRISTIN, N. *Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace* [online]. [cit. 2025-02-03]. Dostupné z: <https://www.andrew.cmu.edu/user/nicolasc/publications/Christin-WWW13.pdf>

6.1.2 Liberty Reserve

Společnost Liberty Reserve, fungující jako banka i online směnárna, po dobu sedmi let napomáhala legalizaci přibližně šesti miliard dolarů pocházejících z trestné činnosti. Během své existence uskutečnila 55 milionů transakcí, do nichž se zapojily miliony uživatelů po celém světě. Liberty Reserve se zařadila mezi přední finanční nástroje využívané pachateli pro shromažďování, distribuci, ukládání a následnou legalizaci nelegálních zisků, zejména v souvislosti s investičními podvody, paděláním kreditních karet, krádežemi identity či neoprávněným přístupem do informačních systémů. Podle vyjádření advokáta Preeta Bharary se jednalo o nejrozsáhlejší případ internetového praní špinavých peněz v dějinách. Analogicky k revoluční funkci platební služby PayPal, která umožnila běžným spotřebitelům pohodlné nákupy online, se Liberty Reserve pokoušela nabídnout stejný komfort pachatelům trestné činnosti. Tato směnárna zprostředkovávala uživatelům anonymní a obtížně vystopovatelné nelegální finanční transakce, jež přilákaly podvodníky, hackery i nelegální obchodníky. Služby Liberty Reserve se ukázaly být klíčové v celé řadě případů kyberkriminality, včetně kauzy skupiny osmi osob z New Yorku, které prostřednictvím tohoto systému vypraly 45 milionů dolarů získaných z bankomatů v sedmadvaceti státech.⁶³

Liberty Reserve, jež se sama prezentovala jako „největší internetový platební procesor a systém pro převody peněz“, založil Arthur Budovsky roku 2006 v Kostarice, kam emigroval, aby se vyhnul vlivu a dohledu americké jurisdikce a současně rozšířil svou podnikatelskou činnost. K zaslání finanční částky prostřednictvím této služby postačovalo, aby uživatel uvedl jméno, e-mailovou adresu a datum narození – bez dalšího ověřování, což umožňovalo užívání fiktivních či anonymních identit. Směnárna transakce v hotovosti neprováděla sama, nýbrž prostřednictvím třetích stran, zejména směnáren sídlících v zemích jako Malajsie, Rusko, Nigérie či Vietnam. Vložené prostředky byly následně konvertovány na Liberty Reserve dolary nebo Liberty Reserve eura, jejichž hodnota byla navázána na kurz amerického dolaru, eura anebo zlata a uložena na uživatelském účtu. Prostřednictvím této virtuální měny bylo možné nakupovat narkotika, kradená data z kreditních karet i zbraně jednoduchým převodem mezi jednotlivými účty. Platby probíhaly okamžitě a nemohly být stornovány. Příjemci mohli následně navštívit neregulovanou směnárnou, kde si své Liberty Reserve opět směnili za dolary, přičemž výše

⁶³ Online Currency Exchange Accused of Laundering \$6 Billion. The New York Times - Breaking News, World News & Multimedia [online]. [cit. 2025-02-03]. Dostupné z: <https://www.nytimes.com/2013/05/29/nyregion/liberty-reserve-operators-accused-of-money-laundering.html>

transakcí nebyla nijak omezena. Směnárna dosahovala zisku účtováním 1% poplatku z každého převodu a nabízela rovněž internetový nákupní košík a další obchodní nástroje. V květnu 2013 došlo ze strany vlády Spojených států k ukončení provozu, přičemž v té době existovalo více než pět milionů uživatelských účtů, z toho přes 600 000 spojených s uživateli z USA. Budovsky, společně s dalšími šesti osobami, byl následně obviněn z napomáhání praní špinavých peněz a provozování finanční instituce bez řádné licence. V lednu 2016 se přiznal ke spoluúčasti na legalizaci více než 250 milionů dolarů.⁶⁴

6.1.3 Coin.mx

V červenci 2015 byli na Floridě zadrženi Anthony Murgio a Jurij Lebeděv, považovaní za hlavní provozovatele ilegální směnárně Coin.mx. Oba byli obviněni z legalizace výnosů z trestné činnosti, provozování burzy bez řádné licence a neoznámení podezřelých transakcí. V následném řízení byla stíhána i další skupina osob kvůli obviněním z praní špinavých peněz a kybernetických útoků na finanční instituce v USA. Coin.mx, jejíž doménu Murgio zaregistroval v říjnu 2013, směnila zhruba 1,8 milionu dolarů na bitcoiny od doby vzniku do července 2015, přičemž finanční prostředky byly převáděny i na účty mimo území Spojených států (Hongkong, Kypr či východoevropské země). Ke skrytí ilegálního charakteru činnosti provozovatelé založili fiktivní Klub sběratelů, kde mělo formálně docházet k výměně sběratelských artefaktů za peníze. Podle obžaloby Murgio a Lebeděv prováděli směny s vědomím, že se jedná o nezákonné zisky, a navíc zprostředkovávali prodej bitcoinů napadeným institucím. Ty byly nuceny zaplatit útočníkům v kryptoměně, přičemž FBI konstatuje, že takto Murgio společně s dalšími obviněnými aktivně napomáhali příjemcům těchto plateb k získání zisků z trestné činnosti. V rozporu s federálními předpisy proti praní špinavých peněz nebyla žádná z podezřelých transakcí řádně oznámena. Soudní projednávání případu se mělo uskutečnit v říjnu 2016.⁶⁵

⁶⁴ The New York Times *Online Currency Exchange Accused of Laundering \$6 Billion* [online]. [cit. 2025-02-03]. Dostupné z: <https://www.nytimes.com/2013/05/29/nyregion/liberty-reserve-operators-accused-of-money-laundering.html>

⁶⁵ FILLNER, K. *Coin.mx končí - FBI zatkla dva údajné provozovatele ilegální bitcoinové směnárně*. In: *Budoucnost peněz: bitcoinové zprávy | finanční a technologické inovace* [online]. [cit. 2025-02-03]. Dostupné z: <https://cointelegraph.cz/news/coinmx-konci-fbi-zatkla-dva-udajneprovozovatele-ilegalni-bitcoinove-smenarny>

7 Právní regulace kryptoměn⁶⁶

7.1.1 Právní regulace kryptoměn ve světě

Právní regulace kryptoměn je celosvětově heterogenní a neustále se vyvíjející oblastí. Vzhledem k decentralizované povaze kryptoměn, jejich rostoucí popularitě a potenciálním rizikům spojeným s jejich využitím, se jednotlivé státy snaží implementovat různé formy regulace. Tento článek se zaměří na přístupy k regulaci kryptoměn v různých jurisdikcích, s důrazem na Spojené státy, Evropskou unii a vybrané asijské země.

