

Univerzita Karlova v Praze

Právnická fakulta

Katedra finančního práva a finanční vědy

Jan Pardubický

## **BITCOIN**

### **Právní rámec a praktické aspekty jeho používání v platebním styku**

Diplomová práce

Vedoucí diplomové práce: JUDr. Petr Kotáb

Datum vypracování práce: 30.6.2014

Prohlašuji, že jsem předkládanou diplomovou práci vypracoval samostatně, všechny použité prameny a literatura byly řádně citovány a práce nebyla využita k získání jiného nebo stejného titulu.

V Praze dne .....

.....

Jan Pardubický

## Obsah

Úvod.....	5
1. Popis předmětu výzkumu – Bitcoinový platební systém, jeho charakteristika a popis technických principů jeho fungování.....	7
1.1. Stručná charakteristika bitcoinového platebního systému.....	7
1.2. Dvojitá povaha pojmu bitcoin.....	8
1.3. Princip fungování bitcoinového platebního systému.....	8
1.4. Decentralizovaná povaha bitcoinového systému, implikace této skutečnosti.....	13
1.5. Emise a tržní cena bitcoinu.....	14
1.6. Odvozené platební systémy.....	16
2. Otázka souladu bitcoinového systému s právním řádem.....	17
2.1. Existence norem zakazujících účast na bitcoinovém platebním systému.....	18
3. Zařazení bitcoinu do existujících právních kategorií.....	19
3.1. Kategorie věci v právním slova smyslu.....	19
3.2. Právní úprava měny a peněz.....	22
3.2.1. Zařazení bitcoinu pod kategorii peněz.....	23
3.2.2. Zařazení bitcoinu pod kategorii měny.....	31
3.2.3. Jsou bitcoiny elektronické peníze?.....	33
3.3. Další v úvahu připadající kategorie.....	34
4. Bitcoinový ekosystém – společenské a právní vztahy obklopující bitcoinový platební systém.....	34
4.1. Uživatelé bitcoinového platebního systému.....	35
4.2. Komunita vývojářů bitcoinového platebního systému.....	38
4.3. Bitcoinové burzy, směnární a bankomaty.....	40
4.3.1. Bitcoinové směnární.....	41
4.3.2. Bitcoinové burzy.....	43
4.3.2.1. Subsumpce bitcoinových burz pod zákon o komoditních burzách.....	47

4.3.2.2. Subsumpce bitcoinových burz pod zákon o podnikání na kapitálovém trhu .....	53
4.4. Prodejci zboží a poskytovatelé služeb přijímající bitcoin.....	54
4.5. Poskytovatelé služeb souvisejících s používáním bitcoinového platebního systému.....	55
5. Nelegální a společensky škodlivé činnosti spojované s bitcoinovým platebním systémem.....	56
5.1. Bitcoinový platební systém a praní špinavých peněz.....	57
5.2. Bitcoinový platební systém a nelegální obchod s omamnými a psychotropními látkami.....	62
6. Regulace bitcoinového platebního systému u nás a ve světě de lege ferenda.....	64
7. Další možnosti využití.....	67
Závěr.....	68
Seznam použitých zdrojů.....	72
Webové odkazy.....	76
Seznam použitých zkratk a některých pojmů:.....	77
Abstrakt.....	79
Summary in english.....	81

## Úvod

Bitcoin a jemu podobné systémy jsou novým fenoménem v platebním styku, který se v mnoha ohledech vymyká klasickému pojetí peněz do kterého v této souvislosti zahrnujeme i peníze elektronické.

Jejich existenci právní systémy většiny států světa dosud nereflektují. Je to proto, že během procesu tvorby předpisů upravujících peníze, měnu a platební styk tyto systémy ještě neexistovaly, nebo se jejich užití omezovalo na úzkou skupinu vývojářů, nadšenců a akademiků.

Z toho důvodu je nelze subsumovat pod většinu zákonných definic a tak se lze ve společnosti setkat i s názory že se na ně právní řád vůbec nevztahuje a objevují se proto hlasy volající po jejich explicitní úpravě.

Tato práce naopak vychází z názoru, že přesto, že velké množství předpisů upravujících oblasti jim funkčně podobné (měna, bankovníctví, platební styk, elektronické platební systémy, cenné papíry) se na ně kvůli jejich specifickým vlastnostem nevztahuje, neznámá to, že se by se pohybovaly v nějakém druhu právního vakua – naopak při nakládání s nimi lze aplikovat velké množství právních norem (zejména soukromého práva) tak, jako by se jednalo o jakýkoli jiný druh univerzálního zboží. Při dodržení obecných pravidel toho kterého odvětví pak samozřejmě přichází v úvahu i užití analogie.

Vzhledem k tomu, že se do budoucna jistě dá očekávat vznik právních norem, upravujících bitcoin a jemu podobné systémy ať již zvláštními předpisy nebo formou rozšíření současných legálních definic, dotkneme se také otázky nutnosti a vhodnosti právní úpravy a podobami, jaké by mohla nabývat. Inspiraci a podklady k diskusi nám v tomto ohledu budou poskytovat dokumenty různé povahy a právní závaznosti reflektující existenci bitcoinového platebního systému, které v současné době vznikají napříč státy celého světa.

Protože se jedná o poměrně nový jev (bitcoin spatřil světlo světa teprve v roce 2009), existuje na toto téma, zejména v českém jazyce, nedostatek literatury a prakticky žádná judikatura - Výjimkou jsou některá stanoviska či pokyny orgánů veřejné moci, která se v poslední době začala pomalu objevovat v souvislosti s rozšiřováním použití

bitcoinu v platebním styku a kterým zde samozřejmě budeme věnovat pozornost. Z toho důvodu budou klíčovými prameny články, jak z cizojazyčných odborných časopisů, tak i články publikované na internetových stránkách, které se touto problematikou zabývají. Dalšími důležitými prameny pak bude česká právní literatura zejména z oborů finančního práva a právní teorie.

Existuje reálná možnost, že část právníkové veřejnosti shledá sekci, ve které se budeme poměrně dopodrobna zabývat technologií, jež tvoří základ bitcoinového platebního systému, za poněkud nestravitelnou a těžko pochopitelnou, domnívám se však, že ke správné interpretaci a zejména tvorbě právních norem v libovolné oblasti, je nezbytné pochopení principů které ovládají upravovanou materii. Stejně tak je důležité proniknout do systému společenských a jiných vztahů, který se okolo ní vytváří. Touto myšlenkou se ještě budeme poněkud podrobněji zabývat v části, která vysvětluje fungování bitcoinového platebního systému.

Kromě bitcoinu samotného existuje i větší množství platebních systémů, které se z něj vyvinuly, a které mu jsou v mnoha klíčových aspektech podobné. Ačkoli se tato práce bude zabývat především bitcoinem jako původním zástupcem rodiny decentralizovaných platebních systémů, velkou část z toho co zde řekneme je možné analogicky vztáhnout i na tyto odvozené systémy.

Je poměrně jasné, že tato práce neodpoví na všechny otázky, které mohou vyvstat v souvislosti s právní úpravou platebních systémů bitcoinového typu. Dá se dokonce předpokládat, že nakonec přinese víc otázek než odpovědí. Přesto věřím, že elektronické decentralizované systémy tohoto typu, stejně tak jako i jiné nové technologie, jsou tématem, které by právní věda neměla ignorovat. Přesto, že si uvědomuji, že postavení těchto systémů je v současné době přinejmenším nejisté, doufám že se mi podaří alespoň zachytit relevantní znaky těchto systémů, osvětlit principy na kterých fungují, nahlédnout do společenských vztahů, které ho obklopují a objasnit otázku příslušnosti bitcoinu k některým právně relevantním kategoriím a důsledky, které z toho plynou.

# 1. Popis předmětu výzkumu – Bitcoinový platební systém, jeho charakteristika a popis technických principů jeho fungování

## 1.1. Stručná charakteristika bitcoinového platebního systému

Na neoficiálních webových stránkách<sup>1</sup> bitcoinového platebního systému se lze dočíst že bitcoin je „inovativní platební síť a nový druh peněz“<sup>2</sup>

Jde o systém, který umožňuje provádění plateb prostřednictvím počítačové sítě, bez využití služeb třetí strany (poskytovatele platebních služeb). Zvláštností tohoto systému je vysoká úroveň decentralizace. Platby bitcoinem jsou rychlé, ireverzibilní<sup>3</sup>, v porovnání s jinými způsoby plateb mají velmi nízké transakční náklady a při jejich odesílání či přijímání není nutné zpracovávat ani poskytovat žádné osobní údaje (což může představovat výhodu jak pro podnikatele přijímající platby v bitcoinech, tak pro jejich zákazníky).

Základem systému je tzv. Bitcoinový protokol na jehož vývoji se podílí neuzavřený tým vývojářů. Protokol má otevřený zdrojový kód a je uvolněn pod

---

1

Z decentralizované povahy projektu vyplývá že nic takového jako oficiální stránky vlastně neexistuje. Doména byla zaregistrována prostřednictvím společnosti WhoisGuard, o které se mi nepodařilo zjistit nic bližšího než jejich email, webové stránky a P.O. box v Panamské republice. Byla však patrně zaregistrována Satoshi Nakamotem a správu webových stránek zajišťuje jádro týmu vývojářů.

<sup>2</sup> <http://bitcoin.org/>

<sup>3</sup> Nezvratné, platbu která jednou proběhne již nelze vzít zpět. Tím se liší např. od platby kreditní kartou kde je možné po určité době provést tzv. chargeback. Samozřejmě to nebrání provedení zpětné platby, tu zde však musí provést původní příjemce.

svobodnou tzv. copyleftovou<sup>4</sup> licencí MIT<sup>5</sup>. To často platí i pro programy, které tento protokol implementují a které označujeme jako *bitcoinové klienty* zejména pro referenční klient bitcoind.

## 1.2. Dvojitá povaha pojmu bitcoin

Citace ze začátku předchozího odstavce nám odhaluje dvojitou podstatu pojmu bitcoinu. V jednom pojetí ho můžeme vnímat jako volnou síť navzájem propojených počítačů, která umožňuje posílat a přijímat platby. V druhém pojetí ho pak budeme chápat jako určitý druh univerzálního zboží, které je předmětem těchto plateb. Samotný termín *bitcoin* tu budeme používat pro označení formy peněz (při vyjádření množství se často používá zkratka BTC), kterou bitcoin představuje. Pro pojetí bitcoinu jako sítě budeme používat termín *bitcoinový platební systém*. Je však důležité si uvědomit že jde jen o dva aspekty téhož jevu neboť neexistují bitcoiny bez platebního systému a naopak.

## 1.3. Princip fungování bitcoinového platebního systému

Fungování bitcoinového platebního systému je poměrně složité a zahrnuje aplikaci pokročilé matematiky a kryptografie<sup>6</sup>. Tato práce si nedává za cíl vysvětlit do detailů všechny technické aspekty tohoto systému (ostatně to je daleko za hranicemi schopností autora). Určité pochopení podkladové technologie je však nezbytné k bezpečnému zacházení s bitcoinem v platebním styku. Ke správné právní analýze a diskuzi o možných formách právní regulace je pak nepochybně zapotřebí znalostí o poznání hlubších. V opačném případě by mohlo dojít ke vzniku právních norem a aktů aplikace práva, která buď nepřiměřeně zatěžují uživatele a anulují tak výhody, které

---

<sup>4</sup>Licence MIT v zásadě umožňuje bezplatně nakládat s licencovaným předmětem poměrně širokým okruhem způsobů – zahrnuje zejména oprávnění ho bezplatně používat, kopírovat, pozměňovat, publikovat, distribuovat, nebo dokonce prodávat. Ovšem s touto výhradou, že software je bez jakékoli záruky a všechny kopie nebo podstatné části musí obsahovat právě toto licenční ujednání. (zdroj: <http://opensource.org/licenses/MIT>)

<sup>5</sup>Bitcoin Core integration/staging tree. *GitHub* [online]. 2009 [cit. 2014-02-18]. Dostupné z: <https://github.com/bitcoin/bitcoin>

<sup>6</sup>Kryptografie je nauka o šifrování. Její aplikace zahrnují šifrovaný přenos dat, digitální podpisy, možnosti ověření integrity dat a další. Mnoho z nich je v bitcoinovém protokolu využito.



bitcoinový systém přináší, nebo dokonce ke vzniku vnitřně rozporných a fakticky nevykonatelných právních předpisů a rozhodnutí<sup>7</sup>. V neposlední řadě též považují za vhodné zmínit, že se jedná o systém, jehož sofistikovaný design a vnitřní integrita mohou být a v mnoha případech také jsou, samy o sobě zdrojem intelektuálního potěšení při jeho studiu<sup>8</sup>.

Za zakladatele bitcoinového systému považujeme programátora (možná také skupinu programátorů, neboť jeho skutečná identita je stále neznámá) vystupujícího pod pseudonymem Satoshi Nakamoto, který v roce 2008 zveřejnil na internetu dokument nazvaný „*Bitcoin: A Peer-to-Peer<sup>9</sup> Electronic Cash System*“. Ten popisuje design technologie, která by umožnila platby prostřednictvím počítačové sítě přímo mezi uživateli, bez nutnosti využít služeb finanční instituce. V následujícím roce uvolnil první verzi softwaru implementujícího tuto technologii, na jehož vývoji se od té doby podílí poměrně široká komunita programátorů (podle stránek, kde se soustředí vývoj projektu [www.github.com/bitcoin/bitcoin](http://www.github.com/bitcoin/bitcoin) dosud přispělo svým zdrojovým kódem 167 vývojářů) včetně samotného Satoshiho Nakamoty. Jeho činnost na vývoji se postupně utlumovala, až v roce 2010 předal kontrolu nad zdrojovým kódem programátorovi Gavinu Andresenovi a nadobro se vytratil<sup>10</sup>. Satoshiho skutečná identita je zejména uvnitř bitcoinové komunity předmětem mnoha spekulací.

Lze se setkat s názory, že fakt že není známa identita původního autora podkopává důvěryhodnost celého systému. Takový názor ovšem pramení z neznalosti okolností, za kterých je software vyvíjen: Celý zdrojový kód byl Nakamotem zveřejněn,

---

<sup>7</sup>Ilustrací následků neznalosti principů ovládajících upravovanou technologii může být například rozhodnutí francouzského soudu ve věci užití ochranné známky payline německou společností Brokat (ta měla známku zaregistrovanou na území Německa, zatímco žalobce si již dříve tuto známku zaregistroval ve Francii). Toto rozhodnutí zakazovalo německé společnosti užití ochranné známky payline, včetně užití na webových stránkách brokat.de a to na území Francie. Důsledkem nedostatečného pochopení fungování sítě internet pak byla praktická nevykonatelnost takového rozhodnutí, neboť nebylo v moci společnosti Brokat zabránit přístupu na své stránky z území Francie. (Zdroj: POLČÁK, Radim. *Právo na internetu: spam a odpovědnost ISP*. Vyd. 1. Brno: Computer Press, 2007, s. 23. ISBN 978-80-251-1777-4. )

<sup>8</sup>srov např. The Nature of the Form: Legal and Regulatory Issues Surrounding the Bitcoin Digital Currency System. In: DOGUET, Joshua J. *Louisiana Law Review* č. 73. 2013. V úvodu této práce se konstatuje, že bitcoinový systém bývá experty označován za „mistrovský kousek technologie“ a byl dokonce srovnáván jako geniální výtvar s obrazem Mona Lisa renesančního umělce Leonarda da Vinci.

<sup>9</sup>Anglicky rovný s rovným, často se používá zkratka P2P.

<sup>10</sup>The history of Bitcoin from its very beginning in 2008. In: *Bitcoinsberlin* [online]. [cit. 2014-02-20]. Dostupné z: <https://bitcoinsberlin.com/the-history-of-bitcoin-from-its-very-beginning-2008-2/>

je v každém okamžiku k dispozici a je předmětem diskurzu a neustálého vývoje. Identita původního autora je tak, přinejmenším ve vztahu ke kvalitě systému, zcela bezpředmětná.

Architektura bitcoinového systému je velice propracovaná a učarovala mnoha programátorům a technologickým nadšencům, z jejichž okruhu se rekrutovaly první uživatelé. Popsat ji je poměrně složité, přesto se o to zde pokusím, neboť jak jsem již napsal výše, chápání principů, na kterých je systém založen, je předpokladem další právní analýzy (Naproti tomu samotné používání není o nic složitější než používání internetového bankovníctví). Základem bitcoinového platebního systému je síť navzájem rovných uzlů<sup>11</sup>, které provozují software označovaný jako *bitcoinový klient* a které mezi sebou šíří informaci o probíhajících transakcích a spolupracují na tvorbě veřejně přístupného záznamu o nich.

Uzly sítě sdílejí konsenzus o historii proběhlých transakcí - záznam který je vytvářen podle dohodnutých pravidel a který tvoří jakousi veřejně přístupnou účetní knihu, ze které lze vyčíst z jaké adresy, kdy a kolik bitcoinů na jakou adresu bylo odesláno a tedy i jaký je zůstatek na té či oné adrese. Tento záznam je označován jako tzv. *blockchain* – řetěz bloků.

V rámci sítě můžeme rozlišovat dva druhy uživatelů. Jedním jsou běžní uživatelé, kteří síť používají pro zasílání a přijímání plateb a současně šíří informace o proběhlých transakcích. Druhým jsou takzvaní těžaři nebo též mineři<sup>12</sup>, kteří zajišťují službu nezbytnou pro správné fungování sítě a jsou za to odměňováni – touto službou je právě tvorba *blockchainu* – záznamu o proběhlých transakcích, odměnou jsou dobrovolné transakční poplatky a oprávnění emitovat nové mince.

Autenticitu provedených transakcí zajišťuje asymetrická kryptografie, někdy též označovaná jako kryptografie veřejného klíče<sup>13</sup>. Potřeba veřejného záznamu však

---

<sup>11</sup>Uzel (anglicky node) je označení pro zařízení připojené do sítě.

<sup>12</sup>Z anglického mine - těžit

<sup>13</sup>Jedná se o technologii aplikovanou v tzv. elektronických podpisech. Existují dva klíče, které jsou spolu určitým způsobem matematicky provázány. Tyto klíče jsou označovány jako soukromý klíč a veřejný klíč. Uživatel drží svůj soukromý klíč v tajnosti, a veřejný naopak dá k dispozici. Každý potom může libovolnou informaci zašifrovat veřejným klíčem tak, že rozšifrovat je možné jedině soukromým klíčem. Další aplikací je právě elektronický podpis využívaný i bitcoinové síti – uživatel svým soukromým klíčem podepíše transakci (tedy informace o tom jaký obnos komu posílá) a každý kdo zná veřejný klíč potom může ověřit autenticitu a integritu této informace (tedy to, že informaci skutečně zaslala osoba se znalostí soukromého klíče i to že ji zaslala

vychází z povahy elektronické mince, která je ve své podstatě informací, a je proto možné ji libovolně kopírovat. Problémem, který zůstával dlouho nevyřešen je, jak zamezit takzvanému dvojitému utrácení<sup>14</sup>. Tedy jak je možné zajistit, aby ten od koho transakce vychází neposlal tutéž minci na více adres současně. V tradičních platebních systémech je tento problém řešen existencí centrální autority (například banky), která rozhoduje o pořadí provedení transakcí, ověřuje, zda má uživatel dostatečný zůstatek na účtu a rozhoduje o tom, jestli je uživatel oprávněn takovou transakci provést. Jak už jsme si řekli, architektura bitcoinového systému je řešena tak, aby zde vůbec nevznikala potřeba centrální autority. Na její místo tedy nastupuje *blockchain*. Každá transakce je považována za ověřenou, definitivní, až v okamžiku, kdy se dostane do tohoto veřejného záznamu transakcí. V případě že by se někdo pokusil utratit minci vícekrát, za platnou bude systém považovat jen tu z více transakcí, které se podařilo dostat do *blockchainu* – ostatní budou systémem ignorovány.

Těžaři, tedy uživatelé kteří pracují na tvorbě záznamu, mezi sebou soupeří o to, komu se jako prvnímu podaří nalézt řešení výpočetně náročného matematického problému, jehož řešení, v okamžiku kdy bylo nalezeno, je možné snadno a rychle ověřit. Jako odměnu inkasují transakční poplatky (relativně velmi nízké a v zásadě dobrovolné) a oprávnění uvolňovat do oběhu nové mince při každém úspěšném připojení nového bloku transakcí do záznamu (pro tuto skutečnost se používá termín „*nalezení bloku*“) – odtud právě pramení název blockchain – řetěz bloků<sup>15</sup>.

Soupeření mezi jednotlivými těžaři zde plní funkci decentralizované tvorby rozhodnutí. Předpokládá se totiž, že většina z nich má zájem na spolehlivém fungování sítě, která jim generuje zisk. Většina z nich tedy vytváří poctivý záznam transakcí. K tomu, aby některý těžař mohl síť zneužít a efektivně pozměňovat záznamy, musel by mít k dispozici výrazně větší výpočetní výkon než celý zbytek sítě dohromady. I v takovém případě by mohl pouze vracet zpět své transakce a blokovat transakce ostatních uživatelů, nikoli vytvářet mince z ničeho, nebo podvrhovat transakce ostatních uživatelů (k tomu by musel znát jejich soukromé klíče). I v nepravděpodobném případě, že by k

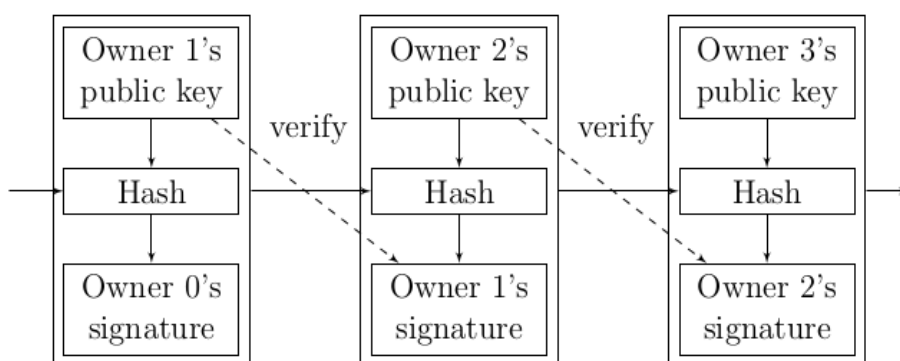
---

přesně v podobě v jaké se ke druhému uživateli dostala)

<sup>14</sup>angl. double-spending

<sup>15</sup>NAKAMOTO, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2008. Dostupné z: <https://bitcoin.org/bitcoin.pdf>

podobné situace došlo, by byl takový těžař motivován pokračovat v poctivé tvorbě záznamu: Vzhledem k tomu že, by inkasoval většinu odměn za nalezené bloky, dá se předpokládat, že by raději vydělával na těchto odměnách, než aby podkopal důvěru v systém, který mu generuje zisk.



Obr. 1: Tento diagram popisuje transakce v bitcoinovém systému. Uživatel číslo 1 pošle minci uživateli číslo 2 tak, že vezme jeho veřejný klíč, připojí k němu digitální otisk (hash) předchozí transakce a to celé podepíše svým soukromým klíčem. Jak napsal Satoshi Nakamoto ve své původní práci, elektronickou minci tak lze definovat jako řetěz digitálních podpisů. (zdroj: DRAINVILLE, Danielle. *An Analysis of the Bitcoin Electronic Cash System*. [online]. 2012 [cit. 2014-06-14]. Dostupné z: <https://math.uwaterloo.ca/combinatorics-and-optimization/sites/ca.combinatorics-and-optimization/files/uploads/files/Drainville,%20Danielle.pdf> )

V předchozím odstavci jsme napsali, že existuje veřejně přístupný záznam o historii a stranách proběhlých transakcí, přesto bývá bitcoinový platební systém označován za anonymní resp. pseudonymní. Je tomu tak proto, že strany transakce jsou určeny pouze pomocí *bitcoinových adres*, řetězců 27-34 alfanumerických znaků začínajících číslem 1 nebo 3, které odpovídají vygenerovaným šifrovacím klíčům. Typická adresa pak vypadá například takto „18yDTWqDSZxMVdYGxQveea2ZK3X4qnegbW“<sup>16</sup>. Tyto adresy však, narozdíl například od čísel bankovních účtů, nejsou v samotném systému nijak spojeny s údaji o skutečné identitě uživatele, v tomto smyslu tedy chápeme pseudonymitu systému. Tato skutečnost představuje způsob, jak lze zajistit vysokou úroveň ochrany soukromí uživatelů, navzdory veřejné povaze historie provedených

<sup>16</sup>Viz <https://en.bitcoin.it/wiki/Address>

transakcí. Současně je však také zdrojem obav před zneužíváním systému k praní špinavých peněz a jiným nekalým aktivitám.

