

Bitcoin jako platební a investiční nástroj

Bakalářská práce

Vedoucí práce:

Ing. Petr Toman, Ph.D.

Tran Thi Thu Ha

Brno 2016

Děkuji vedoucímu mé bakalářské práce Ing. Petru Tomanovi, Ph.D. za ochotu, cenné rady, konzultace a užitečné připomínky, které mi pomohly při tvorbě této práce.

Čestné prohlášení

Prohlašuji, že jsem tuto práci: **Bitcoin jako platební a investiční nástroj** vypracovala samostatně a veškeré použité prameny a informace jsou uvedeny v seznamu použité literatury. Souhlasím, aby moje práce byla zveřejněna v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů, a v souladu s platnou *Směrnicí o zveřejňování vysokoškolských závěrečných prací*.

Jsem si vědoma, že se na moji práci vztahuje zákon č. 121/2000 Sb., autorský zákon, a že Mendelova univerzita v Brně má právo na uzavření licenční smlouvy a užití této práce jako školního díla podle § 60 odst. 1 Autorského zákona.

Dále se zavazuji, že před sepsáním licenční smlouvy o využití díla jinou osobou (subjektem) si vyžádám písemné stanovisko univerzity o tom, že předmetná licenční smlouva není v rozporu s oprávněnými zájmy univerzity, a zavazuji se uhradit případný příspěvek na úhradu nákladů spojených se vznikem díla, a to až do jejich skutečné výše.

V Brně dne 23. května 2016

Abstract

Tran, T. T. H. Bitcoin as instrument for payment and investment. Bachelor thesis. Brno: Mendel University, 2016.

The submitted Bachelor thesis aims to formulate a recommendation for potential user and investor in Czech Republic. The first part is focused on basics of cryptography, principles of Bitcoin, its regulation and Bitcoin's price development from its beginning. The second part is about Bitcoin's use as instrument for foreign payment and its use as instrument for investment.

Keywords

Bitcoin, regulation, development, wallet, foreign payment, investment, return, risk.

Abstrakt

Tran, T. T. H. Bitcoin jako platební a investiční nástroj. Bakalářská práce. Brno: Mendelova univerzita v Brně, 2016.

Předmětem bakalářské práce je formulovat doporučení pro potenciálního uživatele a investora do bitcoinu v České republice. První část je zaměřena na základy kryptografie, principy Bitcoinu, jeho regulaci a vývoj ceny od jeho vzniku. Druhá část je zaměřena na využití Bitcoinu jako nástroj zahraničního platebního styku a dále jeho využití jako investičního nástroje.

Klíčová slova

Bitcoin, regulace, vývoj, peněženka, zahraniční platba, investice, výnos, riziko.

Obsah

1	Úvod	15
2	Cíl práce	16
3	Metodika	17
4	Terminologický slovník	19
5	Literární rešerše	20
5.1	Kryptografie	20
5.2	Co je Bitcoin.....	22
5.3	Jak funguje Bitcoin	22
5.3.1	Transakce.....	23
5.3.2	Blok.....	24
5.3.3	Proof of work.....	25
5.3.4	Mining.....	26
5.3.5	Blockchain	26
5.4	Vlastnosti Bitcoinu	27
5.4.1	Výhody Bitcoinu.....	27
5.4.2	Nevýhody Bitcoinu	28
5.5	Právní regulace Bitcoinu	28
5.5.1	Česká republika.....	29
5.5.2	Německo	30
5.5.3	Rusko.....	30
5.5.4	Evropská unie	31
5.5.5	USA.....	33
5.5.6	Čína	33
5.5.7	Země s restrikcí Bitcoinu.....	34
5.5.8	Závěr kapitoly	35
5.6	Vývoj Bitcoinu	36
5.6.1	Události roku 2009.....	36

5.6.2	Události roku 2010.....	36
5.6.3	Události roku 2011.....	36
5.6.4	Události roku 2012.....	37
5.6.5	Události roku 2013.....	37
5.6.6	Události roku 2014.....	38
5.6.7	Události roku 2015.....	38
6	Bitcoin jako platební nástroj	39
6.1	Jak uchovávat bitcoiny	39
6.2	Softwarová peněženka.....	39
6.2.1	Základní softwarová peněženka	40
6.2.2	Odlehčená softwarová peněženka	40
6.2.3	Online peněženka	41
6.2.4	Mobilní peněženka	41
6.2.5	Papírová peněženka	42
6.2.6	Hardwarová peněženka.....	42
6.2.7	Závěr kapitoly	43
6.3	Jak získat bitcoiny	44
6.3.1	Mining.....	44
6.3.2	Bitcoin směnárný.....	45
6.3.3	Bitcoin burzy	46
6.3.4	Bitcoinmaty.....	48
6.3.5	Localbitcoins	48
6.3.6	Vlastní služby	49
6.3.7	Závěr kapitoly	49
6.4	Možnosti využití bitcoinů	50
6.4.1	Nákup za bitcoiny na e-shopech.....	50
6.4.2	Závěr kapitoly	51
6.5	Převod finančních prostředků	51
6.5.1	Banky	52
6.5.2	Western Union (WU).....	57
6.5.3	Bitcoin	58

6.5.4	Závěr kapitoly	63
7	Bitcoin jako investiční nástroj	64
7.1	Zlato a bitcoin	64
7.2	Investování do zlata.....	65
7.3	Investování do bitcoinu	68
7.4	Porovnání investice do bitcoinu a zlata	71
7.5	Závěr kapitoly.....	73
8	Předpověď budoucího vývoje Bitcoinu	74
9	Diskuse	76
10	Závěr	82
11	Literatura	86

Seznam obrázků

Obr. 1	Příklad SHA-256 funkce s fixní délkou výstupu	21
Obr. 2	Asymetrická kryptografie	21
Obr. 3	Digitální podepisování	22
Obr. 4	Princip transakce	23
Obr. 5	Merkle tree (hlavička bloku)	24
Obr. 6	Řetězec bloků (blockchain)	25
Obr. 7	Příklad nalezení hash hodnoty pro „Hello, world!“ začínající „000“	26
Obr. 8	Větvení blockchainu	27
Obr. 9	Právní regulace bitcoinu na mapě	29
Obr. 10	Vývoj kurzu USD/BTC	36
Obr. 11	Generátor Bitaddress	39
Obr. 12	Velikost blockchainu	40
Obr. 13	Papírová peněženka	42
Obr. 14	Bitcoin Trezor	43
Obr. 15	Nákup bitcoinů	46
Obr. 16	Burza BitStock	47
Obr. 17	Poplatky Western Union	58
Obr. 18	Transakce a poplatek sítě	58
Obr. 19	Vývoj ceny zlata a bitcoinu v USD za posledních 5 let	64
Obr. 20	Vývoj ceny zlata v USD za unci za posledních 10 let	65
Obr. 21	Cena za unci zlata v USD v letech 2010-2015	66
Obr. 22	Grafické znázornění vývoje zlata v %	67

Obr. 23	Grafické znázornění roční rizikovosti zlata v %	68
Obr. 24	Grafické znázornění roční výnosnosti bitcoinu v %	69
Obr. 25	Grafické znázornění roční rizikovosti bitcoinu v %	70
Obr. 26	Volatilita bitcoinu, zlata a eura v USD	72
Obr. 27	Korelace ceny zlata s bitcoinem	73
Obr. 28	Předpověď budoucího vývoje kurzu BTC/USD	74
Obr. 29	Počet transakcí za den	75

Seznam tabulek

Tab. 1	Vybrané státy EU a jejich postoj k virtuálním měnám	32
Tab. 2	Kurzy BTC směnáren v ČR k 18. 12. 2015 23:35	45
Tab. 3	Srovnání cen e-shopů	51
Tab. 4	Poplatky vybraných českých bank za odchozí SEPA platbu	54
Tab. 5	Poplatky vybraných českých bank za odchozí SWIFT platbu	56
Tab. 6	Poplatky za příchozí zahraniční platbu ve vietnamských bankách	57
Tab. 7	BTC burzy ve Vietnamu	59
Tab. 8	Průměrná výše poplatků	59
Tab. 9	Devizový kurz CZK/USD vybraných bank	60
Tab. 10	Srovnání subjektů při převodu 10 000 Kč	61
Tab. 11	Komparace výstupů	62
Tab. 12	Roční výnosnost zlata v %	66
Tab. 13	Roční rizikovost zlata v %	67
Tab. 14	Srovnání ukazatelů u zlata	68
Tab. 15	Roční výnosnost bitcoinu v %	69
Tab. 16	Roční rizikovost bitcoinu v %	69
Tab. 17	Srovnání ukazatelů u bitcoinu	70
Tab. 18	Porovnání výnosnosti investice při nákupu BTC v daných letech	71
Tab. 19	Srovnání investice do bitcoinu a zlata	71
Tab. 20	Srovnání cen e-shopů	76
Tab. 21	Komparace výstupů	78
Tab. 22	Průměrná výše poplatků	79
Tab. 23	Srovnání investice do bitcoinu a zlata	80

1 Úvod

V současnosti dochází k prudkému rozvoji nových technologií, které ovlivňují všechny oblasti našeho života. Tento technologický rozvoj nepochybně zasahuje i svět financí, kde se projevuje v podobě vzniku nových investičních příležitostí, vytvořených díky existenci a rozvoji nových technologií. Vznikají nové platební systémy, nové investiční instrumenty, zdokonalují se technologie pro bezhotovostní platební styk, vzniká množství technologicky orientovaných start-upů a dalších specifických projektů.