Každá jurisdikce definuje kryptoměny odlišně, což má důsledky pro jejich zdanění, dohled a možnosti jejich využití v běžných transakcích. Kryptoměny mohou být klasifikovány jako:

- Komodity (např. v USA dle Commodity Futures Trading Commission - CFTC)
- Digitální aktiva (např. v Evropské unii v rámci nařízení MiCA)
- Elektronické peníze (např. v Japonsku podle regulačních pravidel FSA)
- Nelegální platidlo (např. v části zemí, jako je Čína nebo Bangladéš)

7.1.2 Regulace kryptoměn v USA

Spojené státy přistupují k regulaci kryptoměn na federální i státní úrovni. Komise pro cenné papíry a burzy (SEC) klasifikuje některé kryptoměny jako cenné papíry, pokud splňují tzv. Howeyho test. Komise pro obchod s komoditami (CFTC) považuje bitcoin a ether za komodity a reguluje derivátové trhy založené na těchto aktivech. Kromě toho FinCEN (Financial Crimes Enforcement Network) vyžaduje, aby směnární kryptoměn dodržovaly předpisy proti praní špinavých peněz (AML) a identifikaci klientů (KYC).

⁶⁶ *Fundamentální analýza kryptoměn – regulační vývoj a jeho dopad na kryptoměny*. Online. FXstreet.cz. 2024. Dostupné z: https://www.fxstreet.cz/jakub-matis-fundamentalni-analyza-kryptomen-regulacni-vyvoj-a-jeho-dopad-na-kryptomeny-8-dil.html?utm_source=chatgpt.com. [cit. 2025-02-09].

7.1.3 Právní regulace v Evropské unii

Evropská unie zavedla právní rámec **Markets in Crypto-Assets Regulation (MiCA)**, který vstoupí v platnost v roce 2024. Nařízení MiCA stanovuje pravidla pro:

- Poskytovatele služeb spojených s kryptoměnami (CASP)
- Emitenty stabilních kryptoměn (stablecoinů)
- Transparentnost a dohled nad trhem s kryptoměnami

MiCA usiluje o ochranu investorů a zabránění finanční kriminalitě, avšak jeho dopad na inovace v odvětví zůstává předmětem diskuzí.

7.1.4 Právní regulace v Asii

V Asii se přístupy k regulaci kryptoměn různě liší:

- **Japonsko** uznává bitcoin jako legální platební prostředek a podléhá regulaci ze strany **Financial Services Agency (FSA)**.
- **Čína** přísně zakázala obchodování a těžbu kryptoměn, přičemž podporuje vývoj vlastní digitální měny centrální banky (CBDC).
- **Singapur** aplikuje regulační rámec **Payment Services Act**, který klade důraz na AML/KYC opatření.

7.1.5 Právní regulace kryptoměn v České republice

Právní regulace kryptoměn v České republice je dynamicky se vyvíjející oblastí, která reaguje na změny v evropském právním rámci i globálních finančních trendech. Ačkoli Česká republika zatím nepřijala specifický zákon upravující kryptoměny, subjekty působící v této oblasti podléhají řadě legislativních opatření, zejména v oblasti prevence praní špinavých peněz a ochrany investorů.

7.1.6 Právní status kryptoměn v ČR⁶⁷

Český právní řád v současnosti neuznává kryptoměny jako zákonné platidlo. Nicméně jsou považovány za digitální aktiva a podléhají regulaci v několika oblastech, zejména daňové legislativy, prevence praní špinavých peněz (AML) a obchodního práva.

- **Kryptoměny jako aktiva:** Česká národní banka (ČNB) klasifikuje kryptoměny jako nehmotná aktiva, která nepodléhají dohledu ČNB, pokud nejsou součástí investičních nebo platebních služeb regulovaných evropským právem.
- **Zdanění kryptoměn:** Příjmy z kryptoměn podléhají dani z příjmu fyzických i právnických osob. V případě podnikatelské činnosti se uplatňuje daňová soustava pro podnikatele, včetně DPH v některých případech.
- **Účetní standardy:** Kryptoměny nejsou v českém účetním systému definovány jako měna, ale evidují se jako zásoby nebo nehmotná aktiva.

7.1.7 Regulace v oblasti AML/KYC⁶⁸

V souladu s evropskou směrnicí AMLD5 (Pátá směrnice o boji proti praní špinavých peněz) jsou poskytovatelé služeb spojených s kryptoměnami v České republice považováni za povinné osoby podle zákona č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu. To znamená, že:

- Směnární a poskytovatelé kryptoměnových peněženek musí provádět identifikaci klientů (KYC – Know Your Customer).
- Subjekty poskytující služby spojené s kryptoměnami musí monitorovat podezřelé transakce a hlásit je Finančnímu analytickému úřadu (FAÚ).
- Neidentifikované transakce nad stanovený limit mohou být zablokovány nebo podrobeny dalšímu přezkumu.

⁶⁷ Kořínek, V. *Jak danit kryptoměny v roce 2025* [online]. [cit. 2025-02-02]. Dostupné z: <https://blog.simplecoin.eu/jak-danit-kryptomeny/>

⁶⁸ Clifford Chance *Overview of regulation of cryptocurrencies in the Czech Republic* [online]. [cit. 2025-02-03]. Dostupné z: <https://www.cliffordchance.com/insights/resources/blogs/talking-tech/en/articles/2019/11/overview-of-regulation-of-cryptocurrencies-in-the-czech-republic.html>

7.1.8 Dopad evropské regulace (MiCA) na ČR⁶⁹

Regulace Markets in Crypto-Assets (MiCA), která byla přijata na úrovni Evropské unie a začne platit od roku 2024, bude mít významný dopad i na Českou republiku. MiCA zavádí jednotná pravidla pro:

- Povolení a dohled nad poskytovateli kryptoměnových služeb.
- Ochranu spotřebitelů před vysokou volatilitou digitálních aktiv.
- Transparentnost a podávání zpráv regulačním orgánům.

České úřady budou muset tyto požadavky implementovat a zajistit, aby provozovatelé kryptoměnových služeb splňovali nové regulační standardy.

7.1.9 Výzvy a budoucí vývoj⁷⁰

Ačkoli Česká republika patří mezi státy s relativně liberálním přístupem ke kryptoměnám, stále existují oblasti, které vyžadují jasnější regulaci, zejména:

- **Stabilní právní rámec:** Nedostatek jednotného zákona o kryptoměnách způsobuje právní nejistotu pro investory a podnikatele.
- **Zvýšená regulace:** Přijetí evropské regulace MiCA pravděpodobně povede k větší transparentnosti, ale také ke zpřísnění požadavků na registraci a dozor.
- **Zdanění a účetnictví:** Potřeba jasnějších pravidel pro účetní evidenci a zdanění kryptoměn, včetně mechanismů pro zdanění zisků z obchodování.