## **1.4. Decentralizovaná povaha bitcoinového systému, implikace této skutečnosti**

Již před vynálezem bitcoinu existovaly mnohé způsoby, jak zasílat peněžní hodnotu přes komunikační kanál – příkladem může být běžné používané internetové nebo telefonické bankovníctví, poštovní poukázky, terminály pro platební a kreditní karty a podobně. Všechny takové systémy ale měly jednu společnou vlastnost a tou je existence třetí strany – prostředníka, který zajišťuje převod od jedné strany transakce k druhé. Tato strana je současně také autoritou, která má faktickou moc rozhodovat o tom zda transakce proběhne. Takový systém navíc stojí a padá s finanční institucí která je prostředníkem – v okamžiku, kdy z nějakého důvodu přestane transakce zpracovávat, (ať už proto, že se ocitne ve stavu přechodného nedostatku likvidity, je jí odebrána licence, nebo třeba její budovy zachvátí požár) celý systém přestává fungovat. Naproti tomu v bitcoinovém systému nelze rozlišit centra, jejichž pád by mohl ohrozit fungování systému.

Decentralizace je tu zdrojem stability a odolnosti proti případnému útoku (a to zcela bez ohledu na to zda je takový zásah v souladu s platným právem - tedy zda jde například o výkon soudního rozhodnutí, či nikoli). Právě tato nezávislost na státních orgánech a finančních institucích, které podléhají státnímu doзору a z toho pramenící odolnost vůči vnějším zásahům je pro mnohé zásadním argumentem pro jeho užívání. Stejně tak se však objevují i hlasy, které označují samotnou existenci systému s takovými vlastnostmi za vysoce společensky nebezpečnou.

Výmluvným příkladem odolnosti decentralizovaných systémů proti zásahům zevnějšku je například peer-to-peer protokol BitTorrent. Jedná se o technologii umožňující sdílení souborů přes internet za absence centrálního serveru tak, že soubory jsou uloženy na počítačích uživatelů, kteří si je kousek o kousek navzájem rozesílají. Ačkoliv je protokol v současné době masově využíván k neoprávněnému šíření děl chráněných autorskými právy a samotná existence systému je trnem v oku sdružením na

ochranu autorských práv, zásahy se omezují na občasnou perzekuci provozovatelů webových stránek s vyhledávací chráněného obsahu a v podstatě náhodných uživatelů na základě žalob podaných vykonavatelí autorských práv. Systém jako takový je totiž roztržštěn mezi jednotlivé uživatele po celém světě a účinný zásah proti síti jako celku je tak v podstatě vyloučen<sup>17</sup>.

## **1.5. Emise a tržní cena bitcoinu**

Další zásadní charakteristikou bitcoinového systému je způsob, kterým probíhá jeho emise. Zejména od národních měn se liší tím, že množství bitcoinu v oběhu je předem možné velice přesně předvídat, je totiž řízena počítačovým algoritmem, který tvoří základ sítě. Naproti tomu u národních měn, bývá množství peněz v oběhu upravováno dle uvážení centrální banky, a může tak dojít (a již vícekrát v historii také došlo) ke znehodnocení měny hyperinflací či měnovou reformou. I tento fakt může pro bitcoin představovat konkurenční výhodu, zvláště v případech, kdy je důvěra v instituci emitující peníze nabořána.

---

<sup>17</sup>HELTON, Matthew. Secondary Liability for Copyright Infringement: BitTorrent as a Vehicle for Establishing a new Copyright Definition for Staple Articles of Commerce. *Columbia Journal of Law and Social Problems*. 2007, č. 40.

Obr. 3: Ilustrace množství bitcoinu v oběhu, na ose x roky, na ose y miliony bitcoinů v oběhu. Vidíme že rychlost emise se zpomaluje, až se okolo roku 2033 zastaví na celkových 21 milionech BTC (Zdroj: Wikimedia Commons, [http://upload.wikimedia.org/wikipedia/commons/5/54/Total\\_bitcoins\\_over\\_time.png](http://upload.wikimedia.org/wikipedia/commons/5/54/Total_bitcoins_over_time.png))

Zatímco množství bitcoinu v oběhu je pevně řízeno jeho algoritmem, jeho cena se odvíjí pouze od nabídky a poptávky na trhu a podléhá velice silným výkyvům (v některých případech to byly i desítky procent během jednoho dne). To lze přičítat jednak tomu, že se jedná o poměrně velmi mladou technologii s relativně malou uživatelskou základnou<sup>18</sup>. Jeho cena začínala fakticky na nule, a od té doby se vyšplhala až na současných asi 13 000 Kč za 1 BTC<sup>19</sup>. Je však nutné si uvědomit, že v případě objevení zásadní slabiny v systému, účinně vymáhaného zákazu jeho používání nebo

---

<sup>18</sup>HURST, Brandon. How many people really own bitcoins - and why does it matter?. *BitScan* [online]. 2014 [cit. 2014-06-04]. Dostupné z: <http://bitscan.com/bitnews/item/how-many-people-really-own-bitcoins-and-why-does-it-matter>

<sup>19</sup>Viz například <https://www.bitstock.cz/> - česká burza s bitcoiny.

nástupu vývojově dokonalejšího systému může jeho cena velice dramaticky spadnout na hodnoty na kterých začínala.

*Obr. 4: Tržní cena jednoho bitcoinu v US dolarech od jeho počátku. Na první pohled poněkud nešťastný formát je zvolen proto, aby bylo vidět jak dlouho se cena pohybovala na hodnotách blízkých nule. V únoru 2011 pak cena bitcoinu dosáhla parity s americkým dolarem. Na grafu je hezky vidět, jak během roku 2013 cena prudce narostla až na jeho konci překonala 1000 USD. Poté následoval prudký pád. V současné době (červen 2014) se pohybuje okolo 550 USD za jeden 1 BTC*

## 1.6. Odvozené platební systémy

Licence pod kterou je uvolněn zdrojový kód bitcoinu (MIT license) umožňuje bez právních překážek snadno vytvářet odnože a modifikace tohoto systému. Od doby jeho vzniku se objevilo více než sto<sup>20</sup> odvozených systémů. Tyto systémy, souhrnně označované jako altcoiny (alternative-coins), ať se již jedná o litecoin, peercoin, quark, namecoin, dogecoin, nebo jakýkoli jiný, se od bitcoinového platebního systému ve větší či menší míře odlišují (například ve způsobu, jakým jsou emitovány peněžní jednotky, použitých matematických a kryptografických funkcích, mechanismu a rychlosti potvrzování transakcí), vychází však do značné míry z počítačových algoritmů bitcoinového systému, nebo z konceptů které jsou v něm implementovány – spoléhání na decentralizované P2P síť, decentralizovaná tvorba záznamu transakcí, kryptografie veřejného klíče a další<sup>21</sup>.

---

<sup>20</sup><http://coinmarketcap.com/all.html>

<sup>21</sup>BOŘÁNEK, Romanp. Bitcoin a ti druzí: Přehled zajímavých kryptoměn. *Root.cz* [online]. 2013 [cit. 2014-04-04]. Dostupné z: <http://www.root.cz/clanky/bitcoin-a-ti-druzi-prehled-zajimavych-kryptomen/#ic=articles-related&icc=item-3G>



Jejich právní režim bude obdobný bitcoinu do té míry, do jaké se jeho mechanismy podobají mechanismům použitým v bitcoinovém platebním systému. Bitcoin je však prvním a v současné době stále nejvýznamnějším zástupcem těchto tzv. kryptoměn<sup>22</sup> (ačkoliv se lze zcela rozumně domnívat že v budoucnu může být jeho místo přejato jinou, technicky dokonalejší alternativou) a právě proto se zde budeme zabývat právě bitcoinem, ačkoliv značná část textu bude stejně dobře použitelná i pro podobné systémy.

V případě vzniku nové právní úpravy, která by upravovala tyto technologie by pak bylo dle mého názoru dobré zohlednit absenci překážek a s tím související nekontrolovatelnost a rychlost s jakou vznikají od bitcoinu odvozené systémy a užívat proto v právních normách abstraktní definice s výčtem znaků upravovaných systémů, spíše než například techniky uzavřeného výčtu systémů formou podzákoného předpisu.

## **2. Otázka souladu bitcoinového systému s právním řádem**

Otázkou zda je bitcoin legální, budeme rozumět otázku, zda je legální chování subjektů práva spočívající v účasti na bitcoinové síti. Měli bychom chápat, že v užším, technickém slova smyslu, jsou účastníky jakékoli počítačové sítě jedině navzájem komunikující počítače, které ovšem nejsou subjekty práva. Jejich účast je však důsledkem chování, většinou dokonce úmyslného jednání, subjektů práva, a právě takové chování budeme v této práci nadále rozumět účastí na bitcoinové P2P síti a platebním systému (což je v zásadě jedno a totéž).

Faktem ovšem je, že v úzké souvislosti s účastí na bitcoinové síti se vyskytují i jednání, která nabývají různých rozmanitých forem a jejichž soulad s právním řádem je nutné posuzovat zvlášť: Od samotného přijímání či poskytování plateb v bitcoinech, směny bitcoinu za jinou formu peněz či zboží, spekulativního obchodování s bitcoinem, až po odvádění nebo naopak neodvádění daně z příjmu ve formě bitcoinů, legalizování výnosů z trestné činnosti a obchodování s omamnými a psychotropními látkami.

---

<sup>22</sup>kryptoměny proto, že v procesu autorizace, přenosu a tvorby záznamu spoléhají na poznatky z kryptografie.

Podle autorů učebnice teorie práva budeme chápat pojem legality následovně: „Legální jsou vztahy a chování, které jsou v souladu s platným právem, ilegální ty, které jsou s ním v rozporu. Při hodnocení z hlediska legality se vztahy a chování měří právě jen platným právem<sup>23</sup>“

Právní řády vyspělých právních států vychází ze zásady legální licence, tedy pravidla, že legální je vše, co není právní normou výslovně zakázáno.

V českém právním řádu je tato zásada zakotvena v Čl. 2 odst. 3 Listiny základních práv a svobod, který stanoví že: „Každý může činit, co není zákonem zakázáno, a nikdo nesmí být nucen činit, co zákon neukládá“<sup>24</sup>. Na první pohled shodnou normu obsahuje také Čl. 2 odst. 4 Ústavy ČR, který však ve své dispozici obsahuje pojem občan, nikoli každý.

Z toho můžeme vyvozovat, že účast na bitcoinovém platebním systému, jeho vývoj a použití je na celém území ČR (a obdobně i v jiných státech) legální, pokud není jinou právní normou stanoveno jinak.

## **2.1. Existence norem zakazujících účast na bitcoinovém platebním systému**

Dle mého názoru v současné době není součástí právního řádu České republiky obecně závazná norma, která by reflektovala existenci bitcoinu (ani jiného jemu podobného platebního systému), natož taková, která by zakazovala účast na něm – a to ani implicitně. Nebo se mi přinejmenším nepodařilo žádnou takovou právní normu nalézt.

Ochrana měny je v České republice upravena Zákonem č. 6/1993., o České národní bance. Ten v §16a odst. 1 stanoví že:

*„Nikdo nesmí vyrábět, dovážet, nabízet, prodávat nebo jinak rozšiřovat medaile, žetony nebo podobné předměty, které jsou svým provedením způsobilé uvést jejich držitele v*

---

<sup>23</sup>BOGUSZAK, Jiří, Jiří ČAPEK a Aleš GERLOCH. *Teorie práva*. 2., přeprac. vyd. Praha: ASPI, 2004, s. 208. ISBN 8073570300.

<sup>24</sup>Ústavní zákon č.2/1993 Sb.,o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky.

*omyl, že jde o mince nebo pamětní mince určité nominální hodnoty vydávané Českou národní bankou.“*

Bitcoin, vzhledem ke své elektronické podstatě, není v žádném případě způsobilý uvést držitele v takový omyl. Proto toto ustanovení nelze chápat jako zákaz účasti na bitcoinové síti.

Druhý odstavce pak stanoví že:

*„Nikdo nesmí při označení nebo popisu žetonu, medaile nebo podobného předmětu v souvislosti s jejich nabízením, prodejem nebo jiným rozšiřováním použít slovo „mince“.“*

Aplikace tohoto odstavce bude záviset na posouzení, zda lze bitcoin subsumovat pod pojem *„žeton, medaile nebo podobný předmět“*. Dle mého názoru to možné není neboť elektronicky uchovávaná informace tvořící podstatu bitcoinového systému (šifrovací klíče, záznamy v blockchainu) není předmětem podobným žetonu či medaili. I v případě, že by převládlo pojetí bitcoinu jako takového předmětu, v rozporu se zákonem by se ocitalo jen samotné použití slova „mince“ v souvislosti s nakládáním s ním, nikoli samotné nakládání.

### **3. Zařazení bitcoinu do existujících právních kategorií**

Při pokusu zařadit bitcoin do určitého právního rámce bude důležité vycházet z již existujících, právem upravených kategorií.

Zařazení bitcoinu do kategorií zavedených platným právem je však problematické vzhledem k tomu, že v době vzniku relevantních norem bitcoinový platební systém (a systémy jemu podobné) ještě neexistoval a s jejich existencí nepočítala ani právní teorie, ani zákonodárce.

V následující kapitole se pokusíme vyložit si některé z kategorií, které připadají v úvahu, avšak uvidíme, že ačkoliv bitcoin má mnohé charakteristiky typické pro relevantní právní kategorie u většiny z nich bude chybět některý ze znaků, nutných pro jeho bezpodmínečné zařazení do té či oné kategorie. I v takovém případě však, za

dodržení obecných pravidel konkrétního právního odvětví, bude připadat v úvahu použití analogie.

Nyní si tedy rozebereme některé základní kategorie, které sdílí společné znaky s bitcoinovým platebním systémem a zjistíme zda, a do jaké míry, je možné ho do nich zařadit.

### **3.1. Kategorie věci v právním slova smyslu**

Zdaleka nejširší kategorií, o které budeme zjišťovat, zda do ní bitcoin lze či nelze zařadit je kategorie věci v právním slova smyslu. Rozhodnout o otázce jeho příslušnosti k této kategorii bude zásadní pro určení jeho postavení v rámci právního řádu, neboť bude rozhodovat o faktu, zda na něj dopadá rozsáhlá, byť neurčitá množina právních norem. Jedná se o všechny právní normy, které ve své hypotéze (být tacitně a implicitně) předpokládají věc v právním slova smyslu. Rozhodnutí o této otázce bude důležité pro určení povahy mnoha společenských vztahů vznikajících v souvislosti s použitím bitcoinového platebního systému: zda se jedná o právní vztahy, nebo vztahy právem nerefléktované a neupravené.

Pojem věci je pojmem jehož vnímání je proměnlivé a liší se v historickém období, území i osobu od osoby.

Obdobně se vyvíjí i pojem věci v právním slova smyslu, ten však je právním institutem, jeho obsah je určen platnými právními normami a umožňuje nám ho poměrně přesně vymezit na každém území, v konkrétním čase.<sup>25</sup>

V poslední době došlo i u nás k proměně významu věcí v právním slova smyslu v souvislosti s rekonstrukcí soukromého práva. Liší se tedy pojetí věci podle starého občanského zákoníku č. 40/1964 a nového občanského zákoníku č. 89/2012 Sb. Ačkoliv jsem původně měl v úmyslu rozebrat postavení podle starého i nového občanského zákoníku, vzhledem k tomu, že starý občanský zákoník již není součástí právního řádu České republiky, spokojíme se s výkladem podle nového občanského zákoníku.

Již na začátku práce jsme si vysvětlili, že pojem bitcoin lze chápat dvěma způsoby. Prvním ho chápeme jako platební systém, který umožňuje zasílat a přijímat

---

<sup>25</sup>srov. ELIÁŠ, Karel a kol. Občanský zákoník: velký akademický komentář: úplný text zákona s komentářem, judikaturou a literaturou podle stavu k 1. 4. 2008. Praha: Linde, 2008. 1. sv. Zákony - komentáře. ISBN 978-80-7201-687-7, s. 466-468.

platby, pro toto pojetí zde zavádíme pojem *bitcoinový platební systém*. Druhým způsobem pak bitcoin chápeme jako druh peněz, který může být sekundárním předmětem právních vztahů. Právě pro druhé posouzení bude důležité odpovědět na otázku, zda je bitcoin věcí v právním slova smyslu, a zda tedy může být předmětem vlastnického práva a práv obdobných.

O tom jak můžeme chápat bitcoin jako věc píše vynálezce bitcoinového systému Satoshi Nakamoto následující: „*Elektronickou minci definujeme jako řetěz digitálních podpisů. Každý vlastník převádí minci na dalšího tím, že digitálně podepíše otisk<sup>26</sup> předchozí transakce a veřejný klíč dalšího vlastníka a tyto přidá na konec mince*“<sup>27</sup>

Každý uživatel má na svém počítači soubor, který obsahuje tyto soukromé klíče, které mu umožňují nakládat s bitcoiny, které jsou na této adrese uloženy. Nemá tedy na svém pevném disku bitcoiny, nýbrž soukromé klíče, kterým podle blockchainu náleží určitý obnos denominovaný v bitcoinech.

Určení, zda je bitcoin věcí v právním slova smyslu podle nového občanského zákoníku by nemělo činit velké obtíže. Ten totiž v ustanovení § 489 stanoví, že věc v právním slova smyslu je „*vše, co je rozdílné od osoby a slouží potřebě lidí.*“

Z toho lze tedy vyvodit dva znaky, které musí určitá skutečnost splňovat, aby bylo možné ji považovat za věc v právním slova smyslu: Prvním je rozdílnost od osoby a druhým užitečnost. Bez dlouhého rozboru je myslím možné tvrdit, že bitcoin jako platební systém i jako elektronická mince je nositelem obou těchto znaků a je tedy nutné ho považovat za věc v právním slova smyslu.

Občanský zákoník však také připisuje věcem další atributy. Dělí tak navíc věci na hmotné a nehmotné, movité a nemovité, zastupitelné a nezastupitelné, zužitelné a nezužitelné.

Hmotná věc podle § 496 je ovladatelnou částí vnějšího světa, která má povahu samostatného předmětu, zatímco nehmotné věci jsou práva jejichž povaha to připouští a jiné věci bez hmotné podstaty. Vzhledem k tomu, že bitcoin je vlastně složen ze zápisu ve veřejném záznamu transakcí a šifrovaných klíčů, které mají podstatu

---

<sup>26</sup>Angl. Hash, tedy výstup hashovacího algoritmu, v českém prostředí bývá označován jako výtah, miniatura, otisk, fingerprint či haš – zdroj. [http://cs.wikipedia.org/wiki/Ha%C5%A1ov%C3%AD\\_funkce](http://cs.wikipedia.org/wiki/Ha%C5%A1ov%C3%AD_funkce)

<sup>27</sup>Nakamoto, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Dostupné z: <https://bitcoin.org/bitcoin.pdf>

několikamístného čísla, dá se dovodit, že jde o informaci - věc bez hmotné podstaty, kterou lze uchovávat zachycenou na hmotném nosiči<sup>28</sup>. Tímto nosičem pak může být jak substrát elektronické povahy, tak třeba list papíru nebo dokonce lidská paměť.

Ustanovení § 498 dělí věci na movité a nemovité. Nemovité věci vymezuje jako „*pozemky a podzemní stavby se samostatným účelovým určením, jakož i věcná práva k nim, a práva, která za nemovité věci prohlásí zákon...*“. Jako movité pak popisuje veškeré další věci ať již je jejich podstata hmotná a nehmotná. Je jasné že právě do druhé kategorie – věcí nehmotných musíme zařadit i bitcoin.

§ 499 stanoví že „*Movitá věc, která může být nahrazena jinou věcí téhož druhu, je zastupitelná; ostatní věci jsou nezastupitelné. V pochybnostech se případ posoudí podle zvyklostí.*“. Vzhledem k tomu, že v bitcoinovém platebním systému nejsou rozlišovány mince různých druhů, musíme konstatovat že se jedná o věc zastupitelnou.

§ 500 dělí věci na uživatelné a neuzivatelné: „*Movitá věc, jejíž běžné použití spočívá v jejím spotřebování, zpracování nebo zcizení, je uživatelná; uživatelné jsou i ty movité věci, které náleží ke skladu nebo k jinému souboru, pokud jejich běžné užití spočívá v tom, že jsou prodávány jednotlivě. Ostatní věci jsou neuzivatelné.*“ Vzhledem k tomu, že typické použití bitcoinu, spočívá téměř výhradně v jejím zcizení (bez ohledu na právní kauzu), považujeme bitcoin za věc uživatelnou.

Posouzení tedy uzavřeme následovně: Bitcoin je skutečně věcí v právním slova smyslu, a to věcí nehmotnou, movitou, zastupitelnou a uživatelnou.

## 3.2. Právní úprava měny a peněz

Další kategorie, které pro bitcoin připadají v úvahu, jsou kategorie *peníze* a *měna*.

Ačkoli tyto termíny bývají v běžné mluvě zaměňovány nejedná se o tutéž věc. Kolektiv autorů z právnické fakulty Univerzity Karlovy, píše o rozdílu mezi pojmem *měny* a *peněz* následující:

„*Zatímco peníze jsou kategorií ryze ekonomickou a bývají často ve stručnosti definovány jako zvláštní druh univerzálního zboží používaného k vyjadřování cen*

<sup>28</sup>VRBÍKOVÁ, Lenia a Jan VYSKOČIL. Právní a daňové aspekty Bitcoinu. In: *Zkušenosti s virtuálními měnami: Bitcoin měna budoucnosti?*. Praha, 2014, s. 137. Dostupné z: <http://ekon.konference.vsmie.cz/zkusenosti-s-virtualnimi-menami/data/program.pdf>

ostatního zboží, ke zprostředkování jeho koupě a prodeje a k provádění různých druhů plateb, měna je kategorií především právní a znamená obecně určitou konkrétní formu nebo druh peněz.

Co však činí peníze měnou, není jen vyšší míra konkrétnosti, skutečnost, že nějaký předmět je za peníze považován, ale především je to určitá autorita, která za konkretizaci příslušné formy peněz stojí, kvalifikovaným způsobem formu peněz jakožto měnu definuje a stanoví podmínky její existence a používání. Touto autoritou je zpravidla stát, který pro své území určuje měnu a její náležitosti jako součást výkonu svrchovanosti nad tímto územím<sup>29</sup>

Vidíme tedy, že k tomu, abychom určitou věc mohli zařadit do kategorie peněz, musí být způsobilá plnit určité funkce. Zjednodušeně tedy můžeme říct že peníze jsou takové věci, které můžeme používat jako peníze.

Oproti tomu měna je podle právní teorie taková forma peněz, která je uznaná ze strany státu nebo obdobného veřejného společenství (například mezinárodní organizace), a která splňuje formální požadavky, které na ní klade právní řád takového společenství.

### 3.2.1. Zařazení bitcoinu pod kategorii peněz

Autoři ekonomických publikací se více či méně shodují, že peníze jsou aktivum způsobilé plnit určité typické funkce. Rozebereme si tedy jaké jsou funkce peněz, a zda a do jaké míry je bitcoin způsobilý tyto funkce plnit.