Jedním z potenciálně významných výsledků tohoto procesu je i vznik tzv. kryptoměn. Nejznámější z nich je právě Bitcoin. Momentálně se dá za bitcoiny koupit široké spektrum různých produktů a služeb a počet firem, které přijímají bitcoin jako platební možnost, den ode dne roste. Mezi nejznámější firmy, které akceptují bitcoin, patří např. Dell, Amazon, PayPal, Microsoft, Ebay, Wikipedia, Bloomberg a Subway. Původně sice měla tato kryptoměna sloužit jako nový druh peněz, vytvořila se z ní ale spíš spekulativní investice, která láká spoustu investorů. Mnoho lidí dokázalo od počátku jeho vzniku na bitcoinu vydělat, ale taky prodělat.

Vyplatilo se tedy investování do bitcoinů a vyplatí se tato investice nadále? Jak fungují bitcoiny a kde se dají získat? Jak se dá bitcoiny platit? Dá se Bitcoin využít jako nástroj zahraničního platebního styku při současné konkurenci v podobě komerčních bank a velkého Western Union?

2 Cíl práce

Hlavním cílem bakalářské práce je na základě analýzy Bitcoinu jako platebního systému a zhodnocení rizikovosti a výnosnosti investice formulovat doporučení pro potenciálního uživatele a investora do bitcoinu. K dosažení hlavního cíle využiji několika dílčích cílů.

Dílčí cíle práce je možno formulovat do následujících bodů:

- Identifikovat principy a vlastnosti Bitcoinu.
- Zhodnotit stav právní regulace Bitcoinu v jednotlivých zemích.
- Analyzovat vývoj Bitcoinu od jeho počátku po současnost.
- Komparace možností získání a uchování bitcoinů
- Analyzovat Bitcoin jako platební systém, na který se vztahují následující výzkumné otázky:

Výzkumná otázka č. 1: Vyplatí se na českých e-shopech platba za bitcoiny?

Výzkumná otázka č. 2: Jak vychází Bitcoin jako nástroj zahraničního platebního styku?

- Zhodnotit rizikovost a výnosnost investice do bitcoinu a formulovat doporučení pro potenciálního investora. Na tento cíl se vztahuje poslední výzkumná otázka:

Výzkumná otázka č. 3: Byla v letech 2010-2015 lepší investice do bitcoinu než investice do zlata?

- Nastínit možný budoucí vývoj Bitcoinu.

3 Metodika

Tato práce je členěna na literární rešerši, která tvoří kapitolu 5 a dále aplikační část, která tvoří kapitoly 6 a 7.

Literární rešerše vychází z dostupných, převážně zahraničních, odborných publikací, článků, dokumentů a internetových zdrojů. Výchozím dokumentem podkapitoly 5.3 *Jak funguje Bitcoin* je dokument *Bitcoin: A Peer-to-Peer Electronic Cash System* od tvůrce Bitcoinu vystupující pod pseudonymem Satoshi Nakamoto. V dalších podkapitolách literární rešerše bude zhodnocena právní regulace Bitcoinu v jednotlivých zemích a analyzován vývoj kurzu BTC/USD na základě klíčových událostí ovlivňujících Bitcoin od jeho počátku.

V rámci aplikační části budou zodpovězeny výzkumné otázky, přičemž u prvních dvou výzkumných otázek bude provedena metoda komparace dle dostupných dat a pro zodpovězení třetí výzkumné otázky použiji následující vzorce.

Pro porovnání investic použiji jeden z neznámějších a nejpoužívanějších koeficientů k hodnocení investic, a to Sharpe ratio, který se určí jako podíl výnosu aktiva sníženého o bezrizikovou úrokovou míru a směrodatné odchylny výnosů.

$$S = \frac{E(R - R_f)}{\sigma},$$

kde R je výnosnost sledované investice nebo aktiva, R_f je výnos investice, zpravidla bezriziková úroková míra, $E(R - R_f)$ je očekávaný výnos investice a σ je směrodatná odchylka výnosu.

Pro vyjádření výnosnosti v podobě výnosové míry použiji vzorec výnosové míry ex post:

$$r = \frac{(P_1 - P_0) + I - T - C_0}{P_0},$$

kde P_1 je prodejní cena, P_0 je nákupní cena, I je příjem plynoucí z investičního instrumentu, T jsou daňové náklady a C_0 transakční náklady.

Míru rizika spočítám jako rozptyl, resp. směrodatnou odchylku, podle následujícího vzorce:

$$\sigma_{xp} = \sqrt{\sigma_{xp}^2} = \sqrt{\frac{\sum_{t=1}^T (\bar{r} - r_t)^2}{T}},$$

kde σ_{xp}^2 je rozptyl charakterizující míru rizika ex post, \bar{r} je průměrná výnosová míra ex post, r_t jsou jednotlivé výnosové míry ex post odpovídající sledovaným obdobím a T je počet sledovaných období.

4 Terminologický slovník

<i>Termín</i>	<i>Význam</i>
Bitcoin	Bitcoin s velkým B je název protokolu, platebního systému, který vytvořil Satoshi Nakamoto v roce 2008.
bitcoin	Bitcoin s malým b je jednotka měny, jako je např. dolar (USD), tak je bitcoin (BTC/XBT).
blockchain	Blockchain je soubor všech bloků vytvořených od počátku Bitcoinu. Je to veřejný záznam všech uskutečněných transakcí v chronologickém pořádku.
blok	Blok je soubor dat, ve kterém jsou těžaři potvrzovány transakce. Každý blok odkazuje na předchozí blok a dohromady tvoří blockchain.
BTC adresa	Bitcoin adresa je unikátní identifikátor, který vám umožní přijímat bitcoiny. Konkrétně je to řetězec 34 znaků, například "1C2McBicWzrNDmDp3VtSaTjkyvbzpvRotE".
BTC klient	Bitcoin klient je aplikace používaná pro správu adres a soukromých klíčů včetně operací s nimi, jako je vytváření a podepisování transakcí či vytváření nových adres.
BTC peněženka	Peněženka je sada adres a soukromých klíčů vytvořená Bitcoin klientem.
double spend	Double spend je proces, při kterém se utratí stejné peníze vícerokrát než jednou.
kryptoměna	Kryptoměna je měna založená na kryptografii.
mining	Mining neboli těžba je proces, při kterém vznikají nové bitcoiny jako odměna těžařům za poskytnutý výpočetní výkon.
mining pool	Mining pool je sdružení těžařů za účelem snížení variance při miningu výměnou za poplatky provozovateli.
open source	Open source znamená, že má daný software veřejný zdrojový kód, a každý uživatel se může zapojit.
P2P síť	Síť počítačů, kde neexistuje jedna centrála, ale počítače mezi sebou komunikují navzájem.

5 Literární rešerše

Bitcoin je decentralizovaný elektronický platební systém postavený na kryptografii, díky které umožňuje provádět transakce bez potřeby třetí strany, jako je například banka. Poprvé byl tento protokol představen 31. října 2008 v práci *Bitcoin: A Peer-to-Peer Electronic Cash System*, kde se autor podepsal pod pseudonymem Satoshi Nakamoto. Existují spekulace, že se může jednat i o skupinu osob. V této práci jsou formulované technické detaily a principy fungování této sítě, které dále vysvětlím v kapitole 5.3 *Jak funguje Bitcoin*. Pro pochopení Bitcoinu je třeba znát alespoň základy kryptografie, součástí literární rešerše je proto i stručný úvod do kryptografie a hash funkcí.

5.1 Kryptografie

Kryptografie neboli šifrování znamená v podstatě zašifrovat data na straně odesílatele, odeslat je a na straně příjemce zase dešifrovat. (Budiš, 2008, s. 28) Autor dále uvádí: „Kvalita ochrany zprávy je dána šifrovací metodou zahrnující typ užitého šifrovacího algoritmu, navržený bezpečný způsob jeho aplikace (kryptografický protokol) a způsob jeho použití s dodržáním kryptografického protokolu a délkou šifrovacího klíče.“

Hash je matematická funkce, která transformuje vstupní data variabilní délky a převádí je na výstupní hash hodnotu o fixním počtu znaků. Hash je obvykle kratší než původní vstupní řetězec, a i minimální změna ve vstupních datech má za následek absolutně odlišnou hash hodnotu. Hash funkce pracují v jednom směru. Je snadné u ní vypočítat hodnotu hash ze vstupních dat, ale je velice výpočetně náročný postup opačný, tedy vypočtení vstupních dat z hash hodnoty. (Schneier, 1996)

Pro lepší představu jak fungují jednosměrné funkce, dodává Klíma (2005): „Je to, jako když smícháme dvě složky lepidla. Za několik vteřin vytvoří novou sloučeninu se zcela novými vazbami atomů a molekul, které nelze jednoduše rozpojit a vrátit do původní podoby.“ Na obr. 1 je příklad hash funkce SHA-256, kde můžeme vidět variabilní délku vstupního textu a fixní délku výstupu, který je u této hash funkce roven 64 znakům.