⁶⁹ Kinstellar *Digital Finance Act: A new era for crypto-assets in the Czech Republic* [online]. [cit. 2025-02-03]. Dostupné z: <https://www.kinstellar.com/news-and-insights/detail/3213/digital-finance-act-a-new-era-for-crypto-assets-in-the-czech-republic>

⁷⁰ Global Legal Insights *Czech Republic introduces crypto-friendly law* [online]. [cit. 2025-02-03]. Dostupné z: <https://www.globallegalinsights.com/news/czech-republic-introduces-crypto-friendly-law/>

8 Budoucí vývoj

Právní regulace kryptoměn v České republice je součástí širšího procesu harmonizace evropských pravidel v oblasti digitálních aktiv. Přestože zde neexistuje jednotný zákon, české právní prostředí již zahrnuje řadu opatření zaměřených na AML/KYC compliance a daňovou regulaci. V nadcházejících letech lze očekávat další zpřísnění pravidel v návaznosti na přijetí nařízení MiCA, což přinese jak výhody v podobě vyšší ochrany investorů, tak i výzvy v oblasti administrativní zátěže pro subjekty působící na trhu s kryptoměnami.⁷¹

Na globální úrovni se regulace kryptoměn stále vyvíjí, přičemž různé státy volí rozdílné přístupy – od úplné legalizace a integrace kryptoměn do finančního systému (např. Japonsko, Švýcarsko) po striktní zákazy a regulace (např. Čína, Indie). S rostoucím významem digitálních aktiv lze očekávat posilování dohledu a regulací, zejména v oblasti boje proti finanční kriminalitě, daňové správy a ochrany spotřebitelů. Budoucnost kryptoměn tak bude pravděpodobně záviset na schopnosti regulatorních orgánů nalézt rovnováhu mezi podporou inovací a zajištěním stability finančního systému.

8.1.1 Doporučení pro efektivnější prevenci praní špinavých peněz prostřednictvím kryptoměn

Vzhledem k rostoucímu využívání kryptoměn v rámci finanční kriminality je nezbytné dosáhnout právního rámce a zavést efektivní opatření pro odhalování a praní špinavých peněz. Níže uvedená doporučení se zaměřují na klíčové oblasti regulace, technologií a spolupráce mezi institucemi.

8.1.2 Zpřísnění a harmonizace mezinárodní regulace

- **Globální standardizace regulací** – Podporovat širší implementaci doporučení **Financial Action Task Force (FATF)**, zejména **Travel Rule**, která zavádí povinnost sdílení informací o odesílatelích a příjemcích kryptoměnových transakcí.

⁷¹ Forbes *Český trh s kryptoaktivy se dočká regulace. Prezident Pavel podepsal kryptoměnový balíček.* [online] Dostupné z: <https://forbes.cz/cesky-trh-s-kryptoaktivy-se-docka-regulace-prezident-pavel-podepsal-kryptomenovy-balicek/>. [cit. 2025-02-09].

- **Harmonizace regulací mezi státy** – Minimalizovat regulační arbitrage, kdy pachatelé využívají jurisdikce s nízkou úrovní dohledu k praní peněz. Mezinárodní spolupráce mezi regulátory by měla být klíčovým bodem.
- **Licencování a regulace kryptoměnových služeb** – Zavedení povinných licencí pro burzy, směnárny a poskytovatele peněženek, které musí dodržovat AML/KYC požadavky.

8.1.3 Posílení dohledu a AML opatření

- **Povinné KYC (Know Your Customer) procesy** – Zajistit, aby všechny kryptoměnové burzy a poskytovatelé peněženek ověřovali identitu uživatelů a vedli podrobné záznamy o transakcích.⁷²
- **Automatizované systémy hlášení podezřelých transakcí** – Zavést práh pro podezřelé transakce a povinnost jejich automatického hlášení regulačním orgánům.⁷³
- **Blacklistování nelegálních adres a služeb** – Spolupráce s blockchainovými analytickými firmami na sestavování databází adres spojených s nelegálními aktivitami.⁷⁴

8.1.4 Rozvoj technologických nástrojů pro monitorování a analýzu

- **Pokročilé forenzní nástroje pro sledování transakcí** – Implementace softwarů typu Chainalysis, CipherTrace nebo Elliptic, které umožňují sledování podezřelých transakcí a identifikaci propojení mezi různými adresami.⁷⁵

⁷² Comply Advantage *What is KYC and why is it important for crypto exchanges?* [online]. [cit. 2025-03-03]. Dostupné z: <https://complyadvantage.com/insights/what-is-kyc-crypto-exchanges/>

⁷³ FINTRAC's compliance guidance [online]. [cit. 2025-03-03]. Dostupné z: <https://fintrac-canafe.canada.ca/guidance-directives/transaction-operation/str-dod/str-dod-eng>

⁷⁴ Cropty *Blacklisted Bitcoins: Bitcoin Address Transparency Service* [online]. [cit. 2025-03-03]. Dostupné z: <https://www.cropty.io/blacklistedbitcoins>

⁷⁵ Simply Forensic *Dark Crypto: Essential Forensic Techniques for Blockchain Analysis* [online]. [cit. 2025-03-03]. Dostupné z: <https://simplyforensic.com/dark-crypto-essential-forensic-techniques-for-blockchain-analysis/>

- **Monitorování P2P a decentralizovaných platforem (DEX, DeFi)** – Zavedení technologií pro detekci nezákonných aktivit na decentralizovaných burzách a anonymních swapovacích protokolech.⁷⁶
- **Zavedení AI pro identifikaci podezřelých vzorců chování** – Použití strojového učení a AI k analýze transakcí a detekci neobvyklých aktivit, jako je layering a strukturování transakcí.⁷⁷

8.1.5 Zvýšení odpovědnosti a spolupráce soukromého sektoru

- **Povinnost spolupráce kryptoměnových společností s regulačními orgány** – Zajistit, aby burzy a další poskytovatelé digitálních služeb poskytovali regulačním institucím přístup k datům o podezřelých transakcích.⁷⁸
- **Transparentnost stablecoinů a DeFi protokolů** – Povinné auditování a reporting transakcí u stablecoinů, které často slouží jako přechodový most mezi tradičními financemi a kryptoměnami.⁷⁹
- **Zavedení samoregulačních mechanismů** – Podpora seberegulace kryptoměnových společností, podobně jako ve finančním sektoru, kde fungují nezávislé organizace dohlížející na compliance.⁸⁰

8.1.6 Vzdělávání a osvěta pro orgány činné v trestním řízení⁸¹

- **Školení vyšetřovatelů v oblasti blockchainové analýzy** – Zvýšení odborných kapacit a zavedení specializovaných jednotek pro kryptoměnové kriminalistické vyšetřování.