Peníze jsou zvláštní druh zboží, který umožňuje směnu bez nutnosti existence *párové shody potřeb*<sup>30</sup>. Co to znamená si nejlépe ilustrujeme na příkladu: Představme si prostředí, ve kterém neexistují peníze. Pro směnu jakéhokoli statku za jiný by zde bylo vždy nutné najít osobu, která poptává statek, který my nabízíme a naopak. Pokud by v takovém prostředí žil advokát, který by potřeboval navrhnout dům, musel by najít architekta, který poptává právní pomoc. Tomuto druhu obchodu říkáme *naturální směna*, neboli *barter* a ačkoliv se v omezené míře vyskytuje i v současnosti, byl z velké

<sup>29</sup>BAKEŠ, Milan. *Finanční právo*. 6. upr. vyd. V Praze: C.H. Beck, 2012, s. 335-342. ISBN 978-80-7400-440-7.

<sup>30</sup>DORNBUSCH, Rudiger. *Makroekonomie*. 1.vyd. Praha: SPN, 1994, s. 341. ISBN 80-04-25556-6.

míry vytlačen výrazně praktičtějším používáním peněz, jakožto univerzálního zboží. Naturální směna totiž vyvolává příliš vysoké transakční náklady (čas a úsilí na nalezení někoho kdo je ochotný směnit zboží které poptáváme za zboží které nabízíme).

V tomto smyslu jsou peníze velkým vynálezem, neboť umožňují pokročilou dělbu práce (*specializaci*)<sup>31</sup>. Ve skutečnosti by se tedy v prostředí bez peněz žádní advokáti ani architekti nebyli, neboť by taková ekonomika neumožnila dostatečnou dělbu práce k tomu, aby se vyvinuly tyto profese.

Aktiva plnící funkci peněz přitom mohou nabývat množství rozmanitých forem: „*Ekonomové používají výraz peníze pro jakékoli aktivum, které se může použít k nákupu. ... V historii sloužily jako peníze nejrůznější předměty od zlatých a stříbrných mincí až po mušle, korálky a na ostrově Yap nepřemístitelné balvany*“<sup>32</sup>

Forma, kterou peníze nabývají, v historii prochází postupným vývojem. Lze přitom rozlišit několik významně odlišných vývojových fází:

První předměty, plnící funkci peněz, byly hmotné předměty s vnitřní hodnotou, jejichž vlastnosti (relativní vzácnost, snadná manipulace, dělitelnost apod.) je předurčovaly k použití jako prostředku směny – takzvané *komoditní peníze*. Vnitřní hodnotou vlastně rozumíme fakt, že takové peníze lze, kromě jejich použití jako protihodnoty ve směně, využít i jiným způsobem (například je sníst, nebo z nich vyrábět nástroje).

Další vývojovou fází pak byly plnohodnotné peníze z drahých kovů (zlato, stříbro, měď), které však stále představovaly předmět s vlastní, vnitřní hodnotou (zlatou minci je pořád možné roztavit a vyrobit z ní šperky).

Odtud se postupně dostáváme do další fáze, kdy se již objevují peníze ve formě bankovek – cenných papírů, které představují vklad v bance splatný na viděnou, a které je mohou samostatně plnit funkce peněz. Tyto peníze, ačkoliv již nemají samy o sobě jiné než peněžní využití, jsou stále provázány s komoditou, kterou jsou takzvaně kryty<sup>33</sup>.

Další fází ve vývoji peněz jsou státem vydávané bankovky nekryté zlatem (tzv.

---

<sup>31</sup>HOLMAN, Robert. *Ekonomie*. 5. vyd. V Praze: C.H. Beck, c2011, s. 448. Beckovy ekonomické učebnice. ISBN 978-80-7400-006-5.

<sup>32</sup>FRANK, Robert H. *Ekonomie*. 1. vyd. Praha: Grada, 2003, s. 581. Profesionál. ISBN 80-247-0471-4.

<sup>33</sup>V angličtině se používá výraz commodity-backed money



*fiat peníze*<sup>34</sup>, které jsou ve svém státě penězi s nuceným oběhem. Jejich hodnota je tu vlastně stanovena právními normami státu, který bývá současně i jejich emitentem (i když tato podmínka není zcela nutná, stát jistě může uznat jako měnu i peníze, které sám neemituje, ztrácel by tak však kontrolu nad množstvím peněz v oběhu). Ochota subjektů je přijímat je vlastně důsledkem státního donucení.

F. A. von Hayek o tom píše následující: „*Ve svém striktně právním významu neznamená 'zákonné platidlo' nic víc, než že věřitel nemůže odmítnout přijetí dluhu ve vládou<sup>35</sup> emitovaných penězích*“<sup>36</sup>

V České republice jsou tímto zákonným platidlem mince a bankovky vydávané Českou národní bankou, denominované v korunách, o nichž zákon stanoví, že jde o „*zákonné peníze ve své nominální hodnotě při všech platbách na území České republiky*“<sup>37</sup>.

Bankovky amerického dolaru mají na sobě dokonce přímo vytištěno že se jedná o „*zákonné platidlo pro všechny dluhy, soukromé i veřejné*“<sup>38</sup>).

V další vývojové fázi se již objevují peníze nabývající formy nehmotných předmětů. Jedná se o bezhotovostní (žirální) a elektronické peníze. Obdobným způsobem jako komoditou kryté peníze představovaly závazek vůči jejich vydavateli denominovaný v komoditě, představují tyto peníze závazek emitenta denominovaný ve fiat měně – zůstatek na účtu v bance nebo u poskytovatele platebních služeb.

Typickou vlastností peněz je jejich hodnota. Ta spočívá v ochotě lidí je přijímat jako platbu za zboží. Tato ochota pak pramení z důvěry, že přijaté peníze si svoji hodnotu uchovají, tedy že i nadále budou při směně přijímány jako protihodnota za zboží.

Peníze jsou tedy určitou společenskou konvencí, bez ohledu na konkrétní formu, kterou v té či oné společnosti nabývají. Trefně tuto skutečnost shrnul Robert Holman ve

---

<sup>34</sup> fiat znamená v latině „budiž“ - označuje tak fakt, že stát prostřednictvím právní normy stanoví, jaké předměty bez vlastní, vnitřní hodnoty jsou zákonnými penězi na jeho území a jejich znaky.

<sup>35</sup>Výraz vláda je tu použit v extenzivním významu, ve většině zemí totiž není emitentem měny vláda jako orgán moci výkonné, ale na vládě relativně nezávislá centrální banka. Jako vhodnější by se tedy jevil výraz *státem emitované peníze*.

<sup>36</sup> HAYEK, Friedrich August von. *Soukromé peníze: Potřebujeme centrální banku?*. Praha: MegaPrint, 1999, s. 41. ISBN 8090270115.

<sup>37</sup>Zákon České národní rady o České národní bance č. 6/1993, §16 odst. 1

<sup>38</sup>konkrétně jde o nápis: „THIS NOTE IS LEGAL TENDER FOR ALL DEBTS, PUBLIC AND PRIVATE“

své učebnici ekonomie: „*Nezáleží na tom z čeho jsou peníze dělány, nýbrž na tom, že lidé věří že budou ve směně přijímány.*“<sup>39</sup>

Bitcoin je však v některých znacích fundamentálně odlišný od všech výše zmíněných forem peněz, buď se tedy nejedná vůbec o peníze, a nebo jde o nový druh peněz, představující další vývojovou fázi. Pokud však je další vývojovou fází, neznamená to samo o sobě že se udrží a prosadí v platebním styku, může se pochopitelně jednat o slepou vývojovou větev, která z nějakého důvodu zanikne.

Vzhledem k výše uvedenému tedy můžeme tvrdit, že peníze jsou aktiva, schopná plnit určité funkce. Pro rozhodnutí, zda můžeme bitcoin zařadit do kategorie peněz, tedy bude nutné testovat jeho způsobilost plnit funkce peněz. Všichni výše citovaní autoři se vesměs shodují na tom, že se jedná o následující funkce:

- Funkce obecného denominátoru hodnoty
- Všeobecného prostředku směny
- Všeobecného prostředku plateb a převodů kapitálu
- Nositele a prostředku uchování hodnoty

### **Bitcoin jako obecný denominátor hodnoty:**

Peníze v této funkci vystupují jako měřítko hodnoty ostatního zboží a statků – jsou schopny vyjadřovat hodnotu jiného zboží a umožňovat jeho porovnávání.

Přestože bitcoin je teoreticky způsobilý tuto funkci plnit, vzhledem k jeho vysoké volatilitě<sup>40</sup> (která je ovšem u tak mladé technologie poměrně pochopitelná) jí běžně neplní.

Doložíme si to na následujícím schématu, které se běžně vyskytuje při prodeji zboží a služeb za bitcoiny: Prodávající vede cenu v některé měně a tu pak pro účely platby v bitcoinu přepočítává podle aktuálního kurzu. Ukázkou může být jeden z největších online prodejců zboží přijímajících bitcoiny, *Bitcoinstore.org*, ten v okamžiku

---

<sup>39</sup>HOLMAN, Robert. *Ekonomie*. 5. vyd. V Praze: C.H. Beck, c2011, s. 448. Beckovy ekonomické učebnice. ISBN 978-80-7400-006-5.

<sup>40</sup>Tzn. míře kolísání jeho hodnoty

uzavření obchodu vynásobí cenu zboží v dolarech aktuálním kurzem bitcoinu a tuto cenu garantuje pouze následujících 15 minut<sup>41</sup>. Je tedy vidět, že k plnění funkce denominátoru hodnoty je sice bitcoin teoreticky způsobilý, avšak aby tuto funkci mohl opravdu začít spolehlivě plnit, muselo by nejprve dojít ke stabilizaci jeho hodnoty, v poměru k jiným formám peněz.

### **Bitcoin jako všeobecný prostředek směny:**

Peníze v této funkci umožňují nákup a prodej zboží, služeb a jiných statků. Mluvíme o nich v této souvislosti jako o oběživu, neboť obíhají v rámci trhu – v opačném směru než statky za které jsou směňovány. Mohou takto nabývat libovolné formy, od hotovostní (bankovky a mince) přes bezhotovostní (tedy uložené na účtech finančních institucí) až po peníze elektronické (elektronicky uchovávaná hodnota, která představuje závazek emitenta vůči jejich vlastníkovi, a kterou lze používat k provádění plateb vůči jiným osobám)

První zaznamenanou transakcí tohoto typu prostřednictvím bitcoinu byla koupě pizzy, kterou v květnu roku 2010 uskutečnil Floridský programátor za cenu 10 000 BTC<sup>42</sup>. V dnešní době je již možné za bitcoiny pořídit široké spektrum služeb a zboží a přestože podnikatelé přijímající bitcoin jsou stále spíše výjimkou, jejich počet neustále narůstá a to zejména v prostředí internetu.

Povaha bitcoinu – tedy rychlost transakce a nízké transakční náklady ho předurčují k použití tam, kde jiné způsoby platby jsou příliš pomalé, nebo mají nepřiměřené náklady v poměru k objemu transakce – například stále narůstající množství organizací a autorů publikujících na webu přijímá dary a příspěvky na činnost ve formě bitcoinu. Bitcoin umožňuje efektivně zasílat a přijímat i velmi nízké částky. V současné době je dělitelný na 8 desetinných míst a při současné ceně okolo 12 000 Kč za 1 BTC tak lze teoreticky poslat ekvivalent 0.012 haléřů (0.00000001 BTC označovaný po zakladateli bitcoinu jako 1 Satoshi). Bitcoinový protokol a software,

---

<sup>41</sup><http://www.bitcoinstore.com/faq>

<sup>42</sup><http://historyofbitcoin.org/>

který ho implementuje, je však v případě potřeby možné upravit, takže jeho dělitelnost je potenciálně neomezená, což se může projevit jako velice praktické v případě že by jeho cena dále strmě stoupala.

Přestože zdaleka není konvenčním platebním prostředkem, míst, na kterých lze bitcoin použít k (zejména online) nákupu zboží nebo služeb přibývá<sup>43</sup> a i někteří velcí hráči na trhu (například elektronická aukční síť eBay) zvažují jeho zavedení.<sup>44</sup>

Tuto funkci tedy bitcoin plní, a v některých ohledech a pro některé typy transakcí může být vhodnější než konvenční prostředky směny.

### **Bitcoin jako všeobecný prostředek plateb a převodu kapitálu**

Neboli platidlo. Označuje způsob použití peněz k převodu hodnot a kapitálu. Zatímco v předchozím odstavci jsme se bavili o realizační metodě finanční činnosti (bitcoin za zboží), v tomto máme na mysli metodu návratnou a nenávratnou. Při návratné metodě můžeme uvažovat bitcoin jako předmět úvěru, při nenávratné pak jako peněžní prostředky odváděné zejména do veřejných rozpočtů formou daní, poplatků, peněžitých plnění na základě rozhodnutí soudu apod. Tuto funkci dnes bitcoin obecně neplní, i když se nedá říct že by existovaly závažné okolnosti bránící jeho využití tímto způsobem.

### **Bitcoin jako nositel a prostředek uchování hodnoty**

Tato funkce peněz bývá též označována (přiléhavě, i když poněkud archaicky) jako funkce pokladu. Znamená, že peníze můžeme uložit a po určité době je opět použít s tím, že jejich hodnota zůstane zachována. Vzhledem k tomu že hodnota peněz pramení z ochoty účastníků trhu, byť by byla určená zákonnou povinností, přijímat je jako platbu za zboží. Aktivum, které má plnit funkci pokladu musí splňovat předpoklad, že v

---

<sup>43</sup>katalog míst kde lze platit bitcoiny je dostupný například na <http://usebitcoins.info/> či <http://spendbitcoins.cz/>

<sup>44</sup>EBay considering accepting bitcoin as payment. In: *CNBC International* [online]. 2014 [cit. 2014-02-21]. Dostupné z: <http://www.cnbc.com/id/101356642>

okamžiku, kdy ho držitel bude chtít opět uvést do oběhu, bude tato ochota stále zachována.

Ukazuje se, že tuto funkci již peníze nabývající formy národních měn plní jen do určité míry, nemají totiž vlastní, vnitřní hodnotu v nich obsaženého drahého kovu, jako původní měny emitované neúvěrovou metodou a pro jejich charakter peněz je určující jejich právní status. Ten je ovšem proměnlivý v čase tak, jak jsou proměnlivé normy které ho stanovují.

Bitcoin je podobný měnám krytým zlatem a komoditním penězům v tom smyslu, že jeho hodnota vyplývá z omezené dostupnosti určitého zdroje (ačkoli virtuálního) spíše než z diskreční pravomoci instituce, která je pověřena emisí dané formy peněz.

Bitcoin je emitován podle předem nastavených pravidel protokolu a rychlost jeho emise postupně klesá, až se, okolo roku 2029, zastaví na celkovém množství 21 milionů bitcoinů.

Fakt, že lze do budoucna velmi přesně odhadovat množství bitcoinů v oběhu neznamena, že by bylo možné dobře odhadovat hodnotu bitcoinu v budoucnosti. Jeho cena je podobně jako např. cena zlata určována jen nabídkou a poptávkou. Zatímco poptávka po blýskavém žlutém kovu je už několik tisíc let stabilně vysoká (což souvisí i s tím že je možné jeho nepeněžní využití, jako u ostatních komoditních peněz), u bitcoinu existuje několik scénářů, které mohou poptávku po něm drasticky snížit a jeho cenu tak vrátit do hodnot na kterých začínal (tedy vlastně na nulu). Tyto scénáře sahají od relativně nepravděpodobných (například efektivně vymáhaného zákazu používání bitcoinu napříč mezinárodním společenstvím resp. internetovou počítačovou sítí, objev zásadní a neopravitelné slabiny v systému) až po poměrně pravděpodobné a předvídatelné (konkurence vývojově dokonalejšího systému).<sup>45</sup>

Z těchto důvodů se dá tvrdit, že ačkoliv je bitcoin způsobilý uchovávat hodnotu v čase, z dlouhodobého hlediska nemůže tuto funkci zastávat příliš spolehlivě neboť alespoň prozatím nelze předvídat jaká bude jeho hodnota v budoucnosti.

---

<sup>45</sup>GRINBERG, Reuben. Bitcoin: An Innovative Alternative Digital Currency. *Hastings Science and Technology Law Journal*. 2014, 4:1.

V tomto ohledu je ale nutné podotknout, že funkci pokladu pro něj původně nikdo nezamýšlel, bitcoin byl od počátku určen pouze k uskutečňování plateb online. O tom, že by měl plnit funkci prostředku uchování hodnoty se nikde v dokumentu běžně nazývaném jako *original Bitcoin paper*, zveřejněném jeho vynálezcem Satoshi Nakamotem nedočteme<sup>46</sup>

### **Lze tedy bitcoin považovat za peníze?**

Někteří u peněz akcentují jejich atribut všeobecnosti: například autoři publikace *Peněžní ekonomie a bankovníctví* tvrdí o penězích toto:

*„Důležitý je aspekt všeobecnosti – zde v tom smyslu, že dané aktivum je přijímáno všemi subjekty dané společnosti. Pokud tomu tak není, nejde o peníze, nýbrž pouze o jejich neumělou a obvykle jen časově velmi omezenou náhražku“<sup>47</sup>*

Není mi příliš jasné, v jakém smyslu absence všeobecnosti dělá z peněz jejich neumělou a časově omezenou náhražku, ale pokud bychom chápali tuto větu doslovně stačil by jeden člen dané společnosti, který nepřijímá dané aktivum k tomu, aby se nedalo považovat za peníze. Ačkoli chápu roli, kterou hraje u peněz všeobecnost, přikláním se k názoru, že při posouzení zda je dané aktivum penězi či ne, je důležitější jeho způsobilost být všeobecným prostředkem k plnění funkcí peněz, než to jestli tuto funkci fakticky zastává.

Naopak se zde ztotožním s názorem F. A. von Hayeka, že ačkoli je samozřejmě možné zavést definici peněz s ostře vymezenými hranicemi, neodpovídá takový stav skutečnosti. Doslova uvádí:

*„Podobnou fikcí je právníká představa, že existuje jednoznačně definovaná věc zvaná 'peníze', která může být jednoznačně odlišena od ostatních věcí. Je o fikci vytvořenou pro uspokojení potřeb právníků a soudců, která nikdy nepopisovala skutečný stav, pokud se nezabývala věcmi, které měly určité charakteristické vlastnosti peněz. ... Pro následující úvahy bude nezbytné si neustále uvědomovat, že různé druhy peněz se mohou od sebe lišit ve dvou rozdílných, nikoli však zcela nezávislých*

<sup>46</sup>NAKAMOTO, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008.

<sup>47</sup>REVENDA, Zbyněk. *Peněžní ekonomie a bankovníctví*. 2. vyd. Praha: Management Press, 1997, s. 22. ISBN 80-85943-49-2.

dimenzích: akceptovatelnosti (neboli likviditě) a očekávaném vývoji (stabilitě nebo variabilitě) jejich hodnoty. ... Čtenář udělá nejlépe pokud si zapamatuje, že má co do činění s celou škálou aktiv s různou mírou akceptovatelnosti, která přechází nepostřehnutelně od aktiv všeobecně akceptovaných po aktiva, která již zcela zjevně penězi nejsou“<sup>48</sup>

Nemám tu v žádném případě v úmyslu zpochybňovat užitečnost právních fikcí a legálních definic s ostrými hranicemi, neboť jejich význam pro zachování právní jistoty je nesporný. Vrátime-li se však k tomu, co jsme řekli na začátku této kapitoly, tedy že peníze jsou kategorií *ekonomickou*, nikoli právní, bude nutné si připustit, že ostrá hranice mezi tím co lze a co již nelze označit jako peníze prostě *neexistuje*.

Domnívám se, že vzhledem k tomu, že bitcoiny jsou způsobilé ve větší či menší míře zastávat funkci peněz (a také tuto funkci přinejmenším v některých komunitách zastávají), lze je bez větších obtíží považovat za peníze svého druhu.

K obdobnému závěru došla i Evropská centrální banka, když ve svém dokumentu týkajícím se *virtuálních „měn“* opakovaně používá pro bitcoiny výraz peníze (angl. *money*).<sup>49</sup>

### 3.2.2. Zařazení bitcoinu pod kategorii měny

Výše jsme si uvedli, že měna je taková forma peněz, za kterou stojí určitá státní či nadstátní autorita, která tuto formu konkretizuje a stanovuje na ni určité požadavky.

*Národní měna* zastává funkci peněz území konkrétního státu a je upravena (nebo přinejmenším uznána) ze strany tohoto státu – především formou právních předpisů, které stanovují množinu znaků, které tato měna musí splňovat: její název, způsob jakým je uvolňována do oběhu a jaké podoby tato forma peněz nabývá (tedy hmotné předměty). Soustavu těchto právních norem nazýváme *měnové právo*.

---

<sup>48</sup>Hayek, soukromé peníze str. 67-68

<sup>49</sup>EUROPEAN CENTRAL BANK. *Virtual Currency Schemes*. 2012. Dostupné z: <http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>

Pro ilustraci si v hrubých rysech načrtne jak vypadá úprava měny v České republice. Základním právním předpisem upravujícím měnu je zákon č. 6/1993 Sb., o České národní bance, který o měně stanoví následující:

- Česká národní banka je subjektem, který má výhradní právo emitovat měnu.
- Tu představují hmotné předměty ve formě bankovek a mincí.
- Konkrétní formu (hmotnost, materiál, vzhled apod.) včetně nominální hodnoty, kterou mají tyto předměty nabývat stanoví ČNB vyhláškou
- Peněžní jednotkou je koruna česká (zkratka Kč), která se dále dělí na sto haléřů.
- Platné bankovky a mince vydané ČNB jsou *zákonnými penězi*<sup>50</sup> ve své nominální hodnotě při všech platbách na území ČR.

Existují určité požadavky, které musí, v souladu s všeobecně uznávanými právními zásadami, splňovat forma peněz k tomu, aby o ní bylo možné hovořit jako o měně v plném právním slova smyslu.

Prvním je požadavek, aby tomuto druhu peněz byl **přiznán atribut měny prostřednictvím autority státu** (zejména právními předpisy).

Druhým je požadavek, aby takový druh peněz byl **skutečným platebním prostředkem na území státu**. Musí na tomto území plnit všechny funkce peněz a být vydáván ve formě hotovostního oběživa. Tím se měna liší od zúčtovacích jednotek, ty mohou být také uznány ze strany státní moci, nicméně plní pouze funkci *denominátoru* velikosti závazku a nejsou proto měnou.

Třetím je pak požadavek, aby takový druh peněz byl **skutečně všeobecným platebním prostředkem**, tedy musí být možné jeho používání širokým okruhem subjektů všech typů, nikoli například jen omezeným okruhem finančních institucí.

Z výše uvedených podmínek bitcoin v první řadě nesplňuje podmínku, kterou je přiznání statutu měny právním řádem jakéhokoli státu. Čistě teoreticky je však možné, jeho uznání některým státem za národní měnu.

<sup>50</sup>Koncept zákonných peněz (angl. Legal tender) znamená v podstatě to, že hmotné předměty prohlášené za zákonné peníze, jsou ve své nominální hodnotě způsobilé k úhradě závazků, jejichž výše je určena v této měně.



Podmínka existence měny ve formě hotovostního oběživa již dle mého názoru nepředstavuje nepřekonatelný problém, a to ze dvou důvodů. Za prvé, bitcoin je ukázkou toho, že skutečnost, že ta či ona forma peněz nexistuje jako hmotné předměty, není na překážku tomu, aby plnila všechny funkce peněz – i s čistě bezhotovostními penězi lze již uhrazovat závazky, směňovat je za zboží a služby a tak dále.

Za druhé, existence bitcoinu ve formě obdobné hotovostnímu oběživu je možná. Již se také objevily hmotné předměty ve formě mincí, které v sobě obsahovaly inkorporovaný soukromý klíč (tedy vlastně bitcoinový účet)<sup>51</sup>. Podobu hotovostního oběživa může bitcoin nabýt i jinými způsoby, lze si například představit cenné papíry, do nichž je inkorporována povinnost jejich emitenta převést na držitele konkrétní částku v bitcoinech a které obíhají v hotovostním platebním styku.