V asymetrické kryptografii se užívá dvojice klíčů, tzv. soukromý a veřejný. Princip spočívá v tom, že data šifrovaná jedním z klíčů lze v rozumném čase dešifrovat pouze se znalostí druhého z dvojice klíčů a naopak. (Budiš, 2008) Pokud budu chtít poslat někomu zašifrovanou zprávu, použiji k tomu veřejný klíč. Každý s veřejným klíčem může zprávu zašifrovat, dešifrovat ji může ale pouze osoba se soukromým klíčem, viz obr. 2. (Schneier, 1996)

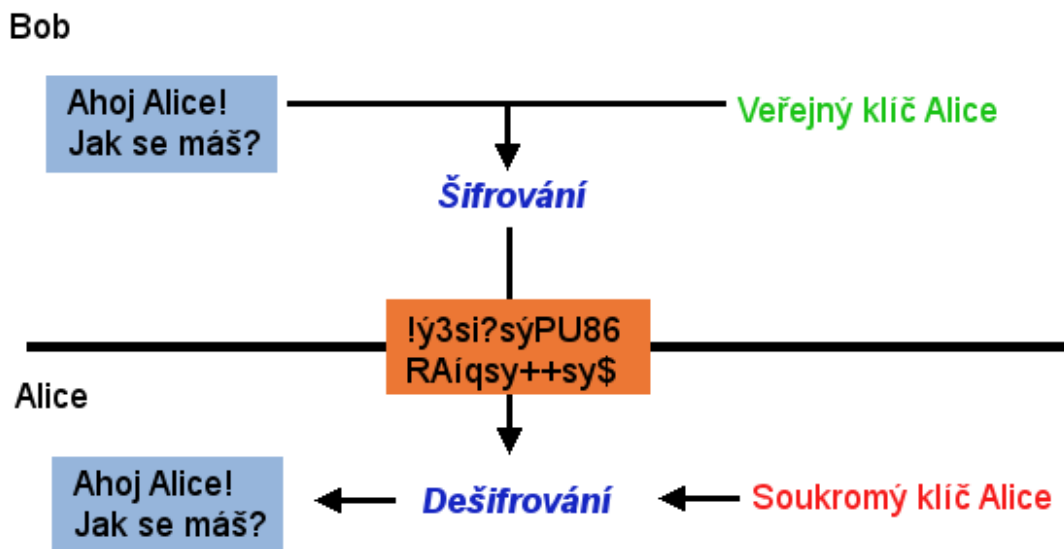
```

Vstup 11 znaků:
  Lorem ipsum
Výstup 64 znaků:
  a9a66978f378456c818fb8a3e7c6ad3d2c83e62724ccbdea7b36253fb8df5edd

Vstup 280 znaků:
  Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec
  scelerisque enim et nisi commodo, id interdum sapien hendrerit.
  Pellentesque ac elit nunc. Ut erat dui, vulputate et auctor ac,
  egestas eget est. Curabitur ut luctus erat. Maecenas imperdiet vel
  est sit amet volutpat.
Výstup 64 znaků:
  4d115e25bef76e79abb7f94fb19a76c8dd53258d69e29d102bf9385d56d05365

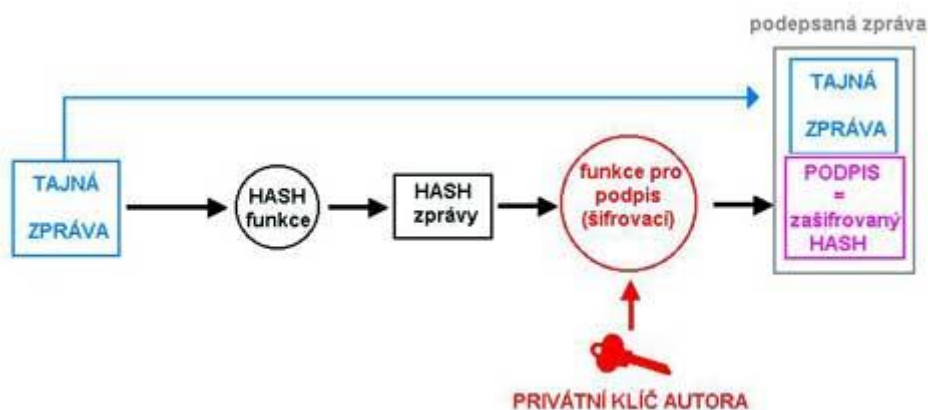
```

Obr. 1 Příklad SHA-256 funkce s fixní délkou výstupu
Zdroj: Huřták, 2013



Obr. 2 Asymetrická kryptografie
Zdroj: Jírotka, 2009-2014

Asymetrická kryptografie se používá také při digitálním podepisování (obr. 3), a to následovně: vytvořím hash zprávy, který zašifruji soukromým klíčem (=podepíšu), tento podpis s původní zprávou pošlu příjemci. Příjemce dešifruje s pomocí mého veřejného klíče podpis, a tím získá hash, který jsem vytvořila. Ten poté porovná s hashem přijaté zprávy. Pokud budou totožné, znamená to, že zprávu nikdo další neupravil.



Obr. 3 Digitální podepisování
Zdroj: Nádeníček, 2003

5.2 Co je Bitcoin

Bitcoin je decentralizovaný systém založený na open-source protokolu v P2P síti¹. Pojem Bitcoin s *velkým B* odkazuje na celý „měnový“ systém, kdežto bitcoin s *malým b* je základní jednotkou této „měny“ (1 bitcoin = 1BTC/XBT). Bitcoin je dále dělitelný až na 8 desetinných míst, nejmenší jednotkou je 0,00 000 001 BTC neboli satoshi.

Stejně jako dolary, eura, koruny nebo zlaté mince, můžeme bitcoiny utratit za zboží a služby, směnit je za jiné měny. Nicméně, Bitcoin je první světová „měna“, která je zároveň digitální i decentralizovaná. Digitální měna je taková měna, která může být uložena a používána na počítači. Podle této definice by i dolary mohly být považovány za digitální měnu, když mohou být jednoduše poslány ostatním nebo používány na online nákupy, ale jejich nabídka je kontrolována centralizovanou bankovní organizací. V porovnání s tím jsou zlaté mince decentralizované, to znamená, že žádná centrální autorita nekontroluje nabídku zlata ve světě. Ve skutečnosti může každý těžit zlato, vytvářet nové mince a distribuovat je. Nicméně, oproti digitálním měnám, není jednoduché používat zlaté mince na platbu za zboží (alespoň ne přesnou částkou) a je nemožné převádět zlaté mince přes internet. Právě proto, že Bitcoin kombinuje tyto dvě vlastnosti, říká se mu „digitální zlato“. (Barski, Wilmer, 2014)

5.3 Jak funguje Bitcoin

V této kapitole pro pochopení nejdříve vysvětlím velmi zjednodušeně principy fungování Bitcoinu, přičemž budou tyto principy dále rozebrány podrobněji.

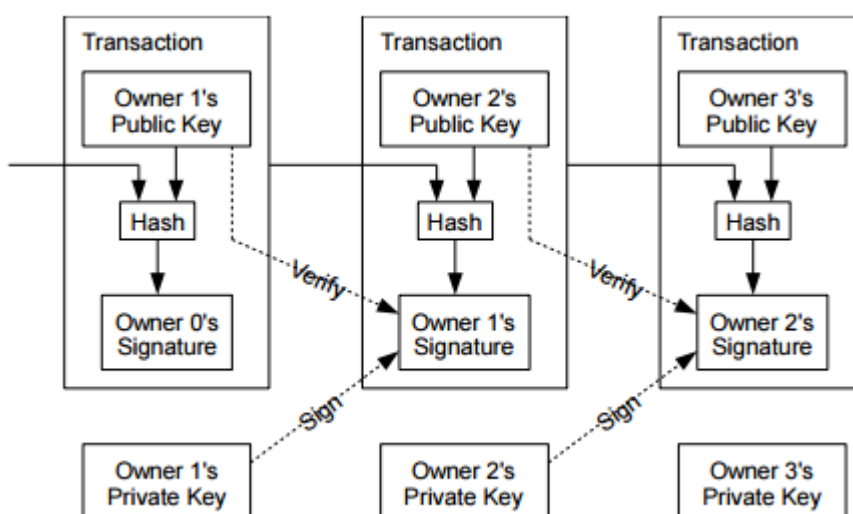
Pro fungování bitcoinové sítě je nezbytné, aby ji někdo udržoval v chodu a především potvrzoval transakce, které v ní probíhají. Tuto činnost mají na starost

¹ P2P neboli peer-to-peer (= rovný s rovným) síť znamená, že uživatelé v této síti komunikují navzájem mezi sebou bez prostředníka

mineři (těžaři). Při vytváření tzv. bitcoin účtu je uživateli vytvořena adresa, na kterou mu mohou ostatní uživatelé posílat bitcoiny (něco jako číslo účtu), těchto adres může mít libovolné množství. Při posílání bitcoinů mezi uživateli se vytvoří transakce, kterou odesílatel podepíše svým soukromým klíčem. Průměrně každých 10 minut jsou transakce shromážděny těžaři do tzv. bloku. Všechny bloky jsou propojené a tvoří dohromady tzv. blockchain. Blockchain je veřejná „účetní kniha“, na kterou spoléhá celá bitcoinová síť. Jsou v něm zapsány veškeré transakce, které proběhly a jednoznačně vymezuje kolik bitcoinů je na jakých adresách. Integrita a chronologické pořadí v blockchainu jsou zabezpečeny kryptografickými algoritmy. (Guttmann, 2014) Transakci, která je součástí blockchainu, můžeme považovat za bezpečnou, protože samotné bloky je velmi obtížné vytvořit, tedy i zfalšovat. Nové bitcoiny vznikají vyřešením kryptografické úlohy, která je spojena s vytvářením bloku a poskytnutím tzv. proof of work.