⁷⁶ Elliptic *Identifying DeFi money laundering risks with Holistic Screening* [online]. [cit. 2025-03-03]. Dostupné z: <https://www.elliptic.co/blog/analysis/identifying-defi-money-laundering-risks-with-holistic-screening>

⁷⁷ Bytefederal *Fraud Detection: How AI Can Identify Suspicious Blockchain Transactions* [online]. [cit. 2025-03-03]. Dostupné z: <https://www.bytefederal.com/byteu/15/167>

⁷⁸ THE EU GLOBAL FACILITY'S STRATEGY ON CRYPTOCURRENCIES [online]. [cit. 2025-03-03]. Dostupné z: https://www.global-amlcft.eu/wp-content/uploads/2023/06/VA-Strategy_EU_GLOBAL_Facility_compressed.pdf

⁷⁹ Dlapiper *Stablecoin Transparency Act introduced in Congress* CRYPTOCURRENCIES [online]. [cit. 2025-03-03]. Dostupné z: <https://www.dlapiper.com/es-pr/insights/publications/2022/07/stablecoin-transparency-act-introduced-in-congress>

⁸⁰ Investopedia *Should Cryptocurrency Exchanges Self-Regulate?* [online]. [cit. 2025-03-03]. Dostupné z: <https://www.investopedia.com/news/should-cryptocurrency-exchanges-selfregulate-themselves/>

⁸¹ Benson, V., Turksen, U. & Adamyk, B *Dark Side of Decentralised Finance: A Call for Enhanced AML Regulation Based on Use-Cases of Illicit Activities* [online]. [cit. 2025-03-03]. Dostupné z: <https://pure.coventry.ac.uk/ws/portalfiles/portal/79100962/Published.pdf>

- **Mezinárodní výměna informací a best practices** – Posílení spolupráce mezi **Interpol, Europol, FATF a národními regulačními orgány** pro efektivnější sdílení informací o praní peněz prostřednictvím kryptoměn.
- **Zvyšování povědomí veřejnosti o rizicích nelegálního využívání kryptoměn** – Vzdělávací kampaně zaměřené na uživatele, aby dokázali rozpoznat podvodné aktivity a chránili se před zneužitím.

Kombinace přísnější legislativy, technologických inovací a mezinárodní spolupráce může výrazně omezit praní špinavých peněz prostřednictvím kryptoměn. Zatímco blockchain sám o sobě poskytuje transparentní infrastrukturu pro sledování transakcí, inovativní metody zločinců vyžadují neustálou adaptaci regulačních a analytických strategií. Klíčovým prvkem prevence musí být efektivní vymáhání regulací, využívání forenzních nástrojů a aktivní spolupráce mezi soukromým sektorem a státními institucemi.

Závěr

V průběhu času se kryptoměny stávají stále více známými a široce přijímanými ve společnosti. Objeví se nový technologický fenomén, zpravidla ke zpoždění v jeho právní regulaci, neboť státní orgány potřebují určitý čas k jeho zaznamenání a následně k přijetí odpovídající legislativy. Toto období regulačního vakua může být využito k nezákonným účelům, neboť pachatelé často hledají způsoby, jak nové technologie zneužít ve svůj prospěch. Tento scénář je patrný i v oblasti kryptoměn. Zatímco některé státy již přistoupily k regulaci tohoto, jiné digitální měny zcela sektor zakázaly a další se teprve připravují na legislativní úpravy.

Kryptoměny představují efektivní nástroj pro legalizaci výnosů z trestné činnosti. Pokud není pachatel ztotožněn s adresou své peněženky, kterých může mít neomezené množství, zůstává anonymním. Navzdory skutečnosti, že veškeré transakce jsou zaznamenávány v blockchainu, a je možné sledovat pohyb jednotlivých prostředků, vytvoření rozsáhlé sítě za minimální poplatek může zkomplikovat jejich zpětnou rekonstrukci. Nejčastěji používanou kryptoměnou je bitcoin, což vede k tomu, že většina souvisejících služeb se orientuje právě na něj. V rámci jak běžného internetu, tak i darknetu, existují specializované služby – např. tzv. mixéry a tumblerové platformy s cílem znesnadnění vysledovatelnosti transakce. Tímto se uživatelé související s finančními toky stávají prakticky nevysledovatelní. Kombinací kryptoměn s anonymizačními či pseudoanonymizačními nástroji mohou pachatelé snížit riziko svého odhalení. Vzhledem k neustálému technologickému vývoji lze předpokládat, že tyto nástroje budou i nadále zdokonalovány.

Přestože se může legalizace výnosů prostřednictvím kryptoměn jevit jako poměrně snadná, je spojena s řadou rizik. Pachatelé musí být obezřetní, neboť nelze s jistotou určit, kdo stojí za provozem konkrétních anonymizačních služeb, což zvyšuje riziko podvodu – například situaci, kdy odeslané prostředky nejsou uživateli vráceny. Dalším faktorem je absence centrální autority, která by garantovala správnost transakce. V případě chybného zadání adresy nelze očekávat návrat finančních prostředků. Kromě problémů je krátkodobě rizikovým faktorem volatilní hodnota kryptoměny, která se může v těchto dramatických horizontech měnit. Pokud pachatelé nehodlají s kryptoměnou spekulovat, je pro ně výhodnější provést veškeré transakce v co nejkratším čase, aby se minimalizovalo riziko ztráty hodnoty prostředků. Další podmínkou úspěšné anonymizace

je technická gramotnost pachatele, zejména schopnost efektivně využívat systémy jako Tor či I2P k minimalizaci digitálních stop. Navzdory zmíněným rizikům lze kryptoměny vnímat jako rychlý a efektivní prostředek pro legalizaci výnosů z trestné činnosti.

Doposud není k dispozici dostatek empirických dat o případech legalizace výnosů z trestné činnosti prostřednictvím kryptoměn v České republice, neboť nebyl zveřejněn žádný konkrétní případ, který by tento dokumentoval. Legislativní orgány se nacházejí ve fázi přípravy legislativních úprav, přičemž s ohledem na dynamiku vývoje v této oblasti je žádoucí, aby byly přijaty nejdříve, zároveň však s dostatečnou flexibilitou pro jejich budoucí aktualizaci. Právní úprava by měla jasně definovat pojem kryptoměny a stanovit, jakým způsobem lze nakládat v kontextu národní ekonomiky. Dále je vhodné věnovat zvláštní pozornost regulaci směnárů a burz, které by měly být zavázány k plnění povinností pro subjekty podléhající regulaci finančního sektoru.