Zásadní problém v použití bitcoinu jako měny je ten, že stát, který by ho takto přijal by nebyl schopen efektivně ovlivňovat ekonomické procesy prostřednictvím měnové politiky, zejména libovolně emitovat nové bitcoiny, neboť jejich emise je řízena výhradně algoritmem v bitcoinovém protokolu.

Je tedy nutné konstatovat, že ačkoli neexistují žádné právní překážky, aby se bitcoin stal měnou některého státu, jedná se o nepříliš pravděpodobnou možnost. Bitcoin tedy v *přinejmenším v současné době není měnou.*

### **3.2.3. Jsou bitcoiny elektronické peníze?**

Již jsme si řekli, že bitcoin můžeme považovat za formu peněz svého druhu. Vzhledem k tomu, že funkčnost bitcoinového platebního systému zajišťuje počítačová síť, zdá se na první pohled, že elektronické peníze jsou kategorií, do níž by bitcoin měl bez obtíží zapadnout. Ukazuje se však, že to není tak jednoduché, neboť pojetí elektronických peněz podle našeho právního řádu nepočítá s možností existence systémů podobným bitcoinu. Důsledkům této skutečnosti se pak budeme více věnovat v sekci týkající se bitcoinových burz a směnár a poskytovatelů webových bitcoinových peněženek.

---

<sup>51</sup>Physical Bitcoins by Casascius. *Casascius* [online]. [cit. 2014-02-23]. Dostupné z: <https://www.casascius.com/>

Právním předpisem upravujícím kategorii elektronických peněz je zákon č. 284/2009 Sb., o platebním styku, který v §4 odst. 1 stanoví že:

*„Elektronickými penězi je hodnota která,*

- a) *Představuje pohledávku vůči tomu, kdo ji vydal,*
- b) *Je uchovávaná elektronicky*
- c) *Je vydávaná proti přijetí peněžních prostředků za účelem provádění platebních transakcí*
- d) *Je přijímána jinými osobami než tím, kdo ji vydal“*

Víme již, že základem bitcoinového systému je kompletní záznam o proběhlých transakcích (tzv. blockchain) ve formě na sebe navazujících tzv. bloků, které si lze představit jako stránky účetní knihy. Emise bitcoinu probíhá tak, že každý účastník-těžař (miner), kterému se jako prvnímu podaří nalézt výpočetně složité řešení matematického problému a přidat tak další blok do blockchainu (pro tuto skutečnost se používá výraz *objevení bloku*), je oprávněn připsat si na svou adresu určitý počet bitcoinů. V současné době je to 25 bitcoinů za každý objevený blok, toto číslo se každých 210000 bloků, tedy přibližně každé 4 roky, snižuje na polovinu<sup>52</sup>.

Bitcoin tedy není vydáván proti přijetí peněžních prostředků a stejně tak nepředstavuje pohledávku vůči tomu kdo ho vydal (těžaři, kterému se jako prvnímu podařilo objevit blok). Bitcoin tedy nejsou de lege lata elektronickými penězi, což znamená, že na ně nedopadá úprava elektronických peněz podle zákona o platebním styku.

### **3.3. Další v úvahu připadající kategorie**

Pro správný výklad právních norem, které se mohou bitcoinu týkat, je důležité jeho zařazení do některé z existujících právních kategorií. Specifická povaha bitcoinu často způsobuje, že ačkoliv bitcoin splňuje některé znaky té či oné kategorie, není ho často možné do ní zařadit z důvodu nesplnění některé z nutných podmínek. Dotkli jsme

---

<sup>52</sup>Mining. In: *Bitcoin wiki* [online], 2014 [cit. 2014-02-24]. Dostupné z: <https://en.bitcoin.it/wiki/Mining>

se těch nejzásadnějších kategorií a ujasnili si, že bitcoiny jsou věcí v právním slova smyslu, jsou to peníze a naopak je nelze zařadit pod kategorii měny a elektronických peněz.

Kromě měny peněz a elektronických peněz připadá v úvahu i množství dalších kategorií, se kterými bitcoinový platební systém sdílí některé své znaky. Zařazení k nim, bude důležité zejména pro posouzení, zda a jakým způsobem jsou právním řádem upravené některé činnosti, které se v souvislosti s bitcoinovým platebním systémem vyskytují a budeme se jim věnovat na stránkách zabývajících se těmito konkrétními činnostmi. Jen pro ilustraci uvádím neuzavřený výčet kategorií, jejichž vztah k bitcoinu může být důležitý pro posouzení jeho postavení v právním řádu. Bude se jednat o tyto kategorie: komodity, (bezhotovostní) peněžní prostředky, cenné papíry a další.

#### **4. Bitcoinový ekosystém – společenské a právní vztahy obklopující bitcoinový platební systém.**

Bitcoinový platební systém obklopuje pestrá škála společenských vztahů, způsobů využití, souvisejících služeb a podobně. Přestože by se na první pohled mohlo jako vhodnější označení pro tuto skutečnost jevit pojem bitcoinový trh, rozhodl jsem se použít pojem ekosystém, neboť podle mého názoru lépe vyjadřuje skutečnost že jde o vnitřně provázaný, neohraňovaný soubor různých uživatelů, druhů a způsobů využití, vztahů které je obklopují a výměny informací a statků, které se vzájemně ovlivňují a vyvíjejí se v čase. Oproti tomu pojem trh chápeme jednoduše jako místo v prostoru (příp. kyberprostoru) a čase, kde se střetává nabídka a poptávka a dochází ke směně statků a peněz (v případě bitcoinového trhu pak půjde o peníze ve formě bitcoinů). V tomto smyslu lze tedy pojem bitcoinový ekosystém chápat jako souhrn společenských a technologických vztahů, obklopujících bitcoinový platební systém, a jako nadřazený pojmu bitcoinový trh.

V této kapitole se budeme snažit odpovědět na otázku, kdo jsou jeho uživatelé, a jaké jsou jejich motivy k jeho využívání. Také nás bude zajímat, kde a jakým způsobem lze bitcoin směnit za jiné formy peněz (tedy především za národní měny), jaké druhy služeb a zboží lze za bitcoin nakoupit, a zda existují některé charakteristiky, které

odlišují trhy na kterých se obchoduje za bitcoiny od trhů, kde se využívá jiný druh peněz.

Pochopení vlastností tohoto ekosystému nám také umožňuje lépe odpovědět na otázku jaké druhy společenských vztahů existují v souvislosti s bitcoinovým platebním systémem, zda a proč je vhodná a nutná jeho specifická právní úprava, a kterým subjektům by v tomto ohledu bylo možné přiznávat práva a ukládat povinnosti.

Kapitolu jsem se rozhodl členit právě podle jednotlivých skupin subjektů, které lze v tomto ekosystému rozlišit. Budou to zaprvé jeho uživatelé, včetně tzv. těžařů (tedy skupiny uživatelů, kteří zajišťují tvorbu záznamu transakcí – blockchainu a za to inkasují odměnu ve formě oprávnění emitovat nové mince), za druhé komunita vývojářů tohoto systému, za třetí bitcoinové burzy a směnárny, za čtvrté prodejci zboží a poskytovatelé služeb přijímající bitcoin a jako poslední, skupina poskytovatelů služeb, které souvisejí s použitím bitcoinu v platebním styku.

Rozebereme-li si, kdo jsou tyto subjekty, jaké jsou jejich motivy k používání bitcoinového systému, k čemu a jakým způsobem tento systém využívají a jaké druhy společenských vztahů (včetně vztahů právních) se zde realizují, umožní nám to lépe pochopit jeho podstatu a také odhalit určitá centra v jinak decentralizovaném systému.

Předpokládáme, že v případě vzniku nových právních norem reflektujících existenci bitcoinu, by v zájmu zajištění jejich vymahatelnosti a efektivity jejich působení mohly být vhodným předmětem úpravy právě společenské vztahy realizující se v těchto centrech.

## **4.1. Uživatelé bitcoinového platebního systému**

Uživateli bitcoinového platebního systému jsou subjekty, které připojují své počítače k bitcoinové síti a využívají ji k platbám. Je to vlastně nejširší skupina, nadmnožina dalších skupin o kterých budeme mluvit. Bude nás zde zajímat kdo jsou uživatelé bitcoinového platebního systému, jaké pohnutky je vedou k jeho užívání a za jakým účelem tak činí.

Již jsme si řekli, že bitcoin je inovativní decentralizovaný platební systém, který umožňuje provádět rychlé platby přes internet s nízkými transakčními náklady. Nemá

centrální autoritu, která by prováděla dohled nad transakcemi, které prochází systémem a jednostranně určovala pravidla jeho fungování, množství peněz v oběhu a která by mohla rozhodovat o tom, zda se transakce uskuteční či ne. Anonymita, respektive pseudonymita, transakcí pak umožňuje efektivní ochranu soukromí stran transakcí. V současné době se tomuto systému dostává pozornosti ze strany médií, cena bitcoinu v posledních měsících dramaticky stoupala a mnozí očekávají její další nárůst.

Tato stručná charakteristika nám také do značné míry určuje z jakých skupin obyvatelstva se rekrutují jeho uživatelé. Zjednodušeně se dá říct, že bitcoin používají ti, kterým tyto jeho charakteristiky z nějakého důvodu vyhovují.

Mezi uživatele bitcoinového systému se tedy řadí různorodá skupina zahrnující technologické a kryptografické nadšence, obhájce ochrany soukromí, jedince s tendencemi nedůvěřovat ve schopnost vlád vykonávat spolehlivě měnovou politiku, zločince a spekulanty. V poslední době se však užití bitcoinu rozšiřuje pomalu i za hranice těchto skupin v souvislosti s pozorností, která je jim v poslední době věnována médii.

Neustále přibývá obchodníků působících v zejména v online prostředí, kteří přijímají bitcoin jako platbu za služby a zboží, a kteří tak cílí na výše zmíněné skupiny uživatelů. Jedná se o různorodé spektrum, od právně a společensky nezávadných činností o poskytovatelů serverů a webhostingu<sup>53</sup>, prodejce elektroniky, technologické konzultanty až po služby pohybující se na hranici legality (případně tuto hranici přímo překračující) – online casina, poskytovatele pornografie různého druhu a tržiště s omamnými a psychotropními látkami.<sup>54</sup>

Zcela specifickou skupinu uživatelů pak představují těžaři – miners. Jak už jsme si řekli, jsou to uživatelé systému, kteří poskytují svůj výpočetní výkon pro zajištění distribuované tvorby kompletního záznamu transakcí. Tito spolu soutěží v řešení výpočetně složitého matematického problému a ten, komu se jako prvnímu podaří najít toto řešení a přidat tak další blok do záznamu, je oprávněn do něj připsat transakci, která

---

<sup>53</sup>služba zajišťující provoz webových stránek

<sup>54</sup>GRINBERG, Reuben. Bitcoin: An Innovative Alternative Digital Currency. *Hastings Science and Technology Law Journal*. 2014, 4:1, str. 165-168.

mu přidává určitý počet bitcoinů (v současné době je to 25 BTC), a inkasuje dobrovolné<sup>55</sup> transakční poplatky, které jsou součástí transakcí zahrnutých do objeveného bloku. Toto bývá obvykle označováno jako „vytěžení bloku“ nebo „nalezení bloku“

Primárním účelem těžení je tedy vytvořit pro uzly platebního systému konsenzuální, důvěryhodný záznam o historii proběhlých transakcí. Sekundární funkcí kterou plní je pak emise nových mincí, kterými jsou odměněni právě ti, kterým se podařilo objevit nový blok a připsat ho na konec blockchainu.

Tak systém motivuje uživatele k tomu, aby pro něj zajišťovali provádění výpočtů.

Systém automaticky nastavuje obtížnost řešení tak, aby k objevení nového bloku docházelo průměrně jednou za deset minut.

Je nutné si uvědomit, že těžaři si v podstatě navzájem konkurují. Čím více je těžařů, tím rychleji je *pravděpodobně* blok objeven. Pravděpodobně proto, že objevení tohoto řešení je náhodné, řešení problému vlastně probíhá metodou pokus omyl – čím více těžařů a čím více výpočetní síly, tím dříve bude toto řešení objeveno. Systém pak nastavuje obtížnost tohoto řešení každých 2016 bloků (zhruba 14 dní) tak, aby při stejné výpočetní síle celé sítě trvalo dalších 2016 bloků přesně 14 dní<sup>56</sup>. Zatímco v počátcích bitcoinového systému mohl prakticky libovolný uživatel s pomocí svého osobního počítače začít těžit a vydělat tak určité množství bitcoinů, v dnešní době již konkurence mezi těžaři značně narostla a obtížnost řešení se velmi dramaticky zvýšila<sup>57</sup>. Proto těžba bitcoinu pomocí procesoru osobního počítače, ačkoli teoreticky stále možná, již naprosto není rentabilní a těžba se přesouvá na ASIC<sup>58</sup> mikročipy, které jsou uzpůsobené a optimalizované přímo pro těžbu bitcoinu.

Protože i při vysokém výpočetním výkonu může osamělému těžaři trvat velice dlouho, než se mu podaří jako prvnímu objevit blok, sdružují se do tzv. mining pools<sup>59</sup>.

<sup>55</sup>Dobrovolné v tom smyslu, že není zcela nutné je zaplatit. Nicméně doporučuje se poplatek ve výši 0.0001 BTC jako incentiva pro těžaře, aby se transakce co nejdříve dostala do blockchainu. V případě nezaplacení poplatku by pak potvrzení transakce trvalo několik hodin nebo i dnů.

<sup>56</sup>Mining. In: *Bitcoin Wiki* [online]. 2014 [cit. 2014-03-24]. Dostupné z: <https://en.bitcoin.it/wiki/Mining>

<sup>57</sup>Viz například <http://www.coindesk.com/data/bitcoin-mining-difficulty-time/>

<sup>58</sup>Application specific integrated circuit – Mikročip jehož design a provedení přímo odpovídá specifickému účelu za kterým byl vytvořen.

<sup>59</sup>Lze přeložit asi jako těžařský svaz, kartel. Běžně se ale i v češtině používá výraz mining pool.

Ty velmi zjednodušeně fungují tak, že jednotliví těžaři spolupracují na řešení výpočetního problému, a v okamžiku, kdy se jim podaří najít nový blok, rozdělí se o odměnu v poměru, v jakém přispěli svojí výpočetní kapacitou<sup>60</sup>. V současné době je většina bitcoinů těžena právě tímto způsobem<sup>61</sup>.

## 4.2. Komunita vývojářů bitcoinového platebního systému

Fungování bitcoinového platebního systému je zajišťováno počítačovým softwarem, který bývá nazýván jako bitcoinový klient. Těchto klientů existuje větší množství, všechny jsou však implementací bitcoinového protokolu, tedy sady předpisů a standardů, které určují pravidla pro komunikaci mezi uzly sítě<sup>62</sup>.

Původní zdrojový kód byl zveřejněn jediným programátorem (ačkoliv jak jsme si již řekli, vzhledem k tomu, že jeho identita zůstává neznámá, je také možné že šlo o více osob, působících pod jedním pseudonymem), Satoshi Nakamotem, který nějakou dobu také působil jako jeho hlavní vývojář a schvalovatel veškerých změn. Od té doby se postupně změnila povaha vývoje a z toho co bylo původně v podstatě osobním projektem se stal decentralizovaný komunitní projekt, na kterém spolupracuje široký tým dobrovolníků. – model, který je typický pro vývoj FOSS – Free and Open Source software<sup>63</sup>.

V zájmu stručnosti poněkud zjednodušený popis vývoje vypadá asi následovně: Vývoj probíhá na webové platformě verzovacího software GitHub, jednotliví developéři diskutují a sdílejí změny, samostatně vyvíjejí a v okamžiku kdy mají hotový kód (tento obvykle řeší nějakou chybu, nebo přináší novou funkcionalitu či jiné vylepšení.), zašlou tzv. pull request tedy žádost o připojení jejich kódu k hlavní větvi bitcoinového software. Současně s tím pošlou na k tomu určené internetové forum příspěvek, který

<sup>60</sup>Pooled Mining. In: *Bitcoin Wiki* [online]. 2014 [cit. 2014-03-24]. Dostupné z: [https://en.bitcoin.it/wiki/Pooled\\_mining](https://en.bitcoin.it/wiki/Pooled_mining)

<sup>61</sup>Viz například <https://blockchain.info/pools> pro graf zobrazující odhadovaný poměr těchto poolů na celkovém výkonu sítě.

<sup>62</sup>NÁDĚLA, Josef. *Velký počítačový slovník*. Vyd. 1. Kralice na Hané: Computer Media, 2004, s. 328. ISBN 80-86686-21-3.

<sup>63</sup>Lze přeložit jako svobodný software s otevřeným zdrojovým kódem – Jde o software, jehož zdrojový kód je volně k dispozici, a který je uvolněný pod licencí, která umožňuje komukoliv svobodně studovat, používat, kopírovat a pozměňovat takový software. Těmto požadavkům vyhovuje přes padesát typů licenčních ujednání nejznámější jsou asi – MIT License (právě pod ní je vydáván bitcoinový referenční klient), GNU General Public License, Apache License. Seznam a obsah těchto licencí je k dispozici na <http://opensource.org/licenses/alphabetical>.

vysvětluje změny a jejich zdůvodnění. Na fóru poté probíhá diskuze o přínosu tohoto kódu, jeho bezpečnosti, testování a v okamžiku, kdy je dosaženo konsenzu, je kód připojen k hlavní vývojové větvi nebo odmítnut. Hlavní vývojová větev je pravidelně testována a jednou za určité časové období je prohlášena za tzv. release candidate<sup>64</sup>, tato kandidátská verze je opět nějakou dobu testována a následně prohlášena za novou verzi bitcoinového software<sup>65</sup>.

Zatímco na počátku vývoje existoval jen jediný bitcoinový klient – *bitcoind* zveřejněný Nakamotem (a po něm označovaný jako Satoshi Client), který i v současné době funguje jako referenční implementace bitcoinového protokolu. Postupně odštěpením vznikají i jiné bitcoinové klienty (tak jak to software uvolněný pod svobodnými licencemi umožňuje). Tyto klienty se liší v mnoha různých aspektech (podporovaném operačním systému, v tom, zda je bitcoinová peněženka chráněna šifrováním, v nutnosti uchovávat na pevném disku počítače celou kopii blockchainu, apod.), ale jejich zásadní charakteristika zůstává stejná: implementují bitcoinový protokol a umožňují tak svým uživatelům zasílat a přijímat platby v rámci bitcoinového platebního systému.

Vidíme tedy, že vývoj probíhá poměrně velmi otevřeně, takovým způsobem, že kdokoli může přispět svým vylepšením a revidovat existující kód. Jeho změny jsou podrobeny diskurzu a důkladnému testování a zkušenost ukazuje, že v případě objevení chyby, bývá tato rychle odstraněna. Každý má také možnost použít již existující kód a odštěpením z něj vytvořit vlastní bitcoinový klient – v takovém případě ovšem musí dodržet pravidla stanovená bitcoinovým protokolem, jinak by takový software nemohl být součástí bitcoinové sítě - ostatní uzly by s ním odmítaly komunikovat.

Vývojářská komunita bitcoinového protokolu a referenčního klientu *bitcoind* také představuje jakési de-facto centrum bitcoinového platebního systému. Vše co je součástí bitcoinového protokolu tudy prochází. Objevují se i názory že existence tohoto centra otevírá cestu k jakémusi „*infiltračnímu útoku*“ - tedy k ovlivnění této komunity určitou zájmovou skupinou a prosazení změn takového rázu, že by ohrožovaly existenci

---

<sup>64</sup>Kandidát na finální verzi, na vydání.

<sup>65</sup>Development process. In: *Bitcoin Wiki* [online]. 2012 [cit. 2014-03-24]. Dostupné z: [https://en.bitcoin.it/wiki/Development\\_process](https://en.bitcoin.it/wiki/Development_process)



systemu, nebo měnily jeho zásadní charakteristiky (například množství emitovaných mincí). Takový útok bohužel nejde vyloučit, ovšem, vzhledem k otevřenému charakteru vývoje, nelze předpokládat možnost *skrytého* prosazení škodlivých změn, neboť celý proces vývoje je podroben veřejnému dohledu. Podle dostupných informací k takovému útoku také zatím nikdy nedošlo.

Důležitou roli zde hraje také fakt, že pro prosazení takové změny by bylo nutné přesvědčit většinu uživatelů, aby začali používat takto pozměněné klienty, v opačném případě by stávající klienty odmítaly komunikaci od pozměněných klientů, protože by neodpovídala v nich implementovanému protokolu<sup>66</sup>.

### 4.3. Bitcoinové burzy, směnárny a bankomaty

Bitcoin, na rozdíl od mnoha jiných druhů elektronických peněz, není vydáván proti přijetí peněžních prostředků a nepředstavuje závazek proti jeho emitentovi. Emise nových mincí probíhá formou odměny pro uživatele-těžaře, kteří přispívají svým výpočetním výkonem k zajištění fungování sítě - potvrzování transakcí vytvářením záznamu označovaného jako blockchain.

V případě, že jakýkoliv subjekt poptává bitcoiny, má v zásadě tři možnosti. Prvním, pro bitcoin specifickým způsobem je začít je těžit, jenomže, jak jsme si již uvedli v sekci věnované uživatelům-těžařům, těžba vyžaduje určité nezanedbatelné technické dovednosti a v současné době již i specializovaný hardware. Další možnosti nabytí už bitcoin sdílí s ostatními formami peněz: lze ho získat jako platbu za služby nebo zboží, nebo směnit za některou národní měnu na burze nebo ve směnárně<sup>67</sup>. Právě tím posledním způsobem se budeme zabývat na následujících řádcích.

Bitcoinové směnárny a burzy jsou tedy institucemi, místy v prostoru (či častěji jen v kyberprostoru), kde probíhá směna bitcoinu za fiat peníze.

---

<sup>66</sup>GRINBERG, Reuben. Bitcoin: An Innovative Alternative Digital Currency. *Hastings Science and Technology Law Journal*. 2014, 4:1. s. 175 - 176

<sup>67</sup>Bitcoin: The Libertarian Introduction. In: VOORHEES, Erik. *On Life and Liberty* [online]. 2012 [cit. 2014-03-24]. Dostupné z: <http://evoorhees.blogspot.cz/2012/04/bitcoin-libertarian-introduction.html>

Princip jejich fungování je v zásadě obdobný směnárnám a burzám jiných komodit/měn. Různé burzy se od sebe navzájem liší v rozmanitých charakteristikách, podle toho zda jednostranně určují kurz, uchovávají peněžní prostředky na uživatelských účtech, vystupují jako strana směny a také v významných technických aspektech, spočívajících ve vnitřním technickém uspořádání – zejména zabezpečení proti kybernetickým útokům.

Provozovatel bitcoinové směnárny většinou jednostranně určuje kurz, ve kterém provádí směnu a je sám jednou z jejích stran. Naproti tomu osoba provozující bitcoinovou burzu funguje jen jako jakýsi organizátor trhu – zabezpečuje provoz platformy, kde se střetává nabídka a poptávka, a zpravidla také vede stranám transakcí účty znějící na bitcoiny či na některou národní měnu.

Úplně novým jevem jsou pak bitcoinové bankomaty, jejich výskyt se v poslední době rozšiřuje a objevují se již i na území ČR<sup>68</sup>.

V následujících řádcích se budu přednostně zabývat burzami a směnárnami působícími na území České republiky, ačkoliv se zřejmě neobejdeme bez toho abychom si zmínili i některé burzy globálního významu.

#### **4.3.1. Bitcoinové směnárny**

Jak již bylo uvedeno výše, bitcoinové směnárny jsou instituce, které umožňují směnit fiat měny za bitcoin. Od burz se liší tím, že provozovatel směnárny zde vystupuje jako strana směny. Také obvykle jednostranně určuje kurz, za který je ochoten směnu provádět.