5.3.1 Transakce

Nakamoto (2008) uvádí, že elektronická mince je v podstatě řetězec digitálních podpisů. Každý vlastník převádí minci na dalšího vlastníka tak, že digitálně podepíše hash předchozí transakce s veřejným klíčem dalšího vlastníka a ten přidá ke konci mince, viz obr. 4. Příjemce dokáže ověřit podpisy a tím i ověřit řetězec vlastnictví bitcoinů.



Obr. 4 Princip transakce
Zdroj: Nakamoto, 2008

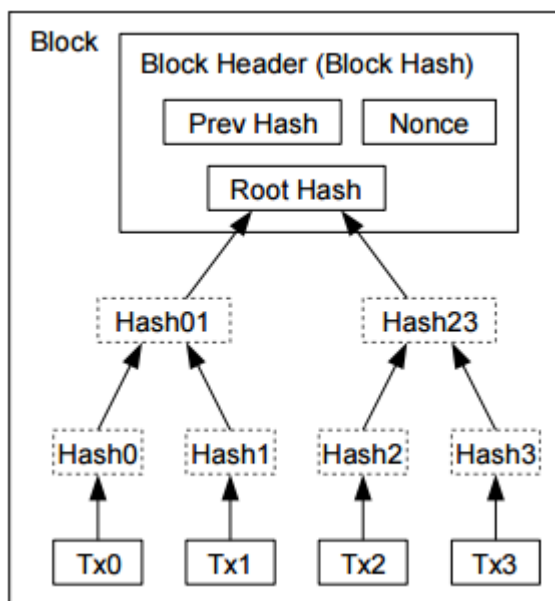
Problémem je, že příjemce nedokáže ověřit, jestli jeden z předchozích vlastníků již tuto minci neutratil dvakrát (double spend). Běžným řešením je představit důvěryhodnou centrální autoritu, nebo mincovnu, která kontroluje každou transakci proti double spending. Po každé transakci by musela být mince vrácena mincovně, aby vydala novou minci, a pouze mince vydané přímo z mincovny by byly důvěry-

hodné. Problém tohoto řešení je, že osud celého peněžního systému závisí na společnosti vlastníci mincovnu.

Potřebujeme, aby příjemce věděl, že předchozí majitelé nepodepsali žádné dřívější transakce. Pro tyto účely se počítají jen první transakce, a proto se nestaráme o pozdější pokusy o double spend. Jediný způsob, jak potvrdit absenci transakce, je vědět o všech transakcích. Příjemce potřebuje důkaz, že při každé transakci, většina uzlů sítě potvrdila, že jde o první přijatou minci. Řešením je systém proof of work spolu s blockchain.

5.3.2 Blok

Blok je datová struktura, která obsahuje hlavičku bloku (block header) a transakce ve formě merkle tree. Hlavička bloku obsahuje tyto informace: verze protokolu, hash předchozí hlavičky bloku, merkle root (hash ověřující integritu transakcí v bloku), timestamp (čas, kdy byl blok vytvořen), bits (hodnota spojená s obtížností pro proof of work) a nonce (hodnota při miningu za účelem nalezení hash kolize). Místo uložení samotných transakcí v hlavičce bloku je zde umístěn Merkle root, což je kořenová hash Merkle tree vypočítaná ze všech transakcí, které mají být zahrnuty do bloku.



Obr. 5 Merkle tree (hlavička bloku)
Zdroj: Nakamoto, 2008

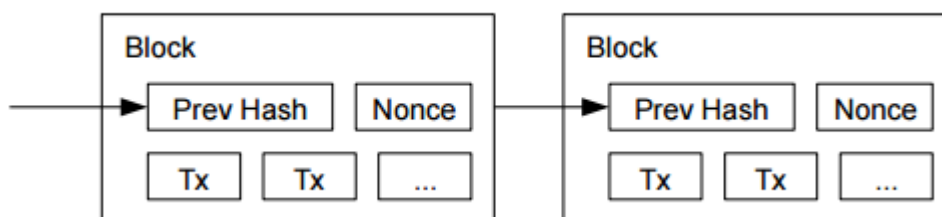
Merkle tree se vytváří tak, že se nejprve vypočte hash pro každou transakci v bloku. Tyto hashe jsou poté dány do párů po dvou, z těchto párů jsou opět vypočteny hashe a vznikne tak nový soubor hashí o polovičním množství. Tento postup se opakuje tak dlouho, dokud nezůstane jedna jediná hash, které se říká merkle root, která je následně umístěná v hlavičce bloku, viz obr. 5. Tomuto procesu

se říká „Simplified Payment Verification“, používá se u některých Bitcoin klientů, které díky tomu nemusí stahovat celý blockchain, viz kapitola 6.2 *Softwarová peněženka*. Bitcoin poskytuje způsob, jak rozdělit a sloučit bitcoiny v jednotlivých transakcích. Každá transakce má input (vstup) a output (výstup), kde každý výstup určuje adresu příjemce bitcoinů a částku, kterou má přijmout, každý vstup odkazuje na předchozí výstup, který byl utracen a digitální podpis plátce s odpovídajícím veřejným klíčem. Při ověřování transakce se vezme veřejný klíč, který byl nalezen na vstupu, vypočítá se z něj hash hodnota a porovná se s adresou uvedenou v dříve odkazovaném výstupu. (Huřták, 2013) Každý blok (kromě bloku Genesis) odkazuje na předchozí blok a tím vzniká blockchain. Blok je proto soubor transakcí s timestamp a připojeným proof of work. (Malone, 2015)

5.3.3 Proof of work

Proof of work byl původně navržen v práci *Hashcash* od Adama Backa z roku 2002 jako opatření k zabránění e-mailovému spamu. Vstup, který vytváří hash začínající na určitý řetězec, je také často označován jako „částečná hash kolize“ a proces hledání vhodného vstupu se nazývá mining. Například pokud budeme potřebovat určitý 32bitů dlouhý řetězec v binární reprezentaci hashe, očekávaný počet vstupů, které musíme vyzkoušet, je 232, což je více než 4 miliardy pokusů. Proof of work se používá v Bitcoinu ze dvou důvodů. Prvním je, že proof of work je prostředkem hlasování o transakční historii, kde čím víc práce člověk vykonává, tím větší hlasovací práva má. Druhým účelem je tvorba peněz.

Každý proof of work je založen na tom předchozím. Toho je dosaženo tím, že hash z předchozího proof of work je zahrnuta do vstupu aktuálního proof of work, tímto se vytváří řetězec bloků, jak je znázorněno na obr. 6. Vstupní údaje jsou pro výpočet proof of work spojeny do bloků a všechny bloky dohromady vytváří blockchain.



Obr. 6 Řetězec bloků (blockchain)
Zdroj: Nakamoto, 2008

BitcoinWiki (2015) vysvětluje proof of work na následujícím příkladu. Řekněme, že základní řetězec, se kterým budeme pracovat, obsahuje text „Hello, world!“ Naším cílem bude nalézt takovou variantu SHA-256 hashe, který začíná „000“. Po každém pokusu přidáme na konec řetězu celé číslo tzv. nonce, které se s každým pokusem zvětší o jednotku (0, 1, 2,...). Nalezení požadované hash hodnoty pro „Hello, world!“ nám v tomto případě zabere 4521 pokusů, viz obr. 7. Vytvoření

4251 hash hodnot nezabere na moderním počítači moc času, většina počítačů dokáže vypočítat 4 miliony hash hodnot za sekundu. Bitcoin automaticky reguluje obtížnost nalezení hashe tak, aby čas mezi jednotlivými vytvořenými bloky byl přibližně 10 minut.

```
"Hello, world!0" => 1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64
"Hello, world!1" => e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8
"Hello, world!2" => ae37343a357a8297591625e7134cbea22f5928be8ca2a32aa475cf05fd4266b7
...
"Hello, world!4248" => 6e110d98b388e77e9c6f042ac6b497cec46660deef75a55ebc7cfd65cc0b965
"Hello, world!4249" => c004190b822f1669cac8dc37e761cb73652e7832fb814565702245cf26ebb9e6
"Hello, world!4250" => 0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9
```