Přestože je bitcoin často spojován s nelegálními aktivitami, je nezbytné na kryptoměny nahlížet především jako na technologickou inovaci s potenciálem využití i v legitimních oblastech. Při analýze dostupných zdrojů lze označit tendenci k jejich stigmatizaci, kdy je bitcoin označován jako „měna terorismu“. Nicméně ve své podstatě jde o nositele hodnoty, jejíž dynamika není odlišná od tradičních měn. Podobná logika by mohla vést k požadavku na omezení používání amerického dolaru, který je v současnosti dominantní měnou při mezinárodních transakcích souvisejících s nelegálními aktivitami, například obchodem se zbraněmi či drogami. Cody Wilson, spoluzakladatel anonymní bitcoinové peněženky Dark Wallet, prohlásil: „Svoboda je nebezpečná věc.“⁸². S tímto tvrzením lze souhlasit, neboť otázka kryptoměn by měla být primárně řešena skrze prevenci a osvětu. Jedinec se silným smyslem pro odpovědnost a morální integritu se s nižší pravděpodobností zapojí do kriminálních aktivit a následné legalizace nelegálních výnosů.

Současná politika států však klade důraz zejména na represivní opatření, jejichž cílem je omezování individuálních svobod pod záminkou zvýšení bezpečnosti. Tuto tendenci již v 80. letech 20. století předpověděl Timothy C. May, výzkumník společnosti Intel, který formuloval koncept tzv. „Čtyř jezdců infokalypsy“⁸³. Podle jeho teorie budou

⁸² GORALE, A. *How to Launder Stolen Bitcoins*. In: CCN: Bitcoin, Blockchain, FinTech, & Cryptocurrency News [online]. [cit. 2025-02-003]. Dostupné z: <https://www.cryptocoinsnews.com/laundry-stolen-bitcoins/>.

⁸³ Paralelní Polis: *Bitcoin a továrna na budoucnost* [online]. [cit. 2002-02-03]. Dostupné z: <https://ekonomicky-denik.cz/paralelni-polis-bitcoin-a-tovarna-na-budoucnost>

státy používat regulaci anonymizačních technologií pod záminkou boje proti dětské pornografii, terorismu, organizovanému zločinu a obchodu s drogami. Tyto čtyři faktory jsou často využívány jako ospravedlnění pro omezení občanských svobod. Kryptoměny jsou s těmito fenomény často spojovány, avšak trestná činnost existovala a bude existovat bez ohledu na konkrétní platební metody. Zbývá tedy otázka, zda se tato předpověď plní, nebo zda kryptoměny – stejně jako další technologické inovace – budou nadále rozvíjeny a zda jsou využívány v širším spektru ekonomických aktivit.

V kontextu současného digitálního finančního ekosystému představují kryptoměny významný fenomén, který s sebou přináší nejen inovace v oblasti platebních systémů a decentralizace financí, ale rovněž výzvy v oblasti regulace a prevence finanční kriminality. Jak bylo v této práci analyzováno, kryptoměny mohou sloužit jako potenciální nástroj legalizace výnosů z trestné činnosti (tzv. praní špinavých peněz), zejména v důsledku své pseudonymity, rychlosti transakcí a globálního dosahu.

Přestože technologie blockchain disponuje vlastnostmi, jež umožňují vyšší transparentnost finančních toků, sofistikované metody, jako jsou mixéry, coinjoin transakce či využívání soukromých kryptoměn (např. Monero nebo Zcash), představují významné riziko pro vyšetřovací orgány. V reakci na tato rizika dochází k postupnému zpříšňování legislativního rámce jak na úrovni jednotlivých států, tak na mezinárodní úrovni, což reflektuje snahu regulatorních institucí eliminovat zneužívání kryptoměn k nezákonným účelům. Zkoumání této problematiky ukazuje, že efektivní regulace a dozor nad kryptoměnovým trhem musí být založeny na vyváženém přístupu mezi podporou technologického rozvoje a ochranou finančního systému před zneužitím. Klíčovou roli v tomto procesu hraje implementace legislativních opatření, jako je KYC (Know Your Customer) a AML (Anti-Money Laundering) požadavky pro kryptoměnové burzy a další poskytovatele služeb v oblasti digitálních aktiv.

Na základě provedené analýzy lze konstatovat, že ačkoli kryptoměny mohou být zneužívány pro účely praní špinavých peněz, technologický vývoj, spolupráce mezi regulatorními orgány a zavádění sofistikovaných forenzních metod umožňují efektivnější boj proti těmto hrozbám. Budoucí vývoj v této oblasti bude do značné míry záviset na schopnosti regulatorních institucí adaptovat se na dynamicky se měnící kryptoměnový ekosystém a nalézt rovnováhu mezi inovacemi a potřebou finanční bezpečnosti.

Seznam použitých zdrojů

Literární zdroje

1. CASTRONOVA, E. *Wildcat currency: how the virtual money revolution is transforming the economy*. New Haven: Yale University Press, 2014. 288 s. ISBN 978-0-300-21249-5.
2. DVOŘÁK, V. *Ekonomické a kriminální aspekty legalizace výnosů z trestné činnosti*. Vyd. 1. Praha: Scientia, 2010. 91 s. ISBN 978-80-86960-63-0.
3. DVOŘÁK, V. *Výnosy z trestné činnosti*. Praha : Scientia, 2010. 235 s. ISBN 978-80-86960-67-8.
4. DVOŘÁK, V. *Výnosy z trestné činnosti, jejich odhalování, identifikace a možnosti jejich odčerpání: sborník studií*. Praha : Scientia, 2010. 207 s. ISBN 978-80-86960-66-1.
5. HLAVINOVÁ, M. a KABEŠ, V.. *Zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu: komentář*. 3. vydání. Beckovy komentáře. V Praze: C.H. Beck, 2022. 552 s. ISBN 978-80-7400-860-3.
6. HUJOVÁ, G., ed. *Zkušenosti s virtuálními měnami - Bitcoin měna budoucnosti?: sborník z konference*: Praha, 26. března 2014. Praha: Vysoká škola manažerské informatiky, ekonomiky a práva, 2014. 149 s. ISBN 978-80-86847-71-9.
7. CHMELÍK, J., HÁJEK, P. a NEČAS, S. *Úvod do hospodářské kriminality*. 1. vydání, Plzeň: Aleš Čeněk, 2005. 168 s. ISBN 978-80-86898-13-1.
8. KOLOUCH, J. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. 528 s. CZ.NIC. ISBN 978- 80-88168-18-8.
9. KOLOUCH, J. a BAŠTA, P. *CyberSecurity*. CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2019. 560 s. ISBN 978-80-88168-31-7.
10. LÁNSKÝ, J. *Kryptoměny*. Praha: C.H. Beck, 2018. 160 s. ISBN 978-80-7400-722-4.
11. LIŠKA, P. *Praní špinavých peněz v České republice*. 1. vydání, Praha: RADIX, spol. s r.o, 1997. 220 s. ISBN 80-86031-09-8.
12. NETT, A. *Praní špinavých peněz*. 1. vyd. Brno: Masarykova univerzita, 1993. 39 s. ISBN 80-210-0630-7.
13. SCHEINOST, M. *Konvence OSN a další dokumenty k organizovanému zločinu*. Prameny. Praha: Institut pro kriminologii a sociální prevenci, 2001. 265 s. ISBN 80-86008-91-6.