Na českém území v současné době funguje několik takových směnáren, většina z nich působí výhradně v prostředí internetu<sup>69</sup>, objevují se však i směnárny v kamenných obchodech. Nové směnárny vznikají a zanikají ve velmi rychlém sledu, což je vzhledem k poněkud pionýrskému charakteru tohoto druhu podnikání pochopitelné a

---

<sup>68</sup>The new gold rush: Bitcoin ATMs are coming. In: *The Verge* [online]. 2014 [cit. 2014-03-29]. Dostupné z: <http://www.theverge.com/2014/3/10/5490534/the-new-gold-rush-bitcoin-atms-are-coming>

<sup>69</sup>Jsou to například simplecoin.cz, dagesia.eu, smenarnabitcoin.cz a jiné. Posledně jmenovaná směnárna je v současné době nefunkční, neboť jí byly dle vyjádření provozovatele ze strany Fio Banky zrušeny účty. Podle dostupných informací však byly všechny transakce dokončeny nebo zrušeny a peněžní prostředky zaslány zpět zákazníkům.

platí to ostatně i pro jiné projekty spojené s bitcoinovým systémem. Proto je při používání směnárny vždy namísto opatrnost a dostatek informací.

Směna obvykle probíhá tak, že osoba, která má v úmyslu směnit bitcoin za nějakou měnu či nebo naopak, uzavře (obvykle online) směnnou smlouvu podle ustanovení § 2184 - § 2188 Občanského zákoníku<sup>70</sup>, ve které odsouhlasí obchodní podmínky směnárny. Klíčovými ustanoveními této smlouvy jsou, kromě zákonných podstatných náležitostí, také kurz a částka ke směně a doba po kterou smlouva platí. Doba po kterou smlouva platí bývá ujednávána z toho důvodu, že cena bitcoinu na trhu podléhá rychlým změnám, a není tak vhodné garantovat dohodnutou cenu příliš dlouho. Po uzavření smlouvy zákazník zašle peněžní prostředky na účet směnárny, vedený u peněžního ústavu a nebo na jeho bitcoinovou adresu, a ten mu obratem zašle odpovídající protiplnění.

V této souvislosti je nutné si uvést, že na směnářenskou činnost se vztahuje zákon č. 277/2013 Sb., o směnářské činnosti, který pro ni stanovuje určité podmínky a omezení. Zejména se jedná o vymezení osob, oprávněných provozovat směnářenskou činnost, o povinnost vykonávat směnářenskou činnost výhradně na základě povolení České národní banky, některé informační povinnosti vůči zákazníkům i ČNB, povinnost poskytovat součinnost při výkonu dohledu a další.

Na otázku, zda se tyto právní normy vztahují i na bitcoinové směnárny, je nutné vyložit si §2 tohoto zákona, který stanoví že:

*„ (1) Směnářským obchodem je obchod spočívající ve směně bankovek, mincí nebo šeků znějících na určitou měnu za bankovky, mince nebo šeky znějící na jinou měnu.*

*(2) Směnářskou činností je soustavná činnost provozovaná vlastním jménem a na vlastní odpovědnost za účelem dosažení zisku, která spočívá v provádění směnářských obchodů.“*

Zjednodušeně lze tedy říci, že směnářskou činností je podnikání spočívající v provádění směnářských obchodů.

<sup>70</sup>Zákon č. 89/2012 Sb., občanský zákoník

Otázka zda lze směnu bitcoinu za měnu subsumovat pod pojem směnárenský obchod už je trochu složitější. V prvním odstavci lze rozlišit několik znaků, které musí transakce kumulativně splňovat, aby bylo možné ji považovat za směnárenský obchod:

1. Musí se jednat o směnu
2. Směňovány musí být bankovky, mince nebo šeky
3. Tyto musí znít na určitou měnu
4. Musí být směňovány za předměty opět splňující znaky uvedené v bodě 2. a 3.

Podle §2148 občanského zákoníku se směnnou smlouvou každá ze stran zavazuje převést vlastnické právo k věci, výměnou za závazek druhé strany převést vlastnické právo k jiné věci. Při výměně bitcoinů za měnu půjde tedy bezpochyby o směnu a první znak tak bude splněn.

Problematické však budou body zbývající, neboť bitcoiny zpravidla nenabývají hmotné formy bankovky, mince ani šeku. I v případě že by této formy nabývaly (což je zřejmě možné – například mince do které je fyzicky inkorporován šifrovací klíč bitcoinové peněženky<sup>71</sup>) nebude splněn požadavek aby zněl na určitou měnu – bitcoin totiž není měna. Blíže se touto otázkou zabývám v sekci Právní úprava měny a peněz zjednodušeně lze ale říct že je to zejména proto, že ho jako svou měnu neuznává žádný stát světa.

Touto argumentací tedy docházíme závěru, že bitcoinové směnární, navzdory názvu, který je pro ně běžně používán, neprovozují směnárenskou činnost, a proto se na ně nevztahují podmínky stanovené zákonem č. 277/2013 Sb. O Směnárenské činnosti. Tento výklad zastává ve svém stanovisku k obchodování s bitcoiny i Česká národní banka:

*„V případě směny (resp. nákupu) bitcoinů za české koruny nebo jinou měnu také nejsou splněny znaky směnárenského obchodu, který je definován jako „směna bankovek, mincí nebo šeků znějících na určitou měnu za bankovky, mince nebo šeky znějící na jinou měnu“ (§ 2 odst. 1 ZSČ), tj. není splněn znak hmotné podoby předmětu směny ani znak „znějící na určitou měnu“.“<sup>72</sup>*

---

<sup>71</sup>Viz např. Physical Bitcoins by Casascius na adrese <https://www.casascius.com/>

### 4.3.2 Bitcoinové burzy

Dalším místem, kde probíhá směna bitcoinů za měny, jsou bitcoinové burzy. Jak už jsme si řekli, od směnárny je odlišuje zejména fakt, že provozovatel burzy není stranou transakce, jen zajišťuje fungování trhu, místa, kde se střetává nabídka a poptávka po bitcoinu. I těchto podniků funguje na globálním trhu poměrně velké množství.

První a dlouho dobu i nejdůležitější burzou byla po velkou část poměrně krátké doby trvání bitcoinového systému Tokijská burza Mt. Gox, o níž se zde krátce rozvedeme, neboť jakožto jeden z nejdůležitějších zástupců ilustruje některá rizika, která se v souvislosti s bitcoinovými burzami mohou vyskytovat.

Byla založena v roce 2010 a v době svého největšího rozmachu vyřizovala až 90% všech směn bitcoinu za měny<sup>73</sup>. V současné době je však již minulostí, neboť v únoru 2014 (po týdnech problémů při vyplácení zůstatků na burzovních účtech a všeobecných spekulacích o jejím špatném finančním stavu) vstoupila do likvidace. Podle dostupných údajů se tak stalo proto, že se neznámému útočníkovi podařilo využít slabiny v jejích systémech, v souvislosti s vlastností bitcoinového systému známé jako *kujnost transakcí - transaction malleability*<sup>74</sup>. Podle jejich vlastního tvrzení bylo při tomto útoku odcizeno 850 000 BTC, ale podle jiných zdrojů bylo množství takto odcizených bitcoinů mnohonásobně menší. Mnozí se ovšem shodují na tom, že existence jedné, majoritně využívané burzy byla slabinou v systému, jehož silnou stránkou je právě decentralizace a že tak pád Mt. Goxu ve skutečnosti posílil stabilitu bitcoinového platebního systému, neboť nadále již není spojen s jednou dominantní burzou, ale je obchodován na větším množství menších burz<sup>75</sup>.

---

<sup>72</sup>ČESKÁ NÁRODNÍ BANKA. *Obchodování s bitcoiny*. 10.2.2014. 2014. Dostupné z:

[http://www.cnb.cz/miranda2/export/sites/www.cnb.cz/cs/faq/obchodovani\\_s\\_bitcoiny.pdf](http://www.cnb.cz/miranda2/export/sites/www.cnb.cz/cs/faq/obchodovani_s_bitcoiny.pdf)

<sup>73</sup>WALLACE, Benjamin. The Rise and Fall of Bitcoin. *Wired Magazine* [online]. 2011 [cit. 2014-04-02]. Dostupné z:

<http://fromm.robertkeahey.com/wp-content/uploads/2013/07/Session-7-The-Rise-and-Fall-of-Bitcoin.pdf>

<sup>74</sup> V překladu kujnost transakcí. Jde o již delší dobu známou možnost změnit identifikátor (ID) transakce ještě předtím, než je zapsána do blockchainu. Transakce tedy proběhne, útočníkovi se ale podaří změnit její identifikátor. Pod tímto zfalšovaným identifikátorem je pak transakce zapsána do veřejného záznamu transakcí. Tato vlastnost sama o sobě nenarušuje bezpečnost bitcoinového systému, neumožňuje útočníkovi například odeslat bitcoiny které nemá, nebo odcizit bitcoiny z cizí peněženky. MtGox ovšem identifikovala všechny provedené transakce pouze na základě tohoto ID (ačkoliv vzhledem k okolnostem měla a mohla vědět, že toto ID může být změněno). Útočník pak transakci reklamoval (tvrdil že neproběhla), MtGox ověřila v blockchainu že transakce s tímto ID skutečně neproběhla a zaslala bitcoiny podruhé.

V současné době tedy funguje těchto burz více, mezi největšími lze uvést původem slovinský Bitstamp<sup>76</sup>, nyní se sídlem ve Spojeném království, Bulharský BTC-e<sup>77</sup>, čínský BTC China<sup>78</sup> a další<sup>79</sup>. Ačkoliv tuzemcům v zásadě nic nebrání nakupovat na těchto zahraničních burzách, vzhledem k poměrně vysokým poplatkům a době, kterou trvají zahraniční bankovní převody, je pro české uživatele bitcoinového systému dobrou zprávou, že existuje byť objemem transakcí nepříliš významná, ale česká burza bitcoinů Bitstock provozovaná společností Digital Financial Services s.r.o. se sídlem v Praze<sup>80</sup>.

Zajímavou alternativou je pak server Localbitcoins.net, který zprostředkovává spojení registrovaných uživatelů z různých zemí světa, za účelem obchodování s bitcoiny ve své národní měně, a to buď bezhotovostně, a nebo i za hotovost s osobním setkáním a směnou bitcoinů obvykle za použití chytrého telefonu s nainstalovanou aplikací, sloužící jako bitcoinová peněženka.

Kromě těchto „oficiálních“ burz pak také dochází k neformálnímu obchodování s bitcoinem na jiných platformách, kterými jsou především diskuzní fóra<sup>81</sup> a IRC kanály<sup>82</sup>.

V rámci této práce nás v každém případě bude zajímat odpověď na otázku, zda a jakým způsobem jsou tyto instituce upraveny platným právem. Právní předpisy, jejichž aplikace by zde připadala v úvahu jsou zákon č. 229/1992 Sb., *o komoditních burzách* a zákon č. 256/2004 Sb., *o podnikání na kapitálovém trhu*.

První předpis upravuje burzovní obchody se zbožím (komoditami) a od nich odvozenými deriváty (komoditní deriváty), pokud nejsou investičním nástrojem upraveným zvláštním předpisem (kterým je právě zákon o podnikání na kapitálovém trhu). Tento předpis stanoví co je burzovním obchodem, jakým způsobem je založena a

---

<sup>75</sup>DECKER, Christian a Roger WATTENHOFER. *Bitcoin Transaction Malleability and MtGox*. Zurich, 2014. Dostupné z: <http://arxiv.org/pdf/1403.6676v1.pdf>. ETH Zurich.

<sup>76</sup><http://www.bitstamp.net>

<sup>77</sup><http://www.btc-e.com>

<sup>78</sup><http://www.btcchina.com>

<sup>79</sup>viz například <http://bitcoincharts.com/markets/>

<sup>80</sup><http://www.bitstock.cz/contact>

<sup>81</sup>například české fórum na serveru bitcoincash.cz - <http://www.bitcash.cz/forum/>

<sup>82</sup>Internet Relay Chat – jeden z prvních internetových protokolů umožňujících komunikaci v reálném čase. Jako příklad můžeme uvést zejména #bitcoin-otc na serveru freenode.net. OTC je zkratka pro pojem *over-the-counter* což označuje mimoburzovní, neoficiální obchodování s finančními instrumenty.

organizována komoditní burza, její orgány a vnitřní poměry, podmínky udělení státního povolení k provozování burzy, otázky členství v burzovní komoře, státní dozor a související správní delikty.

Předmětem úpravy zákona o podnikání na kapitálovém trhu je poskytování služeb v oblasti kapitálového trhu, ochrana kapitálového trhu a investorů a veřejná nabídka investičních cenných papírů. Upravuje postavení poměrně širokého okruhu subjektů od obchodníků s cennými papíry, profesionálních zákazníků, investičních zprostředkovatelů, vázaných zástupců po organizátory regulovaného trhu s cennými papíry, centrálních deponitáře, garanční fondy obchodníků s cennými papíry a také postavení státních orgánů při činnostech souvisejících s obchodováním na kapitálovém trhu. Těmto subjektům jsou ukládány široké povinnosti informačního charakteru (evidence a ukládání dokumentů, sdělování informací), nutnost povolení k činnosti, pravidla obezřetného podnikání investičních služeb. Zákon také upravuje státní dohled nad kapitálovým trhem na individuálním i konsolidovaném základě a oblast správních deliktů, přestupků a správního trestání.

Tak jako v ostatních případech pro nás bude zásadní otázkou, zda a do jaké míry lze tyto předpisy aplikovat na burzy na kterých probíhá výhradně obchodování s bitcoinem, přičemž se nebudeme dopodrobna zabývat konkrétními důsledky, které by pro bitcoinové burzy představovala aplikace těchto předpisů, neboť analýza právní úpravy komoditního a kapitálového trhu není předmětem této práce. Obecně však lze říci že by důsledkem aplikace byla nutnost provozovatelů zajistit pro svou činnost povolení příslušného orgánu (podle zákona o podnikání na kapitálovém trhu<sup>83</sup> je tímto orgánem Česká národní banka, podle zákona o komoditních burzách<sup>84</sup> pak Ministerstvo průmyslu a obchodu nebo Ministerstvo zemědělství v oblastech jejich působnosti podle Kompetenčního zákona<sup>85</sup>) a podrobit se jeho dohledu, splňovat zákonné požadavky v oblasti informačních povinností, zajištění odbornosti osob pomocí kterých vykonávají svou činnost, dodržovat pravidla kapitálové přiměřenosti a obezřetného podnikání a další.

---

<sup>83</sup> §4a zákona č. 256/1994 Sb. O podnikání na kapitálovém trhu

<sup>84</sup> §5 odst. 1 zákona č. 229/1992 Sb. O komoditních burzách

<sup>85</sup> zákon č. 2/1969 Sb. O zřízení ministerstev a jiných ústředních orgánů státní správy České socialistické republiky

Lze se domnívat že důsledkem převládnutí takového výkladu zákona, který by subsumoval bitcoinové burzy pod normy obsažené v těchto právních předpisech (fakticky by zřejmě hrála největší roli otázka zda by takovým způsobem tyto předpisy interpretovaly výše zmíněné dohledem pověřené orgány, v druhé řadě pak soudy v případě přezkumu rozhodnutí těchto orgánů) by byla na jednu stranu likvidace současných provozovatelů, v případě, že by nebyli schopni dostát zákonným požadavkům, na druhé straně pak přesun výkonu této činnosti na provozovatele schopné těmto požadavkům dostát, což by mohlo přinést určitou stabilitu do dosud neregulovaných, divokých vod obchodování s bitcoinem (viz například případ burzy Mt. Gox). Otázku zda by takový vliv na bitcoinovou ekonomiku byl v konečném důsledku pozitivní či negativní však ponecháme alespoň prozatím stranou.

#### **4.3.2.1. Subsumpce bitcoinových burz pod zákon o komoditních burzách**

§ 1 odst. 1 zákona O komoditních burzách vymezuje komoditní burzy následovně:

*„Komoditní burzou je právnická osoba zřízená podle tohoto zákona (dále jen "burza") k organizování burzovních obchodů se zbožím (dále jen "komodity"), deriváty vztahujícími se ke komoditám, které jsou předmětem obchodování na burze (dále jen "komoditní deriváty"), pokud nejsou investičním nástrojem podle zvláštního právního předpisu, nebo se zemědělským skladním listem podle zvláštního právního předpisu“*

Čtvrtý odstavec téhož paragrafu pak stanoví že:

*„Jiné osoby než burzy zřízené podle tohoto zákona nesmí ve své obchodní firmě, názvu, označení poskytovaných služeb nebo v jakékoliv souvislosti se svojí činností použít nebo používat označení „komoditní burza“ nebo jiné označení od těchto slov odvozené nebo s ním zaměnitelné, anebo takové označení, které vyvolává dojem, že jde o činnost burzy.“*

Dalším důležitým pojmem, který tento zákon definuje je pojem *burzovních obchodů* v § 2:



*„(1) Burzovním obchodem je koupě a prodej komodit a komoditních derivátů, které nejsou investičním nástrojem podle zvláštního právního předpisu, osobami oprávněnými k burzovním obchodům sjednaným na burze v místnostech a hodinách určených pro burzovní shromáždění, popřípadě i mimo burzu, za podmínek určených tímto zákonem a statutem, pokud je cena z tohoto obchodu zaznamenána příslušným orgánem burzy.*

*(2) Burzovním obchodem jsou i pomocné obchody uzavírané na burze, jež souvisejí s komoditami prodávanými na burze, zejména pojistné smlouvy, smlouvy o uskladnění, smlouvy o přepravě věci a smlouvy zasílatelské.“*

Mezi relevantní ustanovení bude v tomto případě patřit i § 36 odst. 1 spolu s § 36 odst. 1. První citovaný paragraf stanoví že:

*„Fyzická osoba se dopustí přestupku tím, že*

*a) v rozporu s § 1 odst. 4 užívá neoprávněně označení „komoditní burza“ nebo jiné označení od těchto slov odvozené nebo s ním zaměnitelné, anebo takové označení, které vyvolává dojem, že jde o činnost burzy, nebo*

*b) vykonává činnost burzy bez povolení podle § 5 odst. 1 nebo 5.“*

Druhý paragraf pak označuje stejné jednání za správní delikt, pokud se ho dopustí právnická osoba, nebo podnikající fyzická osoba.

Vidíme zde tedy, že v rozporu se zákonem se ocitá již samotné použití označení „komoditní burza“ nebo označení od těchto slov odvozené nebo s ním zaměnitelné v souvislosti s provozovanou činností, ať již přímo ve své obchodní firmě a také označení, které vyvolává dojem že jde o činnost burzy.

Dále je též v rozporu se zákonem vykonávání činnosti burzy bez příslušného povolení podle § 5. Touto činností bude, v souladu s výše citovaným § 1 odst. 1, organizování burzovních obchodů se komoditami a od nich odvozenými komoditními

deriváty (pokud nejsou investičním nástrojem podle ZPKT) nebo se zemědělským skladním listem.

Důležité pro posouzení, zda je provozování bitcoinové burzy vykonáváním činnosti burzy ve smyslu zákona o komoditních burzách, je odpověď na otázku, zda se jedná o burzovní obchody. § 2, který vymezuje pojem burzovních obchodů určuje následující znaky:

1. Jedná se o koupi a prodej komodit a komoditních derivátů, které nejsou investičním nástrojem podle zvláštního předpisu
2. Tento obchod je uzavřen osobami oprávněnými k burzovním obchodům sjednaným na burze v místnostech a hodinách určených pro burzovní shromáždění. Případně může být uzavřen i mimo burzu, za podmínek určených zákonem O komoditních burzách a statutem burzy, pokud je cena tohoto obchodu zaznamenána příslušným orgánem burzy.

Pro správnou odpověď na otázku, zda byla splněna první podmínka bude nutné zejména vyjasnit, zda jsou bitcoiny komoditou ve smyslu tohoto zákona. Dle mého názoru poněkud nešťastně zákon O komoditních burzách neobsahuje definici pojmu komodity. Jen v § 1 odst. 1 je použita následující formulace: „Komoditní burzou je právnická osoba zřízená podle tohoto zákona (dále jen 'burza') k organizování burzovních obchodů **se zbožím (dále jen 'komodity')**“. Dá se tedy říct že mezi pojem zboží a komodity jsou zaměnitelné, bohužel ani pojem *zboží* zde není dále definován.

Podpůrně bude zřejmě možné při argumentaci využít definici pojmu komodity, kterou obsahuje § 2 odst. 3 písm. a) zákona O podnikání na kapitálovém trhu. Ten stanoví že v tomto zákoně se komoditou rozumí „*komodita podle přímo použitelného předpisu Evropské unie, kterým se provádí směrnice Evropského parlamentu a Rady upravující trhy finančních nástrojů*“

Takovým předpisem je nařízení Komise (ES) č. 1287/2006<sup>86</sup>, které ve svém článku 2 odst. 1 stanoví že „*'komoditou' se rozumí jakékoli zboží zaměnitelné povahy, které lze dodat, včetně kovů a jejich rud a slitin, zemědělských výrobků a energie, např. Elektřiny;*“

Podle tohoto ustanovení lze dovést, že, vykládáno v souladu s evropskou legislativou, bitcoin je komoditou, neboť se jedná o zboží zaměnitelné povahy (jednotlivé bitcoiny se od sebe kvalitativně neliší), které lze dodat (tím že je odešleme na příjemcovu adresu v bitcoinové síti). První podmínka pro posouzení zda na bitcoinových burzách dochází k burzovním obchodům tedy bude dle mého názoru splněna. Lze se ovšem setkat i s názorem opačným, podle kterého bitcoin z definice komodity vylučuje fakt, že jej není možné využít k jiné spotřebě než ke směně<sup>87</sup>.

Sporné bude ovšem také posouzení druhé podmínky, podle které je nutné, aby byl takový obchod uzavřen osobami oprávněnými k burzovním obchodům sjednaným na burze v místnostech a hodinách určených pro burzovní shromáždění, případně i mimo burzu, za podmínek určených zákonem *O komoditních burzách* a statutem burzy, pokud je cena takového obchodu zaznamenána příslušným orgánem burzy. Ke správnému posouzení této otázky, budeme muset provést krátký rozbor pojmu burzy, burzovních obchodů a členského principu, na němž jsou burzy založeny.

---

<sup>86</sup> nařízení Komise č. 1287/2006 ze dne 10.8. 2006, kterým se provádí směrnice Evropského parlamentu a Rady 2004/39/ES, pokud jde o evidenční povinnosti investičních podniků, hlášení obchodů, transparentnost trhu, přijímání finančních nástrojů k obchodování a o vymezení pojmů pro účely zmíněné směrnice.

<sup>87</sup>viz VRBÍKOVÁ, Lenia a Jan VYSKOČIL. Právní a daňové aspekty Bitcoinu. In: *Zkušenosti s virtuálními měnami: Bitcoin měna budoucnosti?*. Praha, 2014, s. 136-139. Dostupné z: <http://ekon.konference.vsmie.cz/zkusenosti-s-virtualnimi-menami/data/program.pdf>

Pojem burza označuje místo, na kterém dochází ke shromáždění kupců, prodejců a zprostředkovatelů a uskutečňuje se zde prodej zboží které není fyzicky přítomno. Postupně se tento pojem stal označením pro zvláštní druh trhu. Nejprve tento pojem označoval jen místo, na kterém dochází k uzavírání obchodů, později význam pojmu vyvíjel až do současné podoby, kdy lze burzu chápat jako instituci organizující trh.

Lze rozlišit několik prvků, kterými lze burzu charakterizovat: Jde o místo, kde se obchoduje, schůzku obchodníků (burzovní shromáždění), formu trhu se specifickým předmětem obchodu a jako instituci organizující trh.

Je přitom možné odlišit stránku prostorovou, ve které burza vystupuje jako určité místo (otázka na jakém místě probíhá obchod ke kterému dochází de facto v kyberprostoru se v této práci nemohu zabývat, uveďme jen, že se nabízí několik různých přístupů: podle místa na kterém se nacházejí osoby jejichž jednáním dochází k uzavírání obchodů, podle místa ke kterému mají vztah osoby zajišťující funkci burzy, resp. místa na kterém se nachází sídlo burzy jako právnické osoby a nebo též podle místa, na kterém se nachází server připojený k síti internet a na kterém tak fakticky dochází k uzavírání transakcí a tvorbě záznamu o nich<sup>88</sup> ).