Obr. 7 Příklad nalezení hash hodnoty pro „Hello, world!“ začínající „000“
Zdroj: BitcoinWiki, 2015

5.3.4 Mining

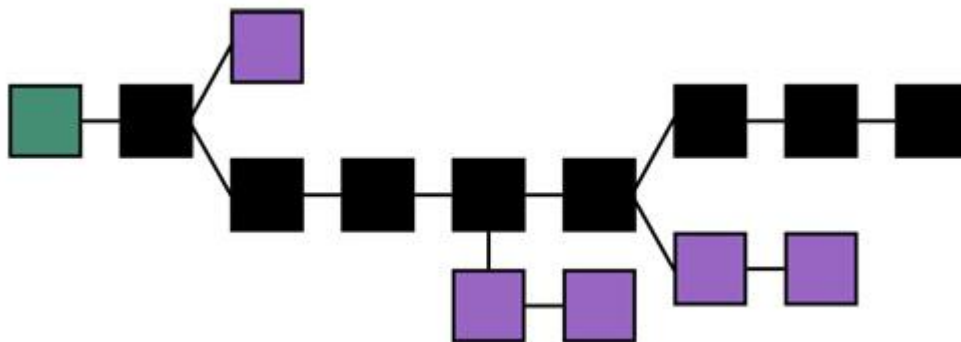
Mining je proces, při kterém se využívá výpočetní výkon k hledání validních bloků, a zároveň vytváření nových bitcoinů. Technicky řečeno, mining je proces počítání hash hlaviček bloku, který zahrnuje kromě jiných věcí, odkaz na předešlý blok, hash transakcí a nonce. Pokud je hash hodnota nalezena menší než aktuální daný „cíl“ (což je inverzně úměrné obtížnosti), vytvoří se nový blok a těžař za odvedenou práci dostane určitý počet nových bitcoinů. Celý proces generování bitcoinů limituje množství vydaných bitcoinů na 21 milionů, které se vytěží zhruba v roce 2140. V době psaní této práce je již vytěženo 15 milionů BTC. Na začátku vzniklo při mining 50 BTC přibližně každých 10 min. Toto číslo se každé 4 roky snižuje na polovinu, takže v současnosti za vytěžený blok dostaneme 25 BTC až do roku 2016, kdy bude opět suma bitcoinů snížena na polovinu, tedy 12,5 BTC. (Wilcox, 2015) Kromě nových bitcoinů je těžař (miner) odměněn ještě transakčními poplatky za potvrzení transakcí, které jsou dobrovolné, doporučený poplatek je 0,0001 BTC, což je přibližně 1 Kč.

5.3.5 Blockchain

Podle Franca (2014) je blockchain nepochybně nejdůležitější inovací představenou protokolem Bitcoin. Díky ní fungují distribuované P2P digitální měny. Blockchain je v podstatě distribuovaná databáze držící všechny bitcoin transakce od počátku (3. ledna 2009) a metoda zabezpečení této databáze použitím proof of work. Útočník, který by chtěl změnit blockchain, by musel vynaložit tak velkou výpočetní sílu, jako byla výpočetní síla, která byla použita od dané chvíle až po současnost.

V případě, že jsou nalezeny různé bloky zároveň různými těžaři, může se stát, že se blockchain dočasně rozvětví. Nakonec ale pouze jeden blok může být součástí blockchainu. (Antonopoulos, 2015) Řetězec, do kterého je investováno více výpočetního výkonu se nakonec stane delší a další uzly (uživatelé) budou preferovat nejdelší podřetězec a tím zaniknou ostatní větvení. Na obr. 8 je ukázka větvení blockchainu, černý řetězec je nejdelší a proto je preferován uzly sítě. V dů-

sledku toho bude blockchain obsahovat jen ty transakce, se kterými bude většina sítě souhlasit. Pokud se uzel řídí výše uvedenými pravidly, považujeme jej za poctivý. Důležitou podmínkou, která musí být dodržena za účelem úspěšného fungování Bitcoinu, je, že poctivé uzly musí mít vždy větší výpočetní výkon než útočníci. (Nakamoto, 2008)



Obr. 8 Větvení blockchainu
Zdroj: Hruska, 2014

5.4 Vlastnosti Bitcoinu

Bitcoin je decentralizovaný, to znamená, že neexistuje žádná centrální autorita, která by ho ovládala. Nemůže se stát, že by nám např. vláda zmrazila účet, nebo omezila výběry z bankomatů jako v případě Kypru v roce 2013. Bitcoin je pseudo-anonymní, protože všechny transakce jsou veřejné v blockchainu, ale nikdo neví, komu patří které bitcoinové adresy. Každý uživatel navíc má právo vlastnit neomezené množství bitcoinových adres. (Guttman, 2014)

Dále shrnu výhody a nevýhody Bitcoinu vyplývající z jeho vlastností a principů.

5.4.1 Výhody Bitcoinu

Výhodami Bitcoinu jsou:

- Rychlost transakcí – u bitcoinu nezáleží na tom, zda je víkend či svátek, transakce probíhají maximálně v řádu minut.
- Nízké náklady – poplatky jsou buď nulové, nebo extrémně nízké. Jsou dobrovolné, jako odměna za připsání transakce do bloku.
- Systém je velmi odolný proti kolapsu. Velká část uživatelů vlastní ve svém počítači kopii transakční historie celé sítě. I kdyby na polovině zeměkoule vyhořely všechny počítače, stavy účtů budou zachovány a systém bude fungovat dál. (Málek, 2013)
- Do jisté míry anonymita – „Každý v historii sítě může vidět, že byly poslány bitcoiny z této adresy na nějakou jinou, ale nikdo neví, že patří zrovna vám, komu a

kolik BTC posíláte. Adresa neobsahuje žádný identifikační znak vašeho počítače. Pro každou platbu si navíc může příjemce i odesílatel vytvořit pokaždé novou adresu.“ (Fillner, 2014)

- Nepodléhá inflaci – právě proto, že je bitcoinů omezený počet, má spíše deflační² charakter.
- Nedají se zfalšovat – všechny transakce jsou pod kontrolou celé sítě.
- Nepodléhají kontrole žádné instituci, ani soukromé osobě – je imunní vůči např. korupci, nehrozí zmrazení účtu.
- Jednotná měna - nemusíme řešit složité převody a přehnané poplatky, když chceme poslat peníze např. do Vietnamu.
- Volatilita kurzu – pro investory, kteří rádi spekulují, i v rámci arbitráže.

5.4.2 Nevýhody Bitcoinu

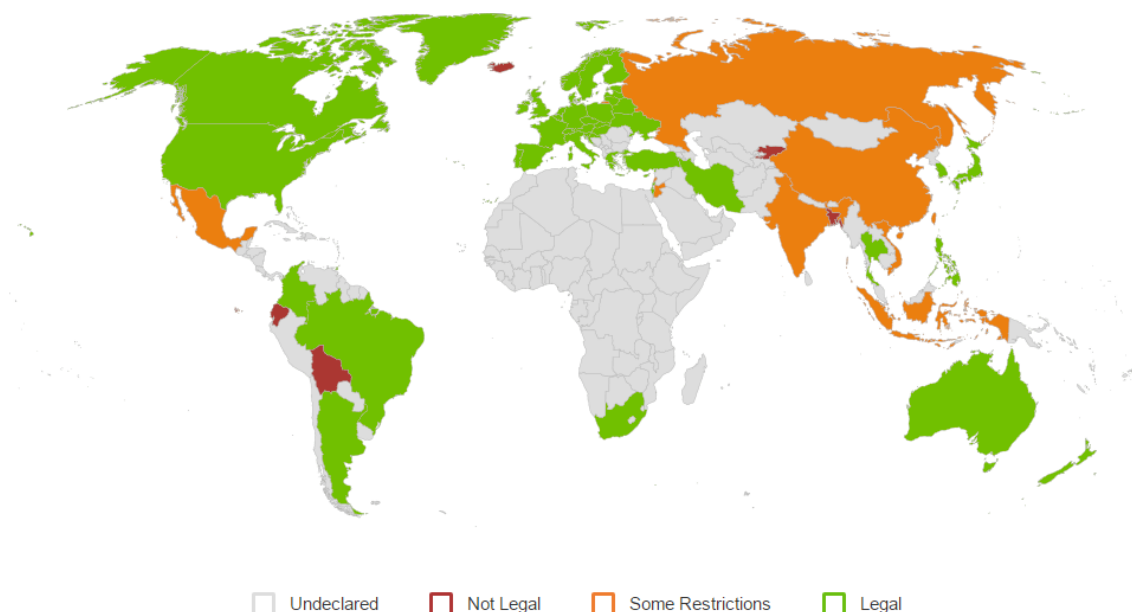
Nevýhodami Bitcoinu jsou:

- Nestabilní kurz – pro běžné uživatele a obchodníky, zejména kamenné obchody.
- Transakce jsou nevratné.
- Bitcoin je závislý na internetu.
- Při ztrátě hesla nebo celé bitcoinové peněženky nemáme šanci se k bitcoinům dostat. Doporučuje se napsat si heslo zvlášť na papír a uchovat odděleně od počítače, či se dá soubor s peněženkou uchovat i offline. Při vlastnění většího obnosu bitcoinů se můžeme zamyslet i nad variantou BTC trezoru, více v kapitole 6.2.6 *Hardwarová peněženka*.
- Zneužití anonymity – na financování nelegálních aktivit (např. nelegální tržiště Silk Road)

5.5 Právní regulace Bitcoinu

Právní status Bitcoinu se v jednotlivých zemích liší a v některých z nich stále není definovaný. Zatímco některé země výslovně povolují užívání a obchod s bitcoiny, jiné země Bitcoin zakazují, či vydávají patřičné restriktce. Různé vlády klasifikují bitcoiny odlišně. Cílem této kapitoly je shrnout postoj jednotlivých států vůči Bitcoinu.