14. STROUKAL, D. a SKALICKÝ, J. *Bitcoin: peníze budoucnosti: historie a ekonomie kryptoměn, stručná příručka pro úplné začátečníky*. Praha: Ludwig von Mises Institut CZ, 2015. 167 s. ISBN 978-80-87733-26-4.
15. TVRDÝ, J. *Zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu a předpisy související: komentář*. Vyd. 1. Praha: C. H. Beck, 2009. 501 s. ISBN 978-80-7400-099-7.
16. TVRDÝ, J. *Zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a předpisy související: komentář*. 1. vyd. Praha: C. H. Beck, 2004. 430 s. ISBN 80-7179-899-1.
17. *Virtual currency schemes*. Frankfurt am Main: European Central Bank, 2012. 55 s. ISBN 978-92-899-0862-7.

Legislativní dokumenty

1. Zákon č. 40/2009 Sb., trestní zákoník. In: Sbírka zákonů. 8. 1. 2009. ISSN 1211-1244.
2. Zákon č. 61/1996 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a o změně a doplnění souvisejících zákonů. In: Sbírka zákonů. 20. 3. 1996.
3. Zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu. In: Sbírka zákonů. 8. 7. 2008. ISSN 1211-1244.
4. Zákon č. 229/1992 Sb., o komoditních burzách. In: Sbírka zákonů. 29. 5. 1992.
5. Zákon č. 277/2013 Sb., o směnářské činnosti. In: Sbírka zákonů. 10. 10. 2013. ISSN 1211-1244.

Elektronické zdroje

1. A Gentle Introduction to How I2P Works. I2P Anonymous Network [online]. [cit. 2025-02-10]. Dostupné z: <https://geti2p.net/en/docs/how/intro>.
2. All Currencies | Crypto-Currency Market Capitalizations [online]. [cit. 2025-02-02]. Dostupné z: <https://coinmarketcap.com/all/views/all/>.
3. Analýza možností odčerpávat majetek pocházející z nelegitimních zdrojů mimotrestními prostředky. In: Hospodářská komora České republiky [online]. [cit. 2025-02-10]. Dostupné z: www.komora.cz/download.aspx?dontparse=true&FileID=634, s. 13.
4. BEDŘICH, V. *Tvůrci české konkurence Bitcoinu rozdávají sto tisíc jednotek zdarma*. In: CzechCrunch; nejčtenější web o startupech a technologiích [online].

- [cit. 2025-02-10]. Dostupné z: <https://cc.cz/tvurci-ceske-kryptomeny-rozdavaji-sto-tisic-jednotek-zdarma/>
5. Benson, V., Turksen, U. & Adamyk, B *Dark Side of Decentralised Finance: A Call for Enhanced AML Regulation Based on Use-Cases of Illicit Activities* [online]. [cit. 2025-03-03]. Dostupné z: <https://pure.coventry.ac.uk/ws/portalfiles/portal/79100962/Published.pdf>
 6. Bitcoin ATM Industry Statistics / Charts [online]. [cit. 2025-02-10]. Dostupné z: <https://coinatmradar.com/charts/>.
 7. Bitcoin jsou peníze, rozhodlo Německo. Ekonomika, byznys, finance - E15.cz / zprávy [online]. [cit. 2025-02-14]. Dostupné z: <https://zpravy.e15.cz/burzy-atrhy/meny/bitcoin-je-penize-rozhodlo-nemecko-1014811>.
 8. Bitcoin už na poště a v Sazce nekoupíte, služba skončila po šesti týdnech. In: Český rozhlas[online]. [cit. 2025-02-09]. Dostupné z: https://www.irozhlas.cz/ekonomika/bitcoin-uz-na-poste-a-v-sazce-nekoupite-sluzba-skoncila-po-sesti-tydnech_201503270315_mkopp.
 9. BOŘÁNEK, R. *Czech Crown Coin: český pokus o národní kryptoměnu*. In: Root.cz - informace nejen ze světa Linuxu [online]. [cit. 2025-02-02]. Dostupné z: <https://www.root.cz/clanky/czech-crown-coin-cesky-pokus-o-narodni-kryptomenu/>.
 10. BUNTINX, P. *Dutch Police Arrests Three People in Bitcoin Money Laundering Investigation*. In: Bitcoinist.net - Bitcoin News, Prices, information & reviews [online]. [cit. 2025-02-13]. Dostupné z: <https://bitcoinist.com/dutch-police-arrests-three-people-bitcoin-money-laundering-investigation/>.
 11. Bytefederal *Fraud Detection: How AI Can Identify Suspicious Blockchain Transactions* [online]. [cit. 2025-03-03]. Dostupné z: <https://www.bytefederal.com/byteu/15/167>
 12. CleanCoin - Low-Fee Bitcoin Mixing/Tumbling/Laundry Service [online]. [cit. 2025-02-10]. Dostupné z: <http://cleancondgja34b.onion>.
 13. Co je bitcoin? Vše o bitcoinu a digitálních měnách [online]. [cit. 2025-02-04]. Dostupné z: <https://btctip.cz/co-je-bitcoin/>.
 14. Co si za to koupím? Vše o bitcoinu a digitálních měnách [online]. [cit. 2025-02-08]. Dostupné z: <https://btctip.cz/btc-obchody-a-sluzby/>.
 15. Cochintu, C. *The next bitcoin (BTC) halving* [online]. [cit. 2025-02-27]. Dostupné z: <https://capex.com/en/academy/bitcoin-halving-2024>