Časový a personální aspekt burzy potom zachycuje skutečnost, že se jedná o schůzku oprávněných obchodníků za účelem uzavírání obchodů v určitém čase (je zde ale nutné poznamenat že s využitím výpočetní techniky je prakticky možné, aby burzovní shromáždění trvalo nepřetržitě)

Je také nutné si uvědomit, že pojem burzy lze chápat jak jako kategorii právní, tak i jako kategorii ekonomickou, přičemž nemusí docházet k dokonalému překryvu významu těchto pojmů a je tak nutné tyto kategorie odlišit.

Burzu jako kategorii ekonomickou můžeme chápat jako zvláštní formu trhu se svými charakteristickými znaky. Těmi jsou zejména zvláštní organizovanost trhu, kterou zpravidla zajišťuje k tomu zřízená právnická osoba, osobní omezenost trhu jen na určitý okruh oprávněných osob, omezení obchodů jen na zastupitelné druhově určené zboží ve větších objemech bez současné fyzické přítomnosti tohoto zboží na burze, pravidelné

---

88

opakování obchodu na určitém místě a určitém čase, standardizovanost obchodních podmínek a podřízenost státnímu dohledu.

Burza jako kategorie právní je pak právnická osoba, zřízená způsobem, předvídaným právními předpisy k organizaci burzovních obchodů – tedy soustředování nabídky a poptávky do určitého místa a času, zajišťování jednotných obchodních podmínek a mechanismů k určení kupní ceny a uzavření kupní smlouvy<sup>89</sup>.

Zdá se že hlavní odpověď na otázku, zda organizování obchodů na bitcoinových burzách spadá pod ustanovení zákona o komoditních burzách, leží v kritickém posouzení zda se vůbec jedná o burzy v ekonomickém slova smyslu. Je vidět že bitcoinové burzy vůbec nespĺňují některé základní znaky burz, zejména osobní omezenost obchodování na členském principu, neboť na většinu z nich se může zaregistrovat kdokoli během několika minut a bez jakýchkoli zvláštních požadavků na jeho osobu. Také požadavek, aby bylo zboží obchodováno jen ve větších objemech zde není splněn neboť většina burz umožňuje obchodování i částek nižších než 0.1 BTC (což je při současných cenách zhruba ekvivalentem 1000 Kč)

Vzhledem k výše uvedenému se tedy domnívám, že projekty, které bývají označovány jako bitcoinové burzy, nejsou burzami v ekonomickém ani právním slova smyslu a že tedy při nich nedochází k provozování komoditní burzy bez příslušného povolení. Jejich provoz tedy není v rozporu s § 5 zákona o komoditních burzách a nedochází k naplnění skutkové podstaty správních deliktů podle § 36 odst. 1 písm. b) ani § 36a odst. 1 písm. b)

Naproti tomu se lze domnívat, že samotné používání označení „burza“, resp. „burzovní“ pro služby poskytované v souvislosti se směnou bitcoinů za jinou formu peněz je v rozporu s dovoleným způsobem tohoto užití podle § 1 odst. 4 a může tak podle subjektu který se takového jednání dopouští naplňovat buď skutkovou podstatu přestupku podle § 36 odst. 1 písm. a) - jedná-li se o fyzickou osobu, nebo správního deliktu podle § 36a odst. 1 písm. a) – jedná-li se o právnickou, nebo podnikající fyzickou osobu.

---

<sup>89</sup>JELÍNEK, Ladislav. *Komoditní burzy v české republice*. Kroměříž: Justiční akademie, 2006.

#### 4.3.2.2. Subsumpce bitcoinových burz pod zákon o podnikání na kapitálovém trhu

Dozor nad dodržováním práv a povinností stanovených zákonem č. 256/2004 Sb., o podnikání na kapitálovém trhu, právními předpisy, i přímo použitelným předpisem Evropské unie v oblasti činnosti na finančních trzích a rozhodnutí vydaných podle tohoto zákona je ustanovením § 135 svěřen České národní bance. Ta 10. 2. 2014 zveřejnila svoji odpověď na dotaz zda je k obchodování s bitcoiny nebo jejich směně potřebné povolení ze strany ČNB.

Odpověď je zamítavá. ČNB zastává názor, že k obchodování s bitcoiny není třeba jejího povolení, ve vztahu k zákonu o podnikání na kapitálovém trhu je tomu tak proto, že bitcoiny nevykazují znaky investičního nástroje podle § 3 ZKPT neboť nemají povahu cenného papíru a to ani zaknihovaného – mimo jiné proto, že v nich není vtěleno žádné právo a nevykazují ani znaky derivátu

Pojem cenného papíru je od prvního ledna 2014 upraven ustanovením § 514 Občanského zákoníku jako „*listina, se kterou je právo spojeno takovým způsobem, že je po vydání cenného papíru nelze bez této listiny uplatnit ani převést*“. Zaknihovaný papír je pak definován v § 525 jako zápis do příslušné evidence, který nahrazuje cenný papír a který nelze převést jinak, než zápisem do této evidence. Ustanovení pro cenné papíry se pak použijí též pro cenné papíry zaknihované, ledaže by to vylučovala jejich povaha nebo právní předpis.

V zákonném vymezení lze tedy odlišit následující znaky:

1. Musí se jednat o listinu (resp. zápis v evidenci v případě zaknihovaného cenného papíru).
2. S touto listinou musí být spojeno subjektivní právo
3. Toto právo musí být s listinou spojeno takovým způsobem, že je po vydání cenného papíru nelze bez této listiny uplatnit ani převést<sup>90</sup>.

Ačkoliv bitcoiny sdílí s cennými papíry některé znaky, opět se jedná o kategorii do které je nelze zařadit:

---

<sup>90</sup>KOTÁSEK, Josef. Cenný papír v § 514 NOBČZ. In: *Obchodněprávní revue: odborný recenzovaný časopis pro obchodní právo a právo finančních trhů*. Praha: C.H. Beck, 2013, s. 256. ISSN 1803-6554.

První podmínka, tedy aby se jednalo o listinu nebo zápis v evidenci bude evidentně splněna neboť bitcoiny lze bezpochyby vnímat i jako zápisy v distribuované databázi transakcí<sup>91</sup>.

Druhá podmínka, tedy aby s tímto záznamem bylo spojeno subjektivní právo však zřejmě splněna nebude neboť ačkoliv je s držetím bitcoinové adresy s určitým obnosem spojena možnost tento obnos odeslat na jinou adresu v bitcoinové síti nejedná se o subjektivní právo, tedy možnost chování vyjádřenou a zaručenou objektivním právem<sup>92</sup>, ale o technickou možnost, zapříčiněnou a chráněnou samotnou architekturou systému, při využití kryptografických principů. Zabývat se třetí podmínkou tedy bude již bezpředmětné, ale pro úplnost dodám, že tuto technickou možnost, která je spojena se záznamem v blockchainu skutečně také nelze uplatnit jinak, než ve spojení s tímto záznamem.

Proto nezbyvá, než se ztotožnit s názorem ČNB, že obchodování s bitcoinem a provoz bitcoinových „směnár a burz“ nespadá pod zákon o podnikání na kapitálovém trhu a nepodléhá proto doзору ČNB a povinnostem stanoveným tímto zákonem.

#### **4.4. Prodejci zboží a poskytovatelé služeb přijímající bitcoin**

Poměrně záhy po vzniku bitcoinového platebního systému se objevuje množství obchodníků, působících zejména v prostředí celosvětové sítě internet, kteří přijímají bitcoin jako platbu za zboží či služby. Tento počet se také neustále zvyšuje se stoupajícím povědomím o jeho existenci a funkcionalitě. Přesto se nedá v žádném případě říct, že by bitcoin byl masově využívanou formou peněz a jeho používání se omezuje spíše na nadšené uživatele a obchodníky.

Nicméně v dnešní době je již možné v globalizovaném prostředí internetu pořídit za bitcoin téměř cokoli, pokud je člověk ochoten akceptovat určité nepohodlí a čas strávený hledáním vhodného obchodníka příkladem mohou být třeba internetové obchody overstock.com a bitcoinstore.com.

Kromě toho se i v České republice (zejména v Praze) vyskytuje několik desítek obchodníků přijímajících bitcoin. I u nás tak lze za bitcoin posedět v baru, zakoupit boty,

<sup>91</sup> Viz například rozhovor „Tom Woods, talks to Eric Voorhees: What is Bitcoin?“, kde americký podnikatel v bitcoinové ekonomice Eric Voorhees popisuje bitcoin v překladu takto: „Bitcoin jsou v podstatě jen účetní záznamy v distribuovaném databázovém systému“ (dostupné na: <http://www.youtube.com/watch?v=yi2WgeJ73IE>)

<sup>92</sup> BOGUSZAK, Jiří, Jiří ČAPEK a Aleš GERLOCH. *Teorie práva*. 2., přeprac. vyd. Praha: ASPI, 2004, s. 115. ISBN 8073570300.

nechat si opravit kolo nebo třeba zaplatit školné v mateřské škole<sup>93</sup>. Vzhledem k výše citovanému stanovisku České národní banky, pak není při přijímání plateb v bitcoinech nutné dodržovat žádná zvláštní pravidla a stejně tak k němu není nutné povolení ČNB.

## **4.5. Poskytovatelé služeb souvisejících s používáním bitcoinového platebního systému**

Zejména se zde bude jednat o *webové bitcoinové peněženky*, tedy služby, jejichž podstatou je poskytování bitcoinové peněženky po účely přijímání a zasílání transakcí v rámci bitcoinového systému, přes webové aplikační rozhraní na základě registrace u jeho poskytovatele. Výhodou tohoto přístupu je jeho rychlost a jednoduchost, související s tím, že uživatel nepotřebuje provozovat bitcoinový klient na svém vlastním počítači. Odpadá mu tak i starost o zabezpečení vlastního počítače s peněženkou. Na druhou stranu to samé co pro někteří uživatelé vnímají jako výhodu, může být současně vnímáno jako slabina – uživatel používající webovou peněženku ztrácí fyzickou kontrolu nad svými penězi. Při tomto přístupu jsou totiž bitcoiny (resp. šifrovací klíče, které uživateli umožňují s nimi nakládat) uloženy na serverech poskytovatele webové peněženky provozovatel serverů nad nimi má kontrolu. Navíc se tyto servery často stávají terčem kybernetických útoků, s cílem zmocnit se zde uložených bitcoinů (V České republice je zejména známý případ útoku na servery provozovatele peněženky bitcash.cz v listopadu 2013, kdy se neznámému útočníkovi podařilo odcizit bitcoiny v hodnotě mezi třemi až čtyřmi miliony korun<sup>94</sup>).

Právní vztahy vznikající při poskytování této služby budou zřejmě založeny nepojmenovanou smlouvou, obsahující některé znaky smlouvy o úschově, upravené Občanským zákoníkem v ustanoveních §§ 2402 – 2408 pokud se jedná o uložení šifrovacích klíčů k bitcoinům uloženým na serverech poskytovatele některé znaky smlouvy příkazní upravené tímž předpisem v ustanoveních §§ 2430 – 2434 pokud jde o vyřizování poskytování a přijímání plateb.

K otázce nutnosti registrace a dohledu vydala ČNB stanovisko, ve kterém vyjadřuje následující názor: Vzhledem k tomu, že se nejedná o platební službu ve smyslu §3 zákona o platebním styku<sup>95</sup>, a to zvláště proto, že bitcoin nelze podřadit pod

<sup>93</sup>Viz například mapu obchodníků, přijímajících bitcoin: <http://coinmap.org>

<sup>94</sup> Rekonstrukce případu Bitcash.cz: Jak se kradou bitcoiny. In: BOŘÁNEK, Roman. *Root.cz* [online]. 2013 [cit. 2014-06-03]. Dostupné z: <http://www.root.cz/clanky/rekonstrukce-pripadu-bitcash-cz-jak-se-kradou-bitcoiny/>

<sup>95</sup>zákon č. 284/2009 Sb., O platebním styku



pojem peněžních prostředků upravených v ustanovení § 1 odst. 1 písm. c) - konkrétně bezhotovostních peněžních prostředků ani elektronických peněz upravených ustanovením § 4, není k této činnosti nutné povolení ČNB, ani tato činnost nepodléhá jejímu dohledu<sup>96</sup>.

## 5. Nelegální a společensky škodlivé činnosti spojované s bitcoinovým platebním systémem

Stejně tak, jako bývá bitcoinový systém považován za zásadní inovaci, která může do oblasti financí přinést mnoho pozitivního, objevují se i hlasy, které oprávněně poukazují na fakt, že ty samé vlastnosti, které ho činí jedinečnou alternativou jiným platebním systémům, mohou také umožňovat či usnadňovat některé společensky škodlivé a v některých případech protiprávní jednání. V tomto ohledu bývá nejčastěji skloňováno obchodování s omamnými a psychotropními látkami, praní špinavých peněz ale i financování terorismu a daňové úniky.

Tyto skutečnosti bývají také hlavními argumenty používanými zastánci právní regulace bitcoinu a podobných systémů, ve snaze eliminovat společensky nebezpečné chování, které se v souvislosti s kryptoměny<sup>97</sup> vyskytuje. Najdou se dokonce i autoři, kteří ho z těchto důvodů označují za „*nebezpečnou hrozbu pro západní svět*“ a kteří požadují buď jeho zařazení pod existující právní úpravu (nejčastěji pod kategorie upravující elektronické peníze a platební služby, bankovníctví nebo i pod právní úpravu cenných papírů) a nebo zavedení právní úpravy, která by ho úplně zakazovala či alespoň podstatně omezovala možnosti jeho použití<sup>98</sup>. Naproti tomu však lze zaslechnout také názory, podle mého názoru oprávněné, že nepromyšlená právní regulace kryptoměn by na jedné straně komplikovala jeho užití k legálním účelům, na druhé straně by zákazy a omezení jeho používání, vzhledem k povaze systému bylo velice obtížné vymáhat. Vedly by tak nakonec jen k tomu, že by se z bitcoinu skutečně staly jakési „*peníze zločinců*“ zapovězené běžné populaci a vytlačené z legální ekonomiky, současně však

<sup>96</sup>ČESKÁ NÁRODNÍ BANKA. *Obchodování s bitcoiny*. 10.2.2014. 2014. Dostupné z:

[http://www.cnb.cz/miranda2/export/sites/www.cnb.cz/cs/faq/obchodovani\\_s\\_bitcoiny.pdf](http://www.cnb.cz/miranda2/export/sites/www.cnb.cz/cs/faq/obchodovani_s_bitcoiny.pdf)

<sup>97</sup>Pojem kryptoměny souhrnně označuje bitcoin a jemu podobné systémy založené na aplikaci kryptografie

<sup>98</sup>viz např. TWOMEY, Peter. Halting a shift in paradigm: The need for bitcoin regulation. *HeinOnline*. 2013

stále používané (teď již především) k nekalým účelům osobami, které se rozhodnou nerespektovat zákonné zákazy<sup>99</sup>.

Hlavní charakteristiky bitcoinu, které z něj dělají nástroj vhodný pro tyto škodlivé činnosti jsou anonymita (resp. pseudonymita) transakcí a absence centrální autority, která by disponovala pravomocí (a také faktickou možností) vykonávat nad nimi dozor.

Nyní se na dvě skupiny škodlivých činností nejčastěji spojovaných s používáním bitcoinového systému podíváme blíže. Bude to právě obchodování s omamnými a psychotropními látkami a praní špinavých peněz.

## 5.1. Bitcoinový platební systém a praní špinavých peněz

Praní špinavých peněz je světově používaný termín pro legalizaci výnosů z trestné činnosti. Není tedy úplně přesný, neboť označuje legalizaci všech výnosů, nikoliv jen výnosů ve formě peněz (ale i např. drahých kamenů, cenných papírů a jakéhokoli jiného majetku). Legalizací tu rozumíme proces resp. činnost, při které jde o zastření nelegálního původu majetku a navození zdání jeho nabytí v souladu s právem. Jde v podstatě o poslední fázi utajování trestné (či v širším pojetí vůbec protiprávní) činnosti. To má následně umožnit jejich použití v legální sféře ekonomiky.

Na mezinárodní úrovni byl boj proti praní špinavých peněz nejprve zaměřen na výnosy z obchodu s drogami, ale později se rozšířil na všechny druhy výnosů z trestné činnosti.

Mezinárodním standardem a materiálním pramenem právní úpravy boje proti legalizaci výnosů z trestné činnosti se celosvětově stala doporučení výboru skupiny G7 Financial Action Task Force on Money Laundering (dále jen FATF). Konkrétně se jedná o „40 doporučení FATF v boji proti praní peněz“, vydaných v roce 1990 a 9 takzvaných „zvláštních doporučení“ zaměřených na potírání financování terorismu, vydaných v roce 2001. Obsahem těchto dokumentů jsou doporučení směřující ke stanovení povinností subjektům, u kterých hrozí zneužití jejich činnosti pro praní špinavých peněz (banky, instituce elektronických peněz).

Tyto povinnosti spočívají zejména v hlášení transakcí vyvolávajících podezření z takové činnosti a identifikace a kontroly klientů a zřízení zvláštních útvarů pověřených

---

<sup>99</sup>viz např. KAPLANOV, Nikolei M. Nerdy Money: Bitcoin, The Private Digital Currency, And The Case Against Its Regulation. In: *Loyola Consumer Law Review*. Chicago US, 2013, 167 an.

přijímáním a prošetřováním těchto podezření, obecně označovaných jako „finanční zpravodajské jednotky“. V České republice je takovou jednotkou *Finanční analytický útvar*, založený v rámci Ministerstva financí k datu účinnosti zákona č. 61/1996 Sb., O některých opatřeních proti legalizaci výnosů z trestné činnosti. Tento útvar je finanční zpravodajskou jednotkou *administrativního typu*, které se od jednotek *policejního typu* (jaká funguje například ve Slovenské republice), liší tím, že má obecně širší a volnější přístup k informacím z finančního sektoru (bankovníctví, obchod s cennými papíry, někdy i údaje získané v rámci daňového řízení), obvykle bez nutnosti souhlasu soudce či státního zástupce, a má stanoveno, v jakých případech může tyto informace předat policejním orgánům, či jiným orgánům činným v trestním řízení.

Vzhledem k tomu, že opatření proti praní špinavých peněz jsou založena na identifikaci klientů, vymezení povinných osob a uchovávání a poskytování informací o proběhlých transakcích, je nepochybné, že s bitcoinovým platebním systémem je spojeno riziko obcházení těchto opatření. Je tomu tak zejména proto, že existující právní předpisy zřídka reflektují existenci podobných systémů a nezahrnují tak subjekty poskytující související služby mezi povinné subjekty (navíc jedním z hlavních rysů bitcoinového systému je i fakt, že strany mohou provádět transakce přímo, bez využití jakékoli třetí osoby), a také to, že ačkoliv všechny proběhlé transakce v bitcoinovém systému jsou evidovány ve veřejně přístupném záznamu – blockchainu, nejsou tyto údaje samy o sobě spojeny s ničím co by identifikovalo jednotlivé strany transakce jako osoby ve fyzickém světě.

Dá se říci, že tyto zpravodajské jednotky po celém světě si uvědomují rizika spojená s existencí a charakteristickými vlastnostmi bitcoinového systému i to, jakým způsobem je možné je zneužívat k praní špinavých peněz – to dokládají jimi vydávané dokumenty různého charakteru podle jejich právní závaznosti. Na celosvětové úrovni to může být například příručka FATF varující před riziky předplacených karet, mobilních plateb a internetových platebních služeb<sup>100</sup>, na evropské úrovni třeba varování Evropského orgánu pro bankovníctví (EBA), které zejména informuje spotřebitele o rizicích spojených s užíváním a obchodováním s virtuálními měnami (zejména možnost jejich odcizení formou kybernetického útoku a dramatickými výkyvy jejich ceny na trhu) ale také varuje před možnostmi jejich zneužívání k trestné činnosti včetně praní

<sup>100</sup>FINANCIAL ACTION TASK FORCE ON MONEY LAUNDERING. *Guidance for a risk based approach: Prepaid cards, mobile payments and internet-based payment services*. 2013. Dostupné z: <http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf>

špinavých peněz<sup>101</sup> či dokument Virtual Currency Schemes vydaný Evropskou centrální bankou<sup>102</sup>.

Hlavními prameny práva v boji proti praní špinavých peněz v České republice jsou jednak právní předpisy Evropské unie představované směrnicí 2005/60/ES, *O předcházení zneužití finančního systému k praní peněz a financování terorismu*, nařízením č. 1889/2005, *O kontrolách peněžní hotovosti vstupující do Společenství* nebo je opouštějící a nařízením č. 1781/2006, *O informacích o plátcích doprovázejících převody peněžních prostředků*. Co se týče vnitrostátních předpisů v České republice, bude hlavní roli hrát zákon č. 253/2008 Sb., *o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu* (dále jen AML<sup>103</sup> zákon) a také zákon č. 254/2004 Sb., *o omezení plateb v hotovosti a o změně zákona č. 337/1992 Sb., o správě daní a poplatků, ve znění pozdějších předpisů* (dále jen zákon o omezení plateb v hotovosti).

AML zákon mimo jiné vymezuje pojem legalizace výnosů z trestné činnosti a financování terorismu, určuje tzv. *povinné osoby*, tedy osoby, kterým jsou ukládány povinnosti v rámci opatření proti praní špinavých peněz, vymezuje pojem podezřelého obchodu a povinnosti povinných osob, spočívající zejména ve stanovení systému vnitřních zásad, identifikaci klienta, uchovávání podstatných informací o proběhlých obchodech, oznamování podezřelých obchodů. Dále také upravuje činnosti Ministerstva financí v této oblasti – zejména způsob, jakým ministerstvo získává a zpracovává informace, nakládá s výsledky šetření včetně podávání trestního oznámení v případě že jsou zjištěny skutečnosti nasvědčující tomu, že byl spáchán trestný čin (legalizace výnosů z trestné činnosti – a to jak úmyslná, tak za určitých podmínek i nedbalostní je trestným činem podle §§ 216 a 217 trestního zákoníku<sup>104</sup>) a činnost spočívající v dozoru nad plněním povinností z tohoto zákona. Upravuje také povinnost mlčenlivosti, mezinárodní spolupráci a stanoví správní delikty spočívající v porušení povinností podle tohoto zákona a sankce za ně.

Zákon o omezení plateb v hotovosti pak ve svých devíti paragrafech určuje, kdy jsou právnícké a fyzické osoby povinny provést platbu bezhotovostním způsobem

<sup>101</sup>EUROPEAN BANKING AUTHORITY. *Warning to consumers on virtual currencies*. 2013. Dostupné z: <https://www.eba.europa.eu/documents/10180/598344/EBA+Warning+on+Virtual+Currencies.pdf>

<sup>102</sup>EUROPEAN CENTRAL BANK. *Virtual Currency Schemes*. 2012. Dostupné z: <http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>

<sup>103</sup>Anti money laundering- angl. proti praní peněz

<sup>104</sup>Zákon č. 40/2009 Sb., trestní zákoník

(jedná se zejména o platby nad limit 350 000 Kč prováděné osobami s místem trvalého pobytu, místem pobytu či sídlem na území české republiky pokud nejsou tímto zákonem vyloučeny), vymezuje pojmy bezhotovostní a hotovostní platby a určuje související správní delikty a sankce za ně.

V České republice se bitcoinovým platebním systémem v ohledu na rizika praní špinavých peněz zabýval právě Finanční analytický útvar Ministerstva Financí, který v září 2013 vydal metodický pokyn „*O přístupu povinných osob k digitálním měnám*“ určený osobám povinným podle AML zákona, kde označuje platby prostřednictvím bitcoinového systému v tomto ohledu za rizikové a kterým vyzývá povinné osoby, aby „*V souvislosti s nákupem/prodejem jakékoli digitální měny, jako je například Bitcoin, byla jako velmi riziková k posouzení a k rozhodnutí o dalších opatřeních podle okolností každá platba nad hodnotu 1.000 EUR a vždy jako podezřelý obchod postupem podle § 18 AML zákona oznámena transakce nad hodnotu 15.000 EUR.*“<sup>105</sup> V tomto ohledu je však vhodné zdůraznit, že přesto, že povinnými osobami podle §2 AML zákona je poměrně široký okruh osob, zahrnující zejména banky, spořitelní a úvěrová družstva a jiné finanční a platební instituce, ale i mnoho dalších osob, podle vyjádření České národní banky samotný nákup a prodej bitcoinu statut povinné osoby nezakládá<sup>106</sup>.