² Deflace je opakem inflace. Peníze tedy získávají na hodnotě.



Obr. 9 Právní regulace bitcoinu na mapě
Zdroj: coin.co, 2015

5.5.1 Česká republika

V únoru 2014 vydala Česká národní banka (ČNB) dokument *Obchodování s bitcoiny*, ve kterém uvádí, že obchodování s bitcoiny nevyžaduje povolení ČNB, ani nepodléhá jejímu dohledu, protože data v Bitcoinu nemají charakter pohledávky držitele bitcoinů za jinou osobou (nejsou to tedy bezhotovostní peníze, ani elektronické peníze), také proto, že nákup či prodej bitcoinů na vlastní účet nepředstavuje žádnou z platebních služeb. Dále uvádí: „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.“ Avšak výjimkou je obchodování s deriváty bitcoinu, správa fondu investujícího do bitcoinů a provádění platebních transakcí v souvislosti s organizací obchodů s bitcoiny. Důsledkem je současně to, že finanční instituce s povolením ČNB nesmějí na základě tohoto povolení s bitcoiny obchodovat nad rámec správy vlastního majetku, tedy způsobem vyžadujícím podnikatelské oprávnění. Z hlediska aplikace opatření proti legalizaci výnosů z trestné činnosti a financování terorismu je v první řadě podstatné vymezení okruhu povinných osob (§2 AMLZ). Pokud se povinná osoba (tj. finanční instituce, obchodník s nemovitostmi či kulturními památkami, provozovatel loterie aj.) v rámci své podnikatelské činnosti setká s obchody s bitcoiny, měla by jim věnovat zvýšenou pozornost.

V září 2013 vydal Finanční analytický útvar Ministerstva financí (FAÚ) *Metodický pokyn o přístupu povinných osob k digitálním měnám*. V tomto dokumentu vyzývá všechny povinné osoby, aby v souvislosti s nákupem/prodejem jakékoli

digitální měny (např. Bitcoin), byla každá platba nad hodnotu 1 000 EUR posouzena jako velmi riziková, a každá transakce nad hodnotu 15 000 EUR vždy oznámena jako podezřelý obchod.

V dubnu 2015 vydal guvernér ČNB Miroslav Singer dokument *Bezpečnost internetových plateb a virtuální „měny“ z pohledu ČNB*, ve kterém mimo jiné definuje postoj ČNB k virtuálním měnám. Podle ČNB virtuální „měny“ nejsou plnohodnotnou národní měnou, nejsou peněžní jednotkou žádného existujícího státu, ani peněžními prostředky ve smyslu zákona o platebním styku. Zdůrazňuje, že to nejsou měny. Naopak jsou virtuální měny používány jako zvláštní prostředek směny; představují hodnotu, která je vyjádřena digitálně a mohou být evidovány nebo obchodovány v elektronické podobě. Dále upozorňuje, že je používání virtuálních měn spojeno s mnoha riziky, které s jejich rozšiřováním pravděpodobně porostou. Česká republika tedy v současné době neuplatňuje žádná zvláštní zákonná opatření proti virtuálním měnám, která by je zakazovala, nebo omezovala. ČNB nevykonává dohled nad subjekty, které obchodují s virtuálními měnami. Jejich vývoj nekomentuje, ale monitoruje oblast virtuálních měn.

5.5.2 Německo

V prosinci 2013 se vyjádřilo Ministerstvo financí k virtuálním měnám, které nepovažuje za elektronické peníze, ale soukromé peníze. Soukromé bitcoinové transakce či jejich zprostředkování je považováno za obchodování s pohledávkami a tudíž osvobozeno od DPH. V prosinci 2013 vydal Německý úřad pro regulaci bank dokument, ve kterém označil bitcoiny za účetní jednotku, tzn. že mohou být zařazeny pod finanční instrumenty. V podstatě to znamená, že regulace týkající se finančních instrumentů je aplikovatelná i na virtuální měny. Německo i Velká Británie vycházejí z Evropské směrnice o DPH, konkrétně z článku 135, který říká, že všechny aktivity označené jako obchodní nástroje jsou osvobozeny od DPH. Z pohledu Velké Británie je bitcoin obchodní nástroj, z pohledu Německa ale není. Hlavním rozdílem mezi těmito dvěma státy je ten, že v Německu existuje spousta regionálních měn vedle eura (např. v Bavorsku mají Chiembauger, který funguje na fyzické i digitální bázi). (Jackson, 2015)

5.5.3 Rusko

Ještě v polovině roku 2014 Rusko relativně podporovalo Bitcoin. Varovalo občany stejně jako ostatní země, nicméně viceguvernér Ruské centrální banky Georgij Lutnovskij na mezinárodním bankovním kongresu dokonce prohlásil, že kryptoměnám může patřit budoucnost. Doplnil však, že stejně jako vše nové se i kryptoměny dostávají do rukou kriminálků.

V polovině ledna roku 2015 se ale vše obrátilo a Rusko zablokovalo přístup na webové stránky, které se věnovaly kryptoměnám. „*Je zakázáno vydávat jiné peněžní jednotky a peněžní instituty. Za těchto okolností jsou kryptoměny včetně bitcoinu peněžními substituty, a jako takové přispívají k růstu stínové ekonomiky a ne-*

smí být používány občany a právníckými osobami na území Ruské federace,“ rozhodl ruský soud. (Stroukal, 2015)

V dubnu 2015 se v Moskvě na konferenci o bitcoinu projednával návrh na zákaz kryptoměn v Rusku, advokát Artem Tolkachev představil dokonce i sankce, které se dají očekávat při používání, distribuci a vytváření kryptoměn na ruském území (pokuta 5 000 až 20 000 rublů (cca 1800 – 7000 Kč)³ pro soukromé osoby a 50 000 až 1 000 000 rublů (cca 18 000-350 000 Kč) pro firemní subjekty. (Scott, 2015) Zatím však není nic oficiálně platné.

5.5.4 Evropská unie

V říjnu 2012 vydala Evropská centrální banka (dále ECB) dokument *Virtual currency schemes (Virtuální měny)*, kde poprvé definovala virtuální měnu jako typ neregulovaných digitálních peněz, které jsou vydávány a obvykle kontrolovány jejich tvůrci a užívány a přijímány mezi členy specifické virtuální komunity.

V prosinci 2013 vydal Evropský orgán pro bankovníctví (EPA) *Varování pro spotřebitele týkající se virtuálních měn*. V tomto dokumentu popsal základní charakteristiku a princip kryptoměn. Jako jedno z hlavních rizik uvedl riziko ztráty virtuálních měn na obchodních platformách a nemožnost spotřebitelů domoci se právní ochrany z důvodu chybějící regulace.

Jelikož si virtuální měny prošly pozoruhodným vývojem v dalších letech, vydala v únoru 2015 ECB další analýzu virtuálních měn *Virtual currency schemes – a further analysis*, kde v úvodu zdůrazňuje, že ačkoli se pojem „virtuální měna“ běžně používá (i v tomto dokumentu), tak ECB nepovažuje virtuální měny jako je Bitcoin za plnohodnotnou formu peněz, jak je definováno v ekonomické literatuře. V ekonomické teorii je v nejobecnějším pojetí za peníze považováno aktivum, které je všeobecně uznáváno a přijímáno ekonomickými subjekty jako prostředek při provádění plateb za zboží, služby nebo k úhradě jiných závazků. (Polouček a kol., 2009) Bitcoin nesplňuje už první část definice, která říká, že peníze musí být všeobecně uznávané.

Tabulka 1 uvádí postoj některých států EU k problematice virtuálních měn.