16. Comply Advantage *What is KYC and why is it important for crypto exchanges?* [online]. [cit. 2025-03-03]. Dostupné z: <https://complyadvantage.com/insights/what-is-kyc-crypto-exchanges/>
17. Crypto-Currency Market Capitalizations [online]. [cit. 2025-02-28]. Dostupné z: <https://coinmarketcap.com>.
18. Český bitcoin čeká regulace a zdanění. Informace pro informované | Ekonomický deník [online]. [cit. 2025-02-14]. Dostupné z: <https://ekonomicky-denik.cz/ceskybitcoin-ceka-regulace-a-zdaneni/>.
19. Daňové ráje [online]. [cit. 2025-02-10]. Dostupné z: <http://www.danoveraje.eu>
20. DVOŘÁK, V. a ZÁMEK D. *Výnos z trestné činnosti a jeho modifikace*. In: Bezpečnostní sbory[online]. [cit. 2025-02-02]. Dostupné z: https://bezpecnostni-sbory.wbs.cz/clanky/6-2011/vynos_z_trestne_cinnosti_a_jeho_modifikace.pdf
21. Edwards, J. *Bitcoin's Price History* [online]. [cit. 2025-02-27]. Dostupné z: <https://www.investopedia.com/articles/forex/121815/bitcoins-price-history.asp>
22. FILLNER, K. *Coin.mx končí - FBI zatkla dva údajné provozovatele ilegální bitcoinové směnárný*. In: Budoucnost peněz: bitcoinové zprávy | finanční a technologické inovace [online]. [cit. 2025-02-03]. Dostupné z: <https://cointelegraph.cz/news/coinmx-konci-fbi-zatkla-dva-udajneprovozovatele-ilegalni-bitcoinove-smenarny>
23. FILLNER, K. *Rozhodnutí Evropského soudního dvoru: Na směnu bitcoinu se nevztahuje DPH*. In: Budoucnost peněz: bitcoinové zprávy | finanční a technologické inovace [online]. [cit. 2025-02-15]. Dostupné z: <https://www.btctip.cz/soudni-dvur-eu-bitcoinove-transakce-osvobozeny-od-dph/>.
24. FILLNER, K. *Ruské ministerstvo financí navrhuje tvrdé tresty za používání kryptoměn*. In: Budoucnost peněz: bitcoinové zprávy | finanční a technologické inovace [online]. [cit. 2025-02-14]. Dostupné z: <https://www.btctip.cz/rusko-planuje-zakaz-bitcoinu-a-kriminalizaci-jeho-pouzivani/>.
25. FINTRAC's compliance guidance [online]. [cit. 2025-03-03]. Dostupné z: <https://fintrac-canafe.canada.ca/guidance-directives/transaction-operation/str-dod/str-dod-eng>
26. Forbes *Český trh s kryptoaktivy se dočká regulace. Prezident Pavel podepsal kryptoměnový balíček*. [online] Dostupné z: <https://forbes.cz/cesky-trh-s>

- kryptoaktivy-se-docka-regulace-prezident-pavel-podepsal-kryptomenovy-balicek/. [cit. 2025-02-09].
27. Founder of Liberty Reserve Pleads Guilty to Laundering More Than \$250 Million through His Digital Currency Business. U.S. Department of Justice [online]. [cit. 2025-03-05]. Dostupné z: <https://www.justice.gov/archives/opa/pr/founder-liberty-reserve-pleads-guilty-laundering-more-250-million-through-his-digital>.
28. GORALE, A. *How to Launder Stolen Bitcoins*. In: CCN: Bitcoin, Blockchain, FinTech, & Cryptocurrency News [online]. [cit. 2025-02-09]. Dostupné z: <https://www.cryptocoinsnews.com/laundry-stolen-bitcoins/>.
29. GRAYDON, C. *What is Cryptocurrency?* In: CCN: Bitcoin, Blockchain, FinTech; Cryptocurrency News[online]. [cit. 2025-02-02]. Dostupné z: <https://www.cryptocoinsnews.com/cryptocurrency/>.
30. HANŽLOVÁ, J. *Evropský bankovní úřad varuje před používáním bitcoinů navrhuje regulaci*. In: Český rozhlas [online]. [cit. 2025-02-15]. Dostupné z: <https://www.irozhlas.cz/node/5944151>.
31. Hidden Wallet *Tor Anonymous Hidden Bitcoin Wallet* [online]. [cit. 2025-02-10]. Dostupné z: <http://nql7pv7k32nnqor2.onion/>.
32. HILL, K. *Bitcoin in China: The Fall-out From Chinese Government Banning Real World Use*. In: Forbes Europe [online]. [cit. 2025-02-04]. Dostupné z: <https://www.forbes.com/sites/kashmirhill/2013/12/06/bitcoin-in-china-the-fall-out-from-chinese-government-banning-real-world-use/>.
33. HORÁČEK, F. *V Česku vznikla první virtuální měna, stránky napadají hackeři*. In: IDNES.cz – zprávy, kterým můžete věřit [online]. [cit. 2025-02-02]. Dostupné z: https://www.idnes.cz/ekonomika/domaci/v-cesku-vznika-prvni-virtualni-mena-czech-crown-coin.A140717_113758_ekonomika_fih.
34. CHRISTIN, N. *Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace* [online]. [cit. 2025-02-19]. Dostupné z: <https://www.andrew.cmu.edu/user/nicolasc/publications/Christin-WWW13.pdf>.
35. Jak se při obchodování s bitcoiny vyhnout podvodům. Bitcoin, digitální měny, vše o kryptoměnách [online]. [cit. 2025-02-04]. Dostupné z: <https://btctip.cz/jak-se-priobchodovani-s-bitcoiny-vyhnout-podvodum>.
36. Japan considers making bitcoin a legal currency. News, sport and opinion from the Guardian's global edition [online]. [cit. 2025-02-13]. Dostupné z: <https://www.theguardian.com/technology/2016/feb/25/japan-to-make-bitcoin-legal-currency>.

37. JEKIELEK, M. *Advokát radí: Bitcoin a právo*. In: OnBusiness: Ekonomika, podnikání, investice [online]. [cit. 2025-03-05]. Dostupné z: <https://onbusiness.cz/advokat-radi-bitcoin-a-pravo-2229>.
38. Kořínek, V. *Jak danit kryptoměny v roce 2025* [online]. [cit. 2025-02-02]. Dostupné z: <https://blog.simplecoin.eu/jak-danit-kryptomeny/>
39. Legislativa AML/CFT. Ministerstvo financí České republiky [online]. [cit. 2025-02-10]. Dostupné z: https://www.mfcr.cz/assets/cs/media/Studie_2018_Podkladova-studie-online-identifikace-a-AML-CFT.pdf.
40. METODICKÝ POKYN č. 2 Finančního analytického útvaru Ministerstva financí ze dne 16. září 2013 určený povinným osobám O PŘÍSTUPU POVINNÝCH OSOB K DIGITÁLNÍM MĚNÁM. In: Ministerstvo financí [online]. [cit. 2025-02-11]. Dostupné z: <https://www.mfcr.cz/cs/zahranicni-sektor/ochrana-financnich-zajmu/boj-protiprani-penez-a-financovani-tero/novinky-fau/2013/digitalni-meny-14568>.
41. Mezinárodní spolupráce - Boj proti praní peněz a financování terorismu. Ministerstvo financí České republiky [online]. [cit. 2025-02-10]. Dostupné z: <https://www.mfcr.cz/cs/zahranicni-sektor/mezinarodnispoluprace/mezinarodni-institute/mezinarodni-spoluprace-boj-proti-prani-11642>.
42. Moneyval. Nejvyšší státní zastupitelství [online]. [cit. 2025-02-10]. Dostupné z: <https://www.nsz.cz/index.php/cs/mezinarodni-spoluprace/daliorganizace/moneyval>.
43. Nákup a prodej prostřednictvím bitcoinu - hotovost. WBTCB [online]. [cit. 2025-02-05]. Dostupné z: <https://www.wbtc.com/cz/sluzby/nakup-a-prodejprostrednictvim-bitcoinu-hotovost>.
44. Obchodování s bitcoiny. In: Česká národní banka [online]. 2014 [cit. 2025-02-05]. Dostupné z: <https://www.cnb.cz/cs/dohled-financni-trh/legislativni-zakladna/stanoviska-k-regulaci-financniho-trhu/RS2014-02>.
45. Online Currency Exchange Accused of Laundering \$6 Billion. The New York Times - Breaking News, World News & Multimedia [online]. [cit. 2025-02-05]. Dostupné z: <https://www.nytimes.com/2013/05/29/nyregion/liberty-reserve-operators-accused-of-money-laundering.html>.
46. Paralelní Polis: Bitcoin a továrna na budoucnost [online]. [cit. 2025-02-15]. Dostupné z: <https://ekonomickydenik.cz/paralelni-polis-bitcoin-a-tovarna-na-budoucnost/>.