V blízké budoucnosti lze pravděpodobně očekávat změnu právních norem tak, aby osoby nakládající s bitcoiny (směnárny, burzy, provozovatelé peněženek) byly zařazeny mezi povinné osoby podle předpisů o praní špinavých peněz. V tomto ohledu bude jistě zajímavé stanovisko připravované pracovní skupinou *Taskforce on Virtual Currencies* Evropského orgánu pro bankovníctví, které může být určující pro další vývoj legislativy na evropské úrovni. Podle dostupných informací pak i Finanční analytický úřad Ministerstva financí připravuje novelu AML zákona, která má zahrnout mezi osoby povinné právě i zprostředkovatele a poskytovatele služeb spojených s virtuálními měnami. Důsledkem toho by byl fakt, že by se na tyto subjekty vztahovaly všechny povinnosti, vyplývající z tohoto zákona, včetně povinnosti uchovávat a poskytovat záznamy o všech proběhlých obchodech<sup>107</sup>.

<sup>105</sup>Dostupné na [http://www.mfcr.cz/assets/cs/media/Pokyn-MF\\_c-002\\_2013-09\\_Metodicky-pokyn-o-pristupu-povinnych-osob-k-digitalnim-menam.pdf](http://www.mfcr.cz/assets/cs/media/Pokyn-MF_c-002_2013-09_Metodicky-pokyn-o-pristupu-povinnych-osob-k-digitalnim-menam.pdf)

<sup>106</sup>ČESKÁ NÁRODNÍ BANKA. *Obchodování s bitcoiny*. 10.2.2014. 2014. Dostupné z: [http://www.cnb.cz/miranda2/export/sites/www.cnb.cz/cs/faq/obchodovani\\_s\\_bitcoiny.pdf](http://www.cnb.cz/miranda2/export/sites/www.cnb.cz/cs/faq/obchodovani_s_bitcoiny.pdf)

<sup>107</sup>TVRDÝ, Jiří. Virtuální měny z pohledu AML/CFT opatření: současnost a očekávaný vývoj. In: *Zkušenosti s virtuálními měnami - Bitcoin měna budoucnosti?: Sborník z konference*. Praha, 2014, s. 109-114. Dostupné z: <http://ekon.konference.vsmie.cz/zkusenosti->

Zbývá také ještě zmínit vztah bitcoinového platebního systému a *zákona č. 254/2004 Sb., o omezení plateb v hotovosti*. Ten určuje, kdy jsou fyzické a právnické osoby povinny provést platbu bezhotovostně, prostřednictvím osoby oprávněné poskytovat platební služby nebo provozovatele poštovních služeb. Limitem, nad který je poskytovatel platby povinen využít služby některé z osob určených podle tohoto zákona je 350 000 Kč (tedy zhruba 30 BTC). Ačkoliv by se na první pohled mohlo zdát, že bitcoin vyhovuje požadavku na bezhotovostní formu platby, není tomu tak: § 2 odst. 1 písm. a) stanoví, že pro účely tohoto zákona se bezhotovostní platbou rozumí

*„platba provedená bezhotovostním převodem peněžních prostředků na území České republiky prostřednictvím peněžního ústavu v české nebo cizí měně a bezhotovostním převodem peněžních prostředků prostřednictvím peněžního ústavu v české nebo cizí měně z území České republiky na území jiného státu“*

Platba v bitcoinu tak zcela zřejmě nebude provedena prostřednictvím peněžního ústavu, ani v české nebo cizí měně (neboť jak jsme již zjistili bitcoin nelze považovat za měnu). Je proto nutné konstatovat, že na platby prostřednictvím bitcoinového platebního systému se uplatní omezení stanovená tímto zákonem, a nejvyšší přípustná platba tak bude činit při současném kurzu něco okolo 30 BTC. Porušení tohoto omezení je správním deliktem, za který lze uložit pokuty ve výši až 500 000 Kč fyzickým osobám a až 5 000 000 Kč právnickým a podnikajícím fyzickým osobám.

## **5.2. Bitcoinový platební systém a nelegální obchod s omamnými a psychotropními látkami**

Vlastnosti bitcoinového platebního systému lze kromě praní špinavých peněz zneužít i jinými způsoby, mezi nimiž kraluje jeho použití k obchodu s nelegálními substancemi.

Opravdu také, jedna ze skutečností, kterou se bitcoin nechvalně proslavil, je jeho spojení s internetovým tržištěm Silk Road<sup>108</sup>. Na něm se až do jeho rozbití ze strany FBI v září 2013 v podstatných objemech obchodovalo zejména s omamnými a psychotropními látkami, ale i pornografií a kradenými a padělanými doklady. Tržiště na

---

[s-virtualnimi-menami/data/sbornik\\_bitcoin\\_2014\\_web.pdf](#)

<sup>108</sup> Angl. Hedvábná stezka – název odkazuje na starodávnou obchodní trasu mezi Evropou a Asií

serverech připojených do anonymizační sítě Tor<sup>109</sup>, což umožňovalo skrývat identitu prodávajících, nakupujících i provozovatelů. Platby potom probíhaly výhradně prostřednictvím bitcoinového platebního systému a zásilky byly zasílány přes běžný poštovní systém. Díky tomu stránka fungovala od února 2011 do září 2013 aniž by bylo možné identifikovat provozovatele nebo umístění serverů na kterých bylo tržiště hostováno.

Screenshot online drogového tržiště Silk Road, všimněte si zejména kategorií zboží v panelu na levé straně obrazovky

Působilo na něm asi 550 prodávajících, z nichž polovina jako místo obchodování uváděla USA a asi 140 000 registrovaných uživatelů. Jeho roční obrat je odhadován na 15 milionů USD. Co se týče vztahu k bitcoinové ekonomice, odhaduje se, že asi 4.5% bitcoinových transakcí v době jeho fungování představovaly právě platby za zboží zakoupené na Silk Road. Všechny tyto propočty je ale dobré brát poněkud s rezervou, neboť se jedná jen o více či méně přesné odhady<sup>110</sup>.

Ačkoliv technické provedení tržiště prakticky znemožňovalo odhalení identity provozovatelů i uživatelů, byl nakonec v roce 2013 odhalen jeho zakladatel a

<sup>109</sup>Bližší informace o principech fungování této sítě lze najít na stránkách projektu Tor <https://www.torproject.org/>

<sup>110</sup>CHRISTIN. *Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace*. 2012. Dostupné z: <http://www.andrew.cmu.edu/user/nicolasc/publications/TR-CMU-CyLab-12-018.pdf>

provozovatel Ross William Ulbricht, známý pod pseudonymem Dread Pirate Roberts (či jen DPR). Tím, co nakonec vedlo k odhalení a rozbití tržiště nebyla slabina v technickém provedení sítě Tor či bitcoinu, ale detektivní práce FBI a několik chyb, kterých se DPR dopustil, díky čemuž se povedlo spojit jeho aktivitu na tržišti Silk Road s jeho aktivitami na běžné síti internet a posléze i s jeho profilem na profesionální sociální síti LinkedIn<sup>111</sup>.

Ačkoliv se od té doby neobjevilo žádné obdobné tržiště podobného rozsahu, případ Silk Roadu podstatným způsobem poškodil bitcoin v očích veřejnosti i úřadů. Je však důležité si uvědomit, že se jedná jen o jeden, byť neblaze proslulý případ, a že samotný fakt, že bitcoin lze používat i k takovýmto účelům, z něj samo o sobě nedělá škodlivou technologii, spíše jen technologii, která může být za určitých podmínek zneužita. Obdobně je to ostatně se všemi technologiemi – skvělým případem může být například jaderná energie, nebo ostatně i hotovostní oběživo. Co je ovšem výzvou do budoucna, je vytvoření zábranných mechanismů proti jejímu zneužití, které je nutné vytvářet s ohledem k jeho legitimním uživatelům a za pochopení technologických principů bitcoinového systému.

## **6. Regulace bitcoinového platebního systému u nás a ve světě de lege ferenda**

Tak, jak se rozšiřuje počet uživatelů bitcoinového platebního systému a s tím i možné způsoby jeho využití, začínají se stále více objevovat hlasy volající po jeho explicitní právní úpravě, nebo zařazení pod existující úpravu platebního styku. Zvláště důraznými podněty pro jeho úpravu pak jsou případy, ve kterých byl bitcoinový platební systém zneužit k usnadnění nezákonné činnosti – můžeme tu uvést zejména výše zmiňované tržiště s omamnými látkami, *Silk Road*.

Nejen v akademické sféře se pak začíná odvíjet debata o tom, zda vůbec a jakým způsobem, by de lege ferenda měly být tyto platební systémy upraveny. Zastánci regulace tvrdí, že jejich nekontrolovaný vývoj může představovat vážný zdroj nestability pro finanční trhy, způsob jak se vyhnout opatřením proti praní špinavých peněz, a omezení možnosti států ovlivňovat hospodářské procesy formou měnové

---

<sup>111</sup>Viz například HUME, Tim. How FBI caught Ross Ulbricht, alleged creator of criminal marketplace Silk Road. *CNN International* [online]. [cit. 2014-06-14]. Dostupné z: <http://edition.cnn.com/2013/10/04/world/americas/silk-road-ross-ulbricht/>



politiky a že je tedy vhodné kryptoměny buď podřídit kontrole ze strany státu a nebo v krajních případech rovnou úplně zničit<sup>112</sup>. Na druhé straně jsou autoři, kteří tvrdí, že při pokusech regulovat tyto systémy je na místě opatrnost. Že je důležité postupovat tak, aby nedošlo k narušení vývoje, jenž má potenciál změnit v mnohém podobu finančních trhů k lepšímu i kdyby jen jako alternativa tradičních způsobů provádění plateb. Tvrdí také, že nepřiměřené zásahy by mohly být jednak velice nákladné a vzhledem k povaze bitcoinu také velmi pravděpodobně neefektivní, a že by mohly mít negativní vliv na ekonomiku<sup>113</sup> (i kdyby jen v tom smyslu, že by se podobné technické inovace nadále odehrávaly ve státech, které k nim připraví vhodné podmínky)<sup>114</sup>. Oba pohledy jsou do jisté míry oprávněné a podle mého názoru může nová podoba právní regulace vyvstat jen z důkladné a svobodné diskuze mezi oběma tábory.

Tak jak stoupá popularita bitcoinového platebního systému, stále větší množství státních orgánů po celém světě začíná pociťovat potřebu změny stávající právní úpravy tak, aby reflektovala existenci tohoto a obdobných platebních systémů. Motivy k regulaci jsou různé: od získání způsobu jak zabránit jeho zneužití, až po ochranu spotřebitelů před amatérsky provozovanými burzami a webovými peněženkami, které mohou být buď řízeny s nedostatečnou odborností, nebo být nedostatečně zabezpečené proti kybernetickým útokům<sup>115</sup>. Ve světě se postupně objevují nové případy rozhodnutí státních orgánů, reflektujících existenci bitcoinového platebního systému a činností s ním souvisejících<sup>116</sup>. Ani Česká republika se zřejmě nevyhne potřebě změny právní úpravy tak, aby odrážela existenci tohoto platebního systému. Vzhledem k tomu, že je členem Evropské unie, a vzhledem ke globálnímu charakteru bitcoinové sítě se dá očekávat, že diskuze nad tvorbou nové právní úpravy bude probíhat nejen na národní úrovni, ale také na úrovni evropské a globální.

Dosud vzniklé dokumenty mají zejména povahu stanovisek k postavení bitcoinového systému v právních rádech *de lege lata*, nebo povahu právně nezávazných doporučení či varování obyvatelstva před nástrahami tohoto systému.

---

<sup>112</sup>Viz například TWOMEY, Peter. Halting a shift in paradigm: The need for bitcoin regulation. *HeinOnline*. 2013, č. 16.

<sup>113</sup>tzv. chilling effect

<sup>114</sup>Viz například KAPLANOV, Nikolei M. Nerdy Money: Bitcoin, The Private Digital Currency, And The Case Against Its Regulation. In: *Loyola Consumer Law Review*. Chicago US, 2013.

<sup>115</sup>Viz například případ burzy MtGox, nebo českého provozovatele webové penženky bitcoincash.cz, o obou jsme se již v této práci zmínili.

<sup>116</sup>Bitcoin regulation news. *CoinDesk: The Voice of digital currency* [online]. [cit. 2014-06-16]. Dostupné z: <http://www.coindesk.com/regulation/>

V první skupině je možné jmenovat zejména stanovisko České národní banky, které vyjasňuje svůj pohled na tuto materii<sup>117</sup> a obdobné stanovisko německého ministerstva financí<sup>118</sup>.

V druhé skupině, tedy ve skupině právně nezávazných doporučení, lze uvést zejména příručku FATF skupiny G7 varující před riziky předplacených karet, mobilních plateb a internetových platebních služeb<sup>119</sup>, „*Varování pro spotřebitele týkající se virtuálních měn*“ Evropského orgánu pro bankovnínictví (EBA), informující spotřebitele před hrozbami, které s sebou může přinášet užívání virtuálních měn – včetně kybernetických útoků, dramatických výkyvů cen a možností zneužití k trestné činnosti<sup>120</sup>. Všechny tyto dokumenty v podstatě varují před hrozbami, které může neregulované používání kryptoměn přinášet, ale nepodávají odpověď na otázku jak by měla vypadat vhodná úprava těchto systémů.

EBA nicméně již v roce 2013 založila pracovní skupinu – *Taskforce on virtual currencies* od které se v nejbližší době očekává stanovisko, které by se mohlo stát základem pro budoucí právní úpravu na evropské úrovni.

Podle dostupných informací se změny v právní úpravě chystají také na vnitrostátní úrovni: Finanční analytický útvar Ministerstva financí připravuje novelu AML zákona, která by kromě změn v AML předpisech EU měla promítnout také opatření z výše zmiňovaného připravovaného stanoviska pracovní skupiny EBA pro virtuální měny. Podle vyjádření Mgr. Tvrdého, zástupce ředitele FAÚ MF touto novelou také pravděpodobně dojde k zahrnutí zprostředkovatelů a poskytovatelů služeb spojených s virtuálními měnami mezi osoby povinné podle AML zákona<sup>121</sup>.

Ačkoliv je tedy v současné době bitcoin stále v poněkud šedé zóně a jeho postavení v právním řádu je přinejmenším nejisté, do budoucna se dá jistě očekávat jeho

---

<sup>117</sup>ČESKÁ NÁRODNÍ BANKA. *Obchodování s bitcoiny*. 10.2.2014. 2014. Dostupné z: [http://www.cnb.cz/miranda2/export/sites/www.cnb.cz/cs/faq/obchodovani\\_s\\_bitcoiny.pdf](http://www.cnb.cz/miranda2/export/sites/www.cnb.cz/cs/faq/obchodovani_s_bitcoiny.pdf)

<sup>118</sup>Viz např. <http://www.spiegel.de/netzwelt/netzpolitik/finanzministerium-erkennt-bitcoins-als-zahlungsmittel-an-a-917151.html>

<sup>119</sup>FINANCIAL ACTION TASK FORCE ON MONEY LAUNDERING. *Guidance for a risk based approach: Prepaid cards, mobile payments and internet-based payment services*. 2013. Dostupné z: <http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf>

<sup>120</sup>Plný text v českém překladu na stránkách ČNB:

[www.cnb.cz/miranda2/export/sites/www.cnb.cz/cs/dohled\\_financni\\_trh/novinky/download/EBA\\_2013\\_varovani\\_bitcoin.pdf](http://www.cnb.cz/miranda2/export/sites/www.cnb.cz/cs/dohled_financni_trh/novinky/download/EBA_2013_varovani_bitcoin.pdf)

<sup>121</sup>TVRDÝ, Jiří. Virtuální měny z pohledu AML/CFT opatření: současnost a očekávaný vývoj. In: *Zkušenosti s virtuálními měnami - Bitcoin měna budoucnosti?: Sborník z konference*. Praha, 2014, s. 109-114. Dostupné z: [http://ekon.konference.vsmie.cz/zkusenosti-s-virtualnimi-menami/data/sbornik\\_bitcoin\\_2014\\_web.pdf](http://ekon.konference.vsmie.cz/zkusenosti-s-virtualnimi-menami/data/sbornik_bitcoin_2014_web.pdf)

zahrnutí mezi existující instituty v systému norem upravujících platební styk a opatření proti legalizaci výnosů z trestné činnosti.

## 7. Další možnosti využití

Úplně na závěr práce bych rád zmínil, že technologické principy, které zavádí bitcoinový platební systém mohou mít i další perspektivní způsoby využití. Jedná se především o nové způsoby využití systému tvorby a udržování decentralizovaného záznamu-blockchainu<sup>122</sup>, který ho činí unikátním. Možné další aplikace zahrnují zejména systémy registrace domén, důkazy existence digitálního dokumentu (tzv. *proof of existence*) nebo důkazy o udělení práv k použití dokumentu v konkrétním čase<sup>123</sup>. Tyto další aplikace mohou buď přímo využívat blockchain tvořený bitcoinovým platebním systémem, nebo vytvářet vlastní obdobný záznam, postavený na stejném principu „*decentralizované důvěry*“.

V této souvislosti se objevuje také termín *Smart contracts*<sup>124</sup>, jedná se o počítačové protokoly, které eliminují nutnost důvěry mezi stranami zcela jiným způsobem, než tak činí současné právo. Jedná se vlastně o kusy počítačového kódu, které samostatně zajistí splnění závazku ze smlouvy, dojde-li k naplnění určité podmínky – ukázkou smart contractu z běžného života může být například prodejní automat. Kupní smlouva je tu uzavřena mezi prodejcem zboží a nakupujícím, ale v okamžiku vhození odpovídající částky je splnění kupní smlouvy vynuceno vnitřním uspořádáním automatu tedy bez ohledu na vůli prodávajícího. Tento typ smluv se může ukázat jako velice praktický v prostředí počítačových sítí, kde je důvěra mezi stranami a právní donucení ke splnění závazku poměrně komplikovanou záležitostí. Aplikace využívající tohoto principu jsou však v současné době téměř výhradně ve fázi konceptů<sup>125</sup>. V každém případě, možnosti kryptoměn a od nich odvozených systémů ještě zdaleka nejsou vyčerpány.

---

<sup>122</sup><https://en.bitcoin.it/wiki/Contracts>

<sup>123</sup>How the Bitcoin Protocol Could Help Improve Copyright. In: *Slate Magazine* [online]. 2014 [cit. 2014-02-24]. Dostupné z: [http://www.slate.com/blogs/future\\_tense/2014/02/17/bitcoin\\_protocol\\_could\\_help\\_improve\\_copyright.html](http://www.slate.com/blogs/future_tense/2014/02/17/bitcoin_protocol_could_help_improve_copyright.html)

<sup>124</sup>Chytré kontrakty, smlouvy

<sup>125</sup>Way Beyond Bitcoin: The Coming of "Smart Contracts. In: *Economic Policy Journal* [online]. 2014 [cit. 2014-07-01]. Dostupné z: <http://www.economicpolicyjournal.com/2014/01/way-beyond-bitcoin-coming-of-smart.html>

## Závěr

Bitcoinový platební systém je fascinující, v mnoha aspektech průlomovou inovací v platebním styku. Mezi jeho odlišující charakteristiky patří absence centrální autority a prostředníků při provádění transakcí, pseudonymita stran, existence veřejně přístupného záznamu o veškerých transakcích, které v systému proběhnou, zvláštní způsob emise nových mincí, rychlost transakcí zcela bez ohledu na geografickou polohu stran, i otevřený způsob, kterým probíhá jeho vývoj jako open-source softwaru.

Decentralizovanost jeho architektury a skutečnost, že zdrojový kód je přístupný dohledu ze strany veřejnosti činí systém jako takový poměrně velmi bezpečným a stabilním.

Jeho zvláštnosti z něj dělají životaschopnou konkurenci ostatním aplikacím na tomto poli zejména v oblasti mezinárodních plateb a mikroplateb. Ačkoliv se v současné době nejedná o masově rozšířený způsob provádění plateb, jeho uživatelů stále přibývá a s nimi přibývají i služby s tímto spojené a způsoby, kterými lze realizovat jeho ekonomické funkce jako inovativního druhu peněz.

Co se týče právní úpravy tohoto a i jemu vývojově a technicky podobných systémů, je nutné konstatovat, že současná podoba právních systémů většiny zemí světa, včetně České republiky, dosud nereflektuje jeho existenci, což přináší obtíže při vyjasňování jeho postavení v právním řádu a určení práv a povinností osob ve společenských vztazích, realizujících se v souvislosti s jeho používáním. Specifika bitcoinového platebního systému činí obtíže při pokusech zařadit ho do existujících, právem upravených kategorií.

Přesto se podařilo vytyčit některé právní kategorie, pod které je možné ho subsumovat. Podle výsledků provedené právní analýzy je možné jej bez větších problémů zařadit pod pojem věci v právním slova smyslu a to věci nehmotné, movité, zastupitelné a užitelné. To má za důsledek fakt, že na něj dopadá velké množství právních norem, především soukromoprávních, které implicitně obsahují pojem věci ve své hypotéze.

Vzhledem k tomu, že je nepochybně způsobilý plnit funkce, které finanční věda přisuzuje penězům, jako jsou funkce denominátoru hodnoty, všeobecného prostředku směny, plateb a převodu kapitálu i uchovatele hodnoty, lze jej také považovat za formu peněz svého druhu.

Naproti pod kategorii měny není bitcoin možné subsumovat, i přesto že toto označení bývá v souvislosti s ním opětovně používáno. Pojem měny je totiž na rozdíl od pojmu peněz kategorií ryze právní a je neoddělitelně svázán s uznáním ze strany státu či jiného veřejnoprávního společenství. Bitcoinu není statut měny přiznán právním řádem žádného státu světa a vzhledem k obtížím s tím spojeným, se nic takového nedá reálně, alespoň v blízké budoucnosti, očekávat.

Poněkud překvapivá může být skutečnost, že bitcoin nelze, navzdory jeho elektronické povaze zařadit do kategorie elektronických peněz. Důvodem k tomu, je způsob jakým je bitcoin emitován, tedy jako odměna za vytěžené transakční bloky. Nepředstavuje tedy pohledávku za jeho vydavatelem a proto ho nelze považovat za elektronické peníze podle zákona o platebním styku, ani podle evropské úpravy, kterou tento zákon implementuje.

Stejně tak není možné jej zařadit pod kategorii cenných papírů, upravené občanským zákoníkem. Cenné papíry jsou totiž listiny, se kterými je spojeno právo takovým způsobem, že ho bez této listiny nelze uplatnit ani převést. Zaknihované cenné papíry jsou pak záznamy v evidenci, které nahrazují takovou listinu. Bitcoin, přestože jeho podstatou je záznam v evidenci proběhlých transakcí, není cenným papírem, a to z toho důvodu, že s ním žádné subjektivní právo spojeno není.

V okolí bitcoinového platebního systému se vyvíjí pestrá síť společenských vztahů hospodářské i právní povahy, vznikají nové projekty zajišťující možnosti směny bitcoinu za národní měny i nákupu zboží a služeb. Tyto entity můžeme zařadit do několika kategorií: uživatelé, vývojáři, obchodníci, burzy a směnárny a poskytovatelé služeb, které s bitcoinovým systémem souvisejí.

Určení práv a povinností osob z těchto vztahů je však nelehkým úkolem a zařazení pod existující právní normy ve většině případů selhává, neboť existující právní rámec vůbec nepočítá s existencí systémů podobných tomu bitcoinovému. Ze stejného důvodu pak dochází k tomu, že oblasti, které jsou v případě použití jiné formy peněz právně regulovány v tomto případě regulovány nejsou – to ostatně konstatuje ve svém stanovisku i Česká národní banka.