³ Při kurzu 0,36 CZK/RUB k 8. 12. 2015

Tab. 1 Vybrané státy EU a jejich postoj k virtuálním měnám

<i>Země</i>	<i>Vyjádření čl. země</i>	<i>Varování</i>	<i>Kontrola</i>
Belgie	Není zákonným platidlem ani elektronickými penězi	ano	
Česká republika	Bitcoin nejsou formou bezhotovostních ani elektronických peněz	ano	Standardní úkony zahrnující bitcoiny nejsou kontrolovány. Některá využití mohou vyžadovat licenci.
Dánsko	Bitcoin není měna a nemá hodnotu v porovnání např. se zlatem	ano	Ne. Bitcoin by měly být regulovány na evropské či globální úrovni.
Finsko	Není měnou ani platebním instrumentem		Ne.
Francie		ano	Pro provoz bitcoinové směnárny je vyžadována licence. V některých případech realizace zisku vyžadováno prohlášení u francouzské agentury proti praní špinavých peněz.
Německo	Není zákonné platidlo, ale finanční instrument, zúčtovací jednotka.	ano	Standardní úkony zahrnující bitcoiny nejsou kontrolovány. Některá využití mohou vyžadovat licenci.
Slovensko		ano	Ne.
Švédsko	Aktivum (není měnou)		Směnárny virtuálních měn se musí registrovat u finančního kontrolora.
Velká Británie	Využívá se jako peníze pouze v omezeném rozsahu a relativně málo lidmi.	ano	

Zdroj: Virtual currency schemes – a further analysis, 2015

Žádná z členských zemí EU nepovažuje virtuální měnu za zákonné platidlo, většina z nich varuje uživatele před používáním virtuálních měn. Koncem října 2015 rozhodl Evropský soudní dvůr, že se na bitcoinové transakce nebude vztahovat daň z přidané hodnoty. Tato zpráva měla pozitivní vliv na tržní cenu bitcoinu, která okamžitě vzrostla z cca 270 USD na cca 300 USD. (Perez, 2015)

5.5.5 USA

Jako první se ve Spojených státech amerických zabývala virtuálními měnami FBI, která už v dubnu 2012 vydala dokument *Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity*, ve kterém vyjádřila obavy ohledně možného zneužití virtuálních měn s nelegálními aktivitami jako je nákup nelegálního zboží, praní špinavých peněz, apod. Dalším orgánem, který se vyjádřil k problematice virtuálních měn je úřad amerického Ministerstva financí FinCEN (Financial Crimes Enforcement Network), který vydal v březnu 2013 *Application of FinCEN's Regulation to Persons Administering, Exchanging, or Using Virtual Currencies*, kde prohlásil, že užívání virtuálních měn nespadá pod peněžní služby (MSB – Money Services Business) v režimu regulace FinCEN a proto není předmětem MSB evidence, hlášení a uchovávání záznamů pro regulaci, což znamená, že v USA nepotřebujete žádné povolení k používání bitcoinu.

Stát New York v červnu 2015 prostřednictvím Úřadu pro kontrolu finančních služeb v New Yorku (NYDFS) vydal dlouho očekávaný seznam pravidel a předpisů (BitLicence), které budou potřebné pro založení a fungování bitcoinových firem. Jedná se o všechny služby, které budou poskytovat transfer měny – burzy a směnárnny, platební brány, těžařské pooly apod. Podle Commodity Futures Trading Commission (CFTC) je Bitcoin považován od září 2015 za komoditu vedle zlata a ropy, a z toho vyplývá regulatorní pravomoc tohoto orgánu na BTC trzích.

5.5.6 Čína

Pro Čínu je Bitcoin zajímavý nejen ze spekulativního hlediska. V zemi jsou totiž relativně tvrdá opatření určená k tomu, aby nebylo možné místní měnu juan vyvážet. Čína podle mnohých pozorovatelů drží svou měnu dlouhodobě podhodnocenou, aby zvýhodnila vývozce, a aby byla taková situace udržitelná, je její směnitelnost omezena.

Striktní zákaz Bitcoinu v Číně vytvořil velké a nestálé cenové výkyvy i na jiných jurisdikcích a trzích. Například v říjnu 2013, prohlášení, že Baidu (čínská obdoba Googlu) přijímá BTC platby, vytvořilo velkou poptávku po bitcoinech, a tím obrovský skok jeho ceny (na začátku října měl Bitcoin hodnotu 120 USD, na konci října 1120 USD). (Cinch, 2013) O dva měsíce později, v prosinci 2013, vydala Čínská centrální banka prohlášení o tom, že bitcoin není měna a nemá stejný právní status jako oficiální měny a zakázala finančním institucím a poskytovatelům platebních služeb účast na transakcích spojených s bitcoiny. (Bloomberg, 2013) Kurz bitcoinu okamžitě propadl na cca 600 USD, kdy hlavní burza BTC China uvedla, že už nepřijímá vklady v čínských juanech. (Riley, Yan, 2013)

Komerční banky byly v červnu 2014 instruovány k upozornění klientů na zákaz Bitcoinu. Navzdory těmto varováním směnárnny digitálních měn identifikovaly kreativní cesty, jak obejít vládní restriktce. Například instalace BTC automatu a spuštění kup-a-prodej aplikace burzy BTC China. Bitcoinové automaty totiž nejsou spojeny s čínskými komerčními bankami. Ačkoli mají finanční instituce striktně zakázané styky s bitcoiny, žádné čínské zákony výslovně nezakazují vlastnění

bitcoinů občanům. Konfliktní pozice Čínské centrální banky způsobily velký zmatek a frustraci uživatelů bitcoinů uvnitř i vně Číny. Například v prosinci 2013, kdy Čínská centrální banka definovala Bitcoin jako virtuální zboží. Nicméně finanční společnosti nesmí podporovat Bitcoin. Bitcoin směnárny se musí registrovat na Ministerstvu průmyslu a informační technologie. Webové stránky sloužící jako Bitcoin obchodní platformy se také musí registrovat na Telekomunikačním úřadě v souladu s Čínskými telekomunikačními regulacemi a Čínskému zákonu proti praní špinavých peněz. Od konce ledna 2014 burza BTC China opět přijímá vklady v yuanech. (Ponsford, 2015)

5.5.7 Země s restrikcí Bitcoinu

Nejaktuálnější zemí, která vyjádřila nepřátelský postoj vůči Bitcoinu, je Taiwan. Po incidentu v listopadu 2015, kdy únosci předního obchodního magnáta v Taiwanu vyžadovali výkupné v bitcoinech, prohlásil předseda Finanční dozorčí komise, že je Bitcoin nelegální. Dále prohlásil, že budou spolupracovat s Taiwanskou národní bankou a „law enforcement agencies“⁵ k ráznému zakročení proti jakýmkoli nelegálním aktivitám v souvislosti s Bitcoinem. (Das, 2015)

V červnu 2014 oficiálně zakázala centrální banka v Bolívii jakoukoli měnu či mince, které nejsou vydávané nebo regulované vládou, a to včetně bitcoinu a dalších kryptoměn jako je namecoin, peercoin, Quark, primecoin a feathercoin. (Rizzo, 2014)

V Bangladéši je Bitcoin úplně zakázaný s trestem odnětí svobody až na 12 let. *„Bitcoin není legální měnou žádné země. Každá transakce přes Bitcoin či jakoukoli jinou kryptoměnou je trestný čin,“* prohlásila Bangladéšská centrální banka v září 2014. (Dhaka Tribune, 2014)

V červenci 2014 Národní shromáždění Ekvádoru účinně zakázalo bitcoin a decentralizované digitální měny, přičemž zakládají pokyny k tvorbě nové státní digitální měny. Ekvádor je tak první zemí s vlastní národní kryptoměnou. (Khaosan, 2014)

V březnu 2014 vydala Centrální banka Islandu prohlášení, ve kterém pojednává o právním postavení digitální měny v Islandu. Její nákup může porušovat Islandský devizový zákon, který specifikuje, že islandská měna nesmí opustit zemi.

V Thajsku není Bitcoin přímo nelegální, ale Thajská banka varuje spotřebitele, že to není měna a že jeho používání je na vlastní riziko. Banka popisuje Bitcoin jako *„digitální data, tudíž není považován za měnu a nedá se jím platit a není považován za zákonné platidlo jako peníze.“* (Palmer, 2014)

V květnu 2014 vydala Centrální banka Kyrgyzstánu prohlášení, ve které považuje Bitcoin a ostatní digitální měny za nelegální. (financemagnates.com, 2014)

Vietnamská centrální banka v březnu 2014 prohlásila, že Bitcoin a ostatní virtuální měny nejsou zákonným platidlem a nejsou platebním nástrojem ve Vietnamu, proto užívání Bitcoinu a dalších virtuálních měn nejsou akceptovány, ani chrá-

⁵ Agentury specifické pro severoamerickou kulturu, částečně odpovídají našim „orgánům činným v trestním řízení“

něny zákonem. Dále varuje občany: „... občané by neměli investovat, držet, ani uskutečňovat transakce související s bitcoiny, ani dalšími virtuálními měny.“ Příímý zákaz ve Vietnamu není, i když se média dále snaží překrucovat fakta. (Phil, 2015)

5.5.8 Závěr kapitoly

V této kapitole jsem shrnula postoj vybraných zemí vůči Bitcoinu a kryptoměnám obecně. V žádné zemi není Bitcoin považován za národní měnu, ale například v Německu je považován za účetní jednotku, což spadá pod finanční instrumenty a veškeré regulace finančních instrumentů se tedy týkají i bitcoinů. Evropská unie zaujímá neutrální postoj, virtuální měny nepodporuje, ani nezakazuje.

V prosinci 2013 vydal Evropský orgán pro bankovníctví (EPA) *Varování pro spotřebitele týkající se virtuálních měn*, kde jako jedno z hlavních rizik uvedl riziko ztráty virtuálních měn na obchodních platformách a nemožnost spotřebitelů domoci se právní ochrany z důvodu chybějící regulace.