47. POPPER, N. *Bitcoin Exchange Receives First License in New York State*. In: The New York Times - Breaking News, World News & Multimedia [online]. [cit. 2025-02-14]. Dostupné z: <https://www.nytimes.com/2015/05/08/business/dealbook/bitcoin-exchange-receives-first-license-in-new-york-state.html>.
48. Rise and Rise of Bitcoin, The [dokumentární film]. Režie MROSS, N. USA, 2014. 66 Silk Road (marketplace). Wikipedia, the free encyclopedia [online]. [cit. 2025-02-12]. Dostupné z: [https://en.wikipedia.org/wiki/Silk_Road_\(marketplace\)#cite_note-nytlife-14](https://en.wikipedia.org/wiki/Silk_Road_(marketplace)#cite_note-nytlife-14).
49. Rooney, B. *Bitcoin prices top \$1,000* [online]. [cit. 2025-02-27]. Dostupné z: <https://money.cnn.com/2013/11/27/investing/bitcoin-1000/>
50. Royal, J. Ph.D. *Bitcoin's price history: From its 2009 launch to its 2025 heights* [online]. [cit. 2025-02-27]. Dostupné z: <https://www.bankrate.com/investing/bitcoin-price-history>
51. Silk Road (marketplace). Wikipedia, the free encyclopedia [online]. [cit. 2025-02-02]. Dostupné z: [https://en.wikipedia.org/wiki/Silk_Road_\(marketplace\)#cite_note-nytlife-14](https://en.wikipedia.org/wiki/Silk_Road_(marketplace)#cite_note-nytlife-14)
52. SimpleCoin - snadný nákup Bitcoinů [online]. [cit. 2025-02-04]. Dostupné z: <https://simplecoin.cz>.
53. Simply Forensic *Dark Crypto: Essential Forensic Techniques for Blockchain Analysis* [online]. [cit. 2025-03-03]. Dostupné z: <https://simplyforensic.com/dark-crypto-essential-forensic-techniques-for-blockchain-analysis/>
54. STERLING, T. *Dutch arrest 10 men suspected of using Bitcoin to launder money*. In: Business & Financial News, Breaking US & International News | Reuters.com [online]. [cit. 2025-02-10]. Dostupné z: <https://www.reuters.com/article/us-netherlands-crime-bitcoin-idUSKCN0UY0V8>.
55. Steuern für Bitcoins. BitcoinBlog.de – das Blog für Bitcoin und andere virtuelle Währungen[online]. [cit. 2025-02-13]. Dostupné z: <https://bitcoinblog.de/2014/01/06/steuern-fuer-bitcoins/>.
56. THE EU GLOBAL FACILITY'S STRATEGY ON CRYPTOCURRENCIES [online]. [cit. 2025-03-03]. Dostupné z: https://www.global-amlcft.eu/wp-content/uploads/2023/06/VA-Strategy_EU_GLOBAL_Facility_compressed.pdf

57. Things you need to know: Important Bitcoin Basics and How It All Works. Bitcoin.com [online]. [cit. 2025-02-04]. Dostupné z: <https://www.bitcoin.com/you-need-to-know>.
58. Tor Project: Overview. Tor Project: Anonymity Online [online]. [cit. 2025-02-10]. Dostupné z: <https://www.torproject.org/about/overview.html.en>.
59. Útvar odhalování korupce a finanční kriminality SKPV. Policie České republiky [online]. [cit. 2025-02-10]. Dostupné z: <https://policie.gov.cz/clanek/uokfk-skp-utvar-odhalovani-korupce-a-financni-kriminality-skp.aspx>.
60. VIGNA, Paul a Michael CASEY. The Age of Cryptocurrency. In: The Investing Podcast [online]. [cit. 2025-02-02]. Dostupné z: <https://archive.org/details/ageofcryptocurre0000vign/>.
61. Vuvuzela: Scalable Private Messaging Resistant to Traffic Analysis. In: PoPETs/PETS [online]. [cit. 2025-02-12]. Dostupné z: <https://petsymposium.org/2015/papers/vandenhooff-vuvuzela-hotpets2015.pdf>.
62. Vznikla "česko-slovenská" kryptoměna Koruna, ešte nedôveryhodnejšia ako CZC. In: Digitálny svet pod lupou [online]. [cit. 2025-02-02]. Dostupné z: <https://www.dsl.sk/article.php?article=15935>.
63. WAGNER, A. *Digital vs. Virtual Currencies*. In: Bitcoin Magazine | Bitcoin and Cryptocurrency News [online]. [cit. 2025-02-14]. Dostupné z: <https://bitcoinmagazine.com/articles/digital-vs-virtual-currencies-1408735507>.
64. Webtrh. Můj byznys roste. [online]. [cit. 2025-02-02]. Dostupné z: <https://webtrh.cz/324470-nabizime-limitovany-podil-ceskoslovenskem-projektu>.
65. Wikipedia.org History of bitcoin [online]. [cit. 2025-02-27]. Dostupné z: https://en.wikipedia.org/wiki/History_of_bitcoin
66. Wikipedia.org Mt. Gox [online]. [cit. 2025-02-27]. Dostupné z: https://en.wikipedia.org/wiki/Mt._Gox
67. Základní informace. Ministerstvo financí České republiky [online]. [cit. 2025-02-10]. Dostupné z: <https://www.mfcr.cz/cs/zahranicni-sektor/ochrana-financnich-zajmu/boj-proti-prani-penez-a-financovani-tero/zakladni-informace>

Obrázky

Obrázek č. 1 Vývoj hodnoty Bitcoin od roku 2016 do 2025 v USD	29
Obrázek č. 2 Vývoj hodnoty Bitcoin od roku 2016 do 2025 v USD	31
Obrázek č. 3 Přehledová mapa bitcoinmatů na území města Prahy	34