Některé skupiny těchto subjektů – zejména směnárny, burzy a poskytovatelé webových peněženek by byly v případě vzniku nové právní úpravy vhodným subjektem práv a povinností, neboť představují faktická centra v jinak decentralizovaném systému.

Se specifickými znaky bitcoinového platebního systému jsou kromě některých nesporných výše zmíněných výhod spojena také některá stejně nesporná nebezpečí. Tato nebezpečí pramení zejména z nestability jeho ceny na trhu, pseudonymity transakcí a právě z faktu, že ho často není možné zařadit pod mechanismy, zajišťující zajištění platebních systémů před zneužitím.

U bitcoinového systému existuje hrozba zneužití, zejména k legalizaci výnosů z trestné činnosti a obchodu s omamnými a psychotropními látkami, k čemuž také doopravdy dochází, což jsme ilustrovali na případu, dnes již zaniklého, drogového on-line tržiště Silk Road.

Rizika spojená s virtuálními měnami si uvědomují orgány pečující o stabilitu národních měn, pověřené dohledem nad finančními trhy, i orgány, kterým je svěřen dozor nad dodržováním opatření proti praní špinavých peněz a financování terorismu.

Právě z těchto důvodů se odehrává celosvětová debata na téma, zda a jakým způsobem je do budoucna vhodné přijmout změny v právní úpravě tak, aby byla eliminována některá výše zmíněná nebezpečí. Jak na straně obhájců, tak na straně odpůrců explicitní právní úpravy virtuálních měn je možné slyšet rozumné argumenty. Je proto nutné, aby budoucí právní úprava vznikla na základě důkladné, svobodné a otevřené debaty na toto téma a aby byla zváženy všechny ekonomické, společenské a kulturní dopady, které tato právní úprava může přinést.

Známky toho, že, i mimo akademickou sféru a komunitu technologických nadšenců, začínají státní i nestátní aktéři brát zřetel na existenci tohoto systému, se projevují na globální, evropské i národní úrovni. Zejména se tu jedná o přijímání dokumentů různé právní povahy: Strategických dokumentů analyzujících rizika spojená s neregulovaným užíváním bitcoinového systému a možné podoby budoucí právní úpravy, varování orgánů veřejné moci před těmito riziky a závazných či nezávazných stanovisek, spojených s výkladem platných právních norem ve vztahu k virtuálním měnám.

Ačkoliv ucelená právní úprava doposud nikde přijata nebyla, na globální, evropské i národní úrovni jsou ustavovány pracovní skupiny pověřené analýzou současného stavu a přípravou návrhů předpisů, které by zařadily bitcoinový platební systém a související služby do existujících kontrolních mechanismů.

Do budoucna lze také očekávat další vývoj bitcoinového a obdobných platebních systémů a také vznik dalších aplikací založených na technologických inovacích, které

tyto systémy přinesly – zejména aplikace využívající průlomový způsob tvorby decentralizovaného a přesto důvěryhodného záznamu o proběhlých skutečnostech, který je použit v jádru bitcoinové architektury.

Bitcoin a jemu podobné systémy ukazují, že vývoj na poli plateb a forem peněz ještě zdaleka není u konce. A přesto, že právní věda z podstaty věci nutně zaostává za technologickým pokrokem, nezbyde jí než se pokusit pochopit základy této i dalších technologií a zařadit je do existujících právních rámců, i přesto, že to může znamenat nutnost změn v tradičním chápání mnoha právních institutů.

## Seznam použitých zdrojů

- 1) POLČÁK, Radim. *Právo na internetu: spam a odpovědnost ISP*. Vyd. 1. Brno: Computer Press, 2007, s. 23. ISBN 978-80-251-1777-4.
- 2) DOGUET, Joshua J. *The Nature of the Form: Legal and Regulatory Issues Surrounding the Bitcoin Digital Currency System*. In: *Luisiana Law Review* nr. 73. 2013
- 3) The history of Bitcoin from its very beginning in 2008. In: *Bitcoinsberlin* [online]. [cit. 2014-02-20]. Dostupné z: <https://bitcoinsberlin.com/the-history-of-bitcoin-from-its-very-beginning-2008-2/>
- 4) NAKAMOTO, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2008. Dostupné z: <https://bitcoin.org/bitcoin.pdf>
- 5) BOŘÁNEK, Roman. Bitcoin a ti druzí: Přehled zajímavých kryptoměn. *Root.cz* [online]. 2013 [cit. 2014-04-04]. Dostupné z: <http://www.root.cz/clanky/bitcoin-a-ti-druzi-prehled-zajimavych-kryptomen/#ic=articles-related&icc=item-3G>
- 6) HELTON, Matthew. Secondary Liability for Copyright Infringement: BitTorrent as a Vehicle for Establishing a new Copyright Definition for Staple Articles of Commerce. *Columbia Journal of Law and Social Problems*. 2007, č. 40.
- 7) HURST, Brandon. How many people really own bitcoins - and why does it matter?. *BitScan* [online]. 2014 [cit. 2014-06-04]. Dostupné z: <http://bitscan.com/bitnews/item/how-many-people-really-own-bitcoins-and-why-does-it-matter>
- 8) BOGUSZAK, Jiří, Jiří ČAPEK a Aleš GERLOCH. *Teorie práva*. 2., přeprac. vyd. Praha: ASPI, 2004, s. 208. ISBN 8073570300.



- 9) ELIÁŠ, Karel a kol. *Občanský zákoník: velký akademický komentář: úplný text zákona s komentářem, judikaturou a literaturou podle stavu k 1. 4. 2008*. Praha: Linde, 2008. 1. sv. *Zákony - komentáře*. ISBN 978-80-7201-687-7, s. 466-468.
- 10) VRBÍKOVÁ, Lenia a Jan VYSKOČIL. *Právní a daňové aspekty Bitcoinu*. In: *Zkušenosti s virtuálními měnami: Bitcoin měna budoucnosti?*. Praha, 2014, s. 137. Dostupné z: <http://ekon.konference.vsmie.cz/zkusenosti-s-virtualnimi-menami/data/program.pdf>
- 11) BAKEŠ, Milan. *Finanční právo*. 6. upr. vyd. V Praze: C.H. Beck, 2012, s. 335-342. ISBN 978-80-7400-440-7.
- 12) DORNBUSCH, Rudiger. *Makroekonomie*. 1.vyd. Praha: SPN, 1994, s. 341. ISBN 80-04-25556-6.
- 13) HOLMAN, Robert. *Ekonomie*. 5. vyd. V Praze: C.H. Beck, c2011, s. 448. Beckovy ekonomické učebnice. ISBN 978-80-7400-006-5.
- 14) FRANK, Robert H. *Ekonomie*. 1. vyd. Praha: Grada, 2003, s. 581. Profesionál. ISBN 80-247-0471-4.
- 15) HAYEK, Friedrich August von. *Soukromé peníze: Potřebujeme centrální banku?*. Praha: MegaPrint, 1999, s. 41. ISBN 8090270115.
- 16) GRINBERG, Reuben. *Bitcoin: An Innovative Alternative Digital Currency*. *Hastings Science and Technology Law Journal*. 2014, 4:1.
- 17) REVENDA, Zbyněk. *Peněžní ekonomie a bankovníctví*. 2. vyd. Praha: Management Press, 1997, s. 22. ISBN 80-85943-49-2.
- 18) *Physical Bitcoins by Casascius*. *Casascius* [online]. [cit. 2014-02-23]. Dostupné z: <https://www.casascius.com/>
- 19) *Mining*. In: *Bitcoin wiki* [online]. 2014 [cit. 2014-02-24]. Dostupné z: <https://en.bitcoin.it/wiki/Mining>

- 20) EUROPEAN CENTRAL BANK. *Virtual Currency Schemes*. 2012. Dostupné z: <http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>
- 21) NÁDBĚLA, Josef. *Velký počítačový slovník*. Vyd. 1. Kralice na Hané: Computer Media, 2004, s. 328. ISBN 80-86686-21-3.
- 22) Bitcoin: The Libertarian Introduction. In: VOORHEES, Erik. *On Life and Liberty* [online]. 2012 [cit. 2014-03-24]. Dostupné z: <http://evoorhees.blogspot.cz/2012/04/bitcoin-libertarian-introduction.html>
- 23) The new gold rush: Bitcoin ATMs are coming. In: *The Verge* [online]. 2014 [cit. 2014-03-29]. Dostupné z: <http://www.theverge.com/2014/3/10/5490534/the-new-gold-rush-bitcoin-atms-are-coming>
- 24) ČESKÁ NÁRODNÍ BANKA. *Obchodování s bitcoiny*. 10.2.2014. 2014. Dostupné z: [http://www.cnb.cz/miranda2/export/sites/www.cnb.cz/cs/faq/obchodovani\\_s\\_bitcoiny.pdf](http://www.cnb.cz/miranda2/export/sites/www.cnb.cz/cs/faq/obchodovani_s_bitcoiny.pdf)
- 25) WALLACE, Benjamin. The Rise and Fall of Bitcoin. *Wired Magazine* [online]. 2011 [cit. 2014-04-02]. Dostupné z: <http://fromm.robertkeahey.com/wp-content/uploads/2013/07/Session-7-The-Rise-and-Fall-of-Bitcoin.pdf>
- 26) EBay considering accepting bitcoin as payment. In: *CNBC International* [online]. 2014 [cit. 2014-02-21]. Dostupné z: <http://www.cnb.com/id/101356642>
- 27) DECKER, Christian a Roger WATTENHOFER. *Bitcoin Transaction Malleability and MtGox*. Zurich, 2014. Dostupné z: <http://arxiv.org/pdf/1403.6676v1.pdf>. ETH Zurich.
- 28) JELÍNEK, Ladislav. *Komoditní burzy v české republice*. Kroměříž: Justiční akademie, 2006.

- 29) KOTÁSEK, Josef. Cenný papír v § 514 NObčZ. In: *Obchodněprávní revue: odborný recenzovaný časopis pro obchodní právo a právo finančních trhů*. Praha: C.H. Beck, 2013, s. 256. ISSN 1803-6554.
- 30) Rekonstrukce případu Bitcash.cz: Jak se kradou bitcoiny. In: BOŘÁNEK, Roman. *Root.cz* [online]. 2013 [cit. 2014-06-03]. Dostupné z: <http://www.root.cz/clanky/rekonstrukce-pripadu-bitcash-cz-jak-se-kradou-bitcoiny/>
- 31) KAPLANOV, Nikolei M. Nerdy Money: Bitcoin, The Private Digital Currency, And The Case Against Its Regulation. In: *Loyola Consumer Law Review*. Chicago US, 2013, 167 an.
- 32) FINANCIAL ACTION TASK FORCE ON MONEY LAUNDERING. *Guidance for a risk based approach: Prepaid cards, mobile payments and internet-based payment services*. 2013. Dostupné z: <http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf>
- 33) EUROPEAN BANKING AUTHORITY. *Warning to consumers on virtual currencies*. 2013. Dostupné z: <https://www.eba.europa.eu/documents/10180/598344/EBA+Warning+on+Virtual+Currencies.pdf>
- 34) *METODICKÝ POKYN č. 2 Finančního analytického útvaru Ministerstva financí ze dne 16. září 2013 určený povinným osobám O PŘÍSTUPU POVINNÝCH OSOB K DIGITÁLNÍM MĚNÁM*. 2013. Dostupné z: [http://www.mfcr.cz/assets/cs/media/Pokyn-MF\\_c-002\\_2013-09\\_Metodicky-pokyn-o-pristupu-povinnych-osob-k-digitalnim-menam.pdf](http://www.mfcr.cz/assets/cs/media/Pokyn-MF_c-002_2013-09_Metodicky-pokyn-o-pristupu-povinnych-osob-k-digitalnim-menam.pdf)
- 35) TVRDÝ, Jiří. Virtuální měny z pohledu AML/CFT opatření: současnost a očekávaný vývoj. In: *Zkušenosti s virtuálními měnami - Bitcoin měna budoucnosti?: Sborník z konference*. Praha, 2014, s. 109-114. Dostupné z: [http://ekon.konference.vsmie.cz/zkusenosti-s-virtualnimi-menami/data/sbornik\\_bitcoin\\_2014\\_web.pdf](http://ekon.konference.vsmie.cz/zkusenosti-s-virtualnimi-menami/data/sbornik_bitcoin_2014_web.pdf)

- 36) CHRISTIN. *Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace*. 2012. Dostupné z: <http://www.andrew.cmu.edu/user/nicolasc/publications/TR-CMU-CyLab-12-018.pdf>
- 37) Viz například HUME, Tim. How FBI caught Ross Ulbricht, alleged creator of criminal marketplace Silk Road. *CNN International* [online]. [cit. 2014-06-14]. Dostupné z: <http://edition.cnn.com/2013/10/04/world/americas/silk-road-ross-ulbricht/>
- 38) Viz například TWOMEY, Peter. Halting a shift in paradigm: The need for bitcoin regulation. *HeinOnline*. 2013, č. 16.
- 39) Bitcoin regulation news. *CoinDesk: The Voice of digital currency* [online]. [cit. 2014-06-16]. Dostupné z: <http://www.coindesk.com/regulation/>
- 40) How the Bitcoin Protocol Could Help Improve Copyright. In: *Slate Magazine* [online]. 2014 [cit. 2014-02-24]. Dostupné z: [http://www.slate.com/blogs/future\\_tense/2014/02/17/bitcoin\\_protocol\\_could\\_help\\_improve\\_copyright.html](http://www.slate.com/blogs/future_tense/2014/02/17/bitcoin_protocol_could_help_improve_copyright.html)
- 41) Way Beyond Bitcoin: The Coming of "Smart Contracts. In: *Economic Policy Journal* [online]. 2014 [cit. 2014-07-01]. Dostupné z: <http://www.economicpolicyjournal.com/2014/01/way-beyond-bitcoin-coming-of-smart.html>

## **Webové odkazy**

- <http://bitcoin.org> - „neoficiální“ stránky bitcoinového systému
- <https://en.bitcoin.it/wiki/> - neoficiální wikipedie o bitcoinu

- <http://github.com/bitcoin/bitcoin> – Úložiště zdrojového kódu bitcoinového platebního systému. Soubor README.md obsahuje důležité informace, týkající například vývojového procesu, sestavení aplikace a použité licence.
- <http://opensource.org/licenses/MIT> – plné znění MIT licence, pod kterou je uvolněn referenční bitcoinový klient bitcoind
- <http://historyofbitcoin.org/> - časová osa s nejvýznamnějšími okamžiky týkající se bitcoinového platebního systému
- <http://www.bitstock.cz> – Webové stránky české elektronické burzy s bitcoiny
- <http://coinmarketcap.com/all.html> – přehled alternativních kryptoměn
- <http://www.bitcoinstore.com/faq> – Jeden z největších obchodů přijímajících platby v bitcoinu - často kladené dotazy
- <http://usebitcoins.info/> - webové stránky s informacemi o místech, kde lze platit bitcoinem
- <http://spendbitcoins.cz/> - obdobné jako stránky výše
- <http://coinmap.org/> - mapa míst, na kterých je možné platit bitcoinem

## Seznam použitých zkratk a některých pojmů:

- **Altcoin:** alternative-coin, platební systémy odvozené od bitcoinu
- **AML zákon:** zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu
- **AML:** Anti money laundering – angl. proti praní špinavých peněz
- **Asymetrická kryptografie:** též kryptografie veřejného klíče. Podstatou je existence dvou provázaných šifrovacích klíčů – soukromého a veřejného. Pomocí soukromého je možné data rozšifrovat či podepsat,

pomocí veřejného zašifrovat či ověřit podpis. Umožňuje šifrování bez existence postranního kanálu

- **Blockchain:** distribuovaný záznam transakcí v bitcoinovém platebním systému
- **BTC:** zkratka pro bitcoin, používá se zejména při vyjádření množství, obdobně jako třeba CZK či USD pro koruny a dolary
- **EBA:** Evropský orgán pro bankovníctví
- **FATF:** Finanční akční skupina pro boj proti praní špinavých peněz skupiny G7
- **FAÚ:** Finanční analytický útvar Ministerstva financí
- **FBI:** Federální úřad pro vyšetřování, Spojené státy americké
- **FOSS:** Free and Open-Source Software, označuje software s otevřeným zdrojovým kódem, uvolněný pod některou z tzv. copyleftových licencí. Umožňuje volné šíření a modifikaci takového software.
- **Kryptoměna:** pojem zahrnující bitcoin a obdobné platební systémy, naráží na skutečnost, že funkcionality těchto systémů je zabezpečena kryptografií
- **OTC:** Over-the-counter – neoficiální, mimoburzovní způsob obchodování s finančními instrumenty
- **P2P síť:** z anglického peer-to-peer (rovný s rovným), označuje síť, kde nelze rozlišit centrální server, všechny uzly jsou si rovny.

## Abstrakt

Cílem této práce je analyzovat bitcoinový platební systém z pohledu právních i praktických otázek, které se vyskytují v souvislosti s jeho používáním.

Bitcoinový platební systém je moderní elektronický platební systém, který k provádění transakcí používá decentralizované tzv. peer-to-peer síť a kryptografii veřejného klíče. Jeho hlavním odlišujícím rysem je absence třetí strany, možnost provádění transakcí přímo, bez využití služeb některé z platebních institucí. Dalšími charakteristickými rysy jsou vysoká rychlost provádění transakcí bez ohledu na geografickou vzdálenost mezi jejími stranami a relativně nízké transakční poplatky.

Spolu s postupným rozšiřováním použití této technologie v platebním styku se čím dál tím více projevuje nutnost vyjasnit jeho postavení v právním řádu. Jeho odlišnosti od ostatních, běžně používaných platebních systémů, společně s faktem, že v době, kdy byla přijímána současná právní úprava, nebyla existence podobných systémů žádným způsobem reflektována podstatně ztěžují jeho zařazení do rámce vymezeného platnými právními předpisy.

Práce se nejprve zabývá popisem předmětu výzkumu: Charakterizuje bitcoinový platební systém, mechanismy jeho fungování a principy na kterých je postaven. Tato část je založena na názoru, že pochopení principů, na kterých je technologie založena, je velmi důležité pro následné smysluplné určení práv a povinností, které subjektům práva vznikají v souvislosti s jeho používáním.

Následující část samostatně posuzuje soulad účasti subjektů na této platební síti s právním řádem a analyzuje právní normy relevantní pro posouzení této otázky.

Třetí část práce vymezuje některé kategorie stanovené platnými předpisy i právní naukou a zkoumá, zda je možné pod ně bitcoin subsumovat a jaké jsou důsledky takového zařazení. Zkoumanými kategoriemi jsou zejména věc v právním slova smyslu, peníze, měna a elektronické peníze.

Čtvrtá část práce zkoumá systém právních a obecně společenských vztahů s relací k bitcoinovému platebnímu systému. Rozlišuje hlavní skupiny uživatelů, vývojářů

obchodníků, burz a dalších institucí a analyzuje jejich činnost ve vztahu k právnímu řádu.

Následující část se zabývá některými protiprávními a společensky nebezpečnými činnostmi, které se v souvislosti s bitcoinovým platebním systémem vyskytují. Rozebírá jeho vztah k legalizaci výnosů z trestné činnosti, financování terorismu a obchodování s omamnými a psychotropními látkami. Také se v této souvislosti věnuje otázce omezení plateb v hotovosti.

Předposlední část obecně zkoumá nutnost a vhodnost přijetí právní úpravy, která by již reflektovala existenci bitcoinu a jemu podobných systémů. Také analyzuje činnost některých institucí a orgánů veřejné moci, směřující ke zjištění, jakým způsobem by měly být tyto systémy upraveny a vytváření návrhů takové úpravy.

Poslední část stručně informuje o skutečnosti, že některé z technologií použitých při implementaci bitcoinového protokolu mají i perspektivy jiných způsobů využití a že se tak dá očekávat vznik dalších aplikací, v některých rysech podobných bitcoinovému platebnímu systému.



## **Abstract in english**

The purpose of this theses is to analyse the Bitcoin electronic peer-to-peer payment system, from the view of the legal, regulatory and also purely practical issues surrounding its use as a modern means of payment processing.

The reason for choosing this topic is that I find the subject to be very interesting and possibly promising for the future of payments. Also, as the use of Bitcoin payment system spreads across the global population, we can see many of legal questions arising: Is the use of Bitcoin network legal? How is it regulated under existing legal system? Can it be subsumed under any existing legal categories? What are the risks of its misuse for criminal activities? Should new legal rules be enacted to regulate its use, and if so, what should these rules be like?

My goal in this paper is to find these relevant questions, elaborate on them and provide as many answers as will be possible. We have to bear in mind the fact, that the technology, underlying the Bitcoin payment system is very new and many ways path-breaking. As usual, the legal theory lags behind technology here, so many questions still have to be settled before we can give any straight answers.

The work is divided into seven chapters, each dealing with different legal or practical aspects connected to the Bitcoin payment system.

First chapter examines the subject of research. It tells us what Bitcoin is and what are its main characteristics. It also reveals the dual essence of the term bitcoin – as a form of money and as a payment system, made to process transaction with this money. Then, we take a closer look to the inner mechanics of the system, as I believe, that understanding of underlying technology is crucial for the correct legal analysis. We also mention other payment systems derived from Bitcoin.

Second chapter concerns itself with the question of legality or illegality of participating in the Bitcoin network. It concludes, that so far, the simple fact of participating on this network is allowed by the Czech legal system as there are no laws

prohibiting its use. But we have to keep in mind, that other activities connected to the use of Bitcoin payment system have to be looked on separately.

Third chapter shows some categories, legal or economical, that Bitcoin could possibly be subsumed under. We elaborate on them and try to tell if the subsumption is really possible. In this way we explore that Bitcoin is very unusual and the subsumptions under existing categories are problematic. Nevertheless we conclude that Bitcoin is an incorporeal thing in legal sense and that it is a form of money. Other categories such as currency and strikingly even electronic money are not suitable.

Fourth chapter examines what we call a Bitcoin ecosystem – a system of social and legal relations connected to the use of Bitcoin. It recognizes several groups and institutions within this system: Users, developers, exchanges and stock-exchanges, merchants and service providers. It also deals with the question of how are these activities regulated under current legal system.

Fifth chapter concentrates on matters of illegal and nefarious activities that the Bitcoin payment system can be used for. It is, in particular, money laundering and financing of terrorism and trade with illegal substances. It tells us why and how can Bitcoin be used for this kind of activities and how are the authorities recognizing and treating this risk.

Sixth chapter focuses on the issue of Bitcoin regulation *de lege ferenda*. It gives arguments for and against its explicit regulation. It also explores the current attempts to embed Bitcoin into existing legal constructs. It concludes, that Bitcoin, same as other new technologies, has to be treated wisely by policymakers, otherwise the regulation could seriously damage the bitcoin economy and potential of the technology itself.

Seventh chapter gives us a hint on what kind of technologies can possibly evolve from Bitcoin and what other implementations of the underlying technology can there be: For example using the decentralised public ledger known as the blockchain as a means to provide proof of existence of documents in certain time. Also the idea of self-enforcing (so called smart) contracts is very promising, I believe.

My conclusions are, that the Bitcoin payment system is very original piece of technology and it is also very interesting from legal perspective. It changes our view on electronic payments in many ways. Its legal status is yet very uncertain and lot of work still has to be done in this field to embed Bitcoin into existing legal framework. We have managed to outline some categories and tell if Bitcoin falls into them or not and why is that so. Bitcoin is surrounded by rich system of economic, legal and social relations. There are also some risks connected to it and existing control mechanisms are not really prepared to deal with them – especially because of the lack of legal regulation. Bitcoin shows us, that the evolution of money is not nearly at its end, and lawyers need to take that into consideration.

**Název práce v českém jazyce:** Bitcoin – právní rámec a praktické aspekty jeho používání v platebním styku

**Klíčová slova:** Bitcoin, virtuální měny, platební systémy

**Name of the thesis in english:** Bitcoin – the legal framework and practical aspects of its use in payments

**Keywords:** Bitcoin, virtual currencies, payment systems