Od října 2015 se na bitcoinová transakce nevztahuje DPH. Česká republika stejně jako EU nepovažuje virtuální „měny“ za měny a v současné době neuplatňuje žádná zvláštní zákonná opatření proti virtuálním měnám, která by je zakazovala, nebo omezovala. ČNB nevykonává dohled nad subjekty, které obchodují s virtuálními měnami.

V Rusku se v dubnu 2015 na konferenci o bitcoinu projednával návrh na zákaz kryptoměn, zatím však není nic oficiálně platné. V USA jsou bitcoiny považovány za komoditu vedle např. zlata a ropy. Stát New York vydal v červnu 2015 BitLicense, tedy předpisy, podle kterých se musí řídit všechny firmy, které obchodují s virtuálními měnami.

V Číně je pro finanční instituce zakázané obchodování s bitcoiny. Další země, které zaujímají nepřátelský postoj k virtuálním měnám s částečným až úplným zákazem, jsou Taiwan, Bolívie, Bangladéš, Ekvádor, Island, Kyrgyzstán, Thajsko a Vietnam. Ekvádor jako první země pracuje na tvorbě vlastní národní kryptoměny.

5.6 Vývoj Bitcoinu

V této kapitole se zaměřím na vývoj ceny (kurzu BTC/USD) bitcoinu od počátku (2009) po současnost (12/2015), který znázorňuje obr. 10. V každém roce stručně popíšu události, které měly či mohly mít vliv na cenu bitcoinu. Informace jsou čerpány z historyofbitcoin.org.



Obr. 10 Vývoj kurzu USD/BTC
Zdroj: blockchain.info, 2016

5.6.1 Události roku 2009

V lednu byl vytěžen první blok, kterému se říká také Genesis, a takto bylo vytěženo prvních 50 bitcoinů na světě. Ve stejném měsíci proběhla první transakce v síti mezi Nakamoto a Hanney, vývojářem a kryptografickým aktivistou, jednalo se o 100 BTC.

V říjnu byl stanoven první kurz BTC, který nedosahoval ani jednoho dolaru. Byl stanoven podle nákladů na elektřinu potřebnou k vytěžení jednoho bitcoinu.

5.6.2 Události roku 2010

V únoru vznikla první směnárna „Bitcoin market“, kde se daly koupit bitcoiny.

V květnu proběhl první nákup zaplacený bitcoiny, jednalo se o nákup dvou pizz v hodnotě 25 USD za neuvěřitelných 10 000 BTC.

V červenci vznikla jedna z největších bitcoin směnárén MtGox.

Koncem tohoto roku byl vytěžen první blok prvního poolu na světě, který založil český programátor Marek „Slush“ Palatinus.

5.6.3 Události roku 2011

V tomto roce vznikl Silk Road, což bylo online tržiště, kde se dalo nakupovat za bitcoiny.

Během ledna a února se kurz bitcoinu začal zvyšovat (už na konci ledna se vytěžilo 25% všech bitcoinů) a v dubnu dosáhl hodnoty 1 USD.

V červnu dokonce dosáhl kurzu 10 USD/BTC na MtGox a za pouhé 4 dny se kurz vyšplhal na neuvěřitelných 32,91 USD/BTC, mluvíme o tzv. velké bublině roku 2011. Ve stejném měsíci byla nahlášena největší krádež bitcoinů do té doby, uživatelem *allinvain*, jednalo se o 25 000 BTC.

Koncem července přišla třetí největší směnárna na světě, Bitomat, o 17 000 BTC a o týden později přišel i MyBitcoin (jeden z prvních poskytovatelů elektronických peněženek) o 150 000 BTC. Po těchto událostech spadla cena bitcoinu na cca 6 USD.

5.6.4 Události roku 2012

Tento rok nebyl pro Bitcoin velmi příznivý, došlo k několika útokům hackerů. Cena za jeden bitcoin se pohybovala okolo 4 USD.

Na konci roku se vytěžil první blok s poloviční odměnou, tedy 25 BTC. Na druhou stranu ale spousta společností začalo přijímat bitcoiny a díky tomu kurz stále pomalu rostl.

5.6.5 Události roku 2013

Tento rok je pro Bitcoin zlomový, začínají se o něj zajímat média, která zvýší popularitu a povědomí o Bitcoinu, což se pozitivně projeví na jeho ceně.

Na konci února dosáhne kurzu 30 USD/BTC, což je poprvé od června 2011.

Na konce března během 2 dnů vzroste kurz o skoro 70 % a dosáhne ceny 74,9 USD. V dubnu se kurz dostane na 266 USD, ve stejném měsíci ale spadne kurz kvůli útoku hackerů na Bitcoin Central, kde došlo ke ztrátě několika tisíc bitcoinů.

V květnu se navíc přišlo na to, že společnost ESEA s online hrami tajně využívala počítače hráčů na těžení bitcoinů. Ve stejném měsíci byl uveden do provozu první automat na bitcoiny na světě, v Kalifornii. Některé státy začínají regulovat tuto měnu. Například v srpnu uznalo Německo bitcoin jako oficiální měnu a v některých případech se můžou transakce i danit. Při držení bitcoinů déle než jeden rok jsou osvobozeni od daně.

V říjnu pozastavila FBI provoz na Silk Road kvůli podezření z prodeje drog a zabavení bitcoiny v hodnotě 3,6 milionů dolarů. Tato událost vedla k malému propadu kurzu, který se ale zase vrátil na původní hodnotu.

V listopadu dosáhne kurzu 1000 USD/BTC, lidé používají bitcoiny k převodům peněz víc než Western Union. „... Tehdy úřadující šéf FEDu Ben Bernanke se o kryptoměnách obecně vyjádřil velmi pozitivně a jeho slova před Senátem měla obrovský vliv i na růst ceny bitcoinu, litecoinu a dalších alternativních měn v závěru roku.“ (Fillner, 2014)

Kurz stále roste díky čínskému trhu. Začátkem prosince se hodnota vyšplhá na úplné maximum, a to 1151 USD, ale dlouho se neudrží kvůli více událostem. Jednak došlo k největší krádeži v historii z Sheep Marketplace, online drogové stránky, jedná se o 96 000 BTC a pár dní na to vyhlásila čínská centrální banka zá-

kaz obchodování s BTC (jen pro banky, ale média většinou špatně interpretovala zprávy). Také se projevují dlouhodobé problémy na burze MtGox, která nevyplácela svým klientům peníze, což způsobilo propad kurzu až o 20 %.

5.6.6 Události roku 2014

V únoru došlo k očekávanému krachu burzy MtGox. Lidé mimo Bitcoin ztrácejí důvěru v tuto měnu, protože si spojují MtGox a Bitcoin právě proto, že vznikla jako jedna z prvních směnárén. Odborníci (např. Palatinus) se však k této události staví pozitivně. Podle Palatina se aspoň trh očistí od špinavých hráčů, problém připisuje hlavně nekompetentnosti provozovatelů. (Slížek, 2014)

V březnu vznikla první bitcoinová banka Neo&Bee v Kypru.

Na konci března Dánsko oznámilo, že veškeré zisky z obchodů s bitcoiny jsou osvobozené od daně z příjmu, výjimkou jsou společnosti, které mají obchod s virtuálními měnami jako hlavní činnost.

V květnu se stal bitcoin součástí volební kampaně USA, což bylo velmi příznivé pro jeho cenu.

V červnu ale přišel krátkodobý pokles jako reakce na to, že vláda USA prodá zabavené bitcoiny ze Silk Road.

V červenci začala společnost Dell (třetí největší společnost v USA) akceptovat bitcoiny, celkově roste počet velkých firem akceptujících BTC.

V září začíná klesat cena, přestože se to v médiích hemží pozitivními zprávami, možných důvodů je více, uvedu jeden z nich. Zvyšující se počet firem akceptujících Bitcoin je sice pozitivní zprávou pro veřejnost, tyto firmy ovšem přijaté bitcoiny dlouho nedoručí a okamžitě je směňují za fiat, zvyšuje se tak nabídka bitcoinů na trhu a klesá tak jejich cena.

5.6.7 Události roku 2015

Od začátku roku začal kurz neuvěřitelně klesat, až o 40 %. Jednou z příčin mohl být další hackerský útok na Bitstamp (jedna z největších BTC směnárén), při kterém zmizelo 19 000 BTC v hodnotě 5 milionů dolarů, mohl to být Ruskem, které zakázalo přístup k bitcoinovým webům, nejpravděpodobnější je ale to, že se už čím dál méně vyplácí těžit bitcoiny kvůli vysokým nákladům.

V únoru se bitcoinová platforma Coinbase dostává i do ČR.

V květnu zrušil ruský soud zákaz webových stránek o bitcoinu.

V červenci čelila bitcoinová síť dosud nevídanému útoku, kdy byl blockchain zaplaven obrovským množstvím mikrotransakcí s velkým objemem dat. Na vrcholu zatížení se nahromadilo více než 50 000 transakcí čekajících na zařazení do bloku. (Donnelly, 2015)

Na konci října rozhodl Evropský soudní dvůr o tom, že budou bitcoinové transakce osvobozeny od DPH, což pozitivně ovlivnilo vývoj kurzu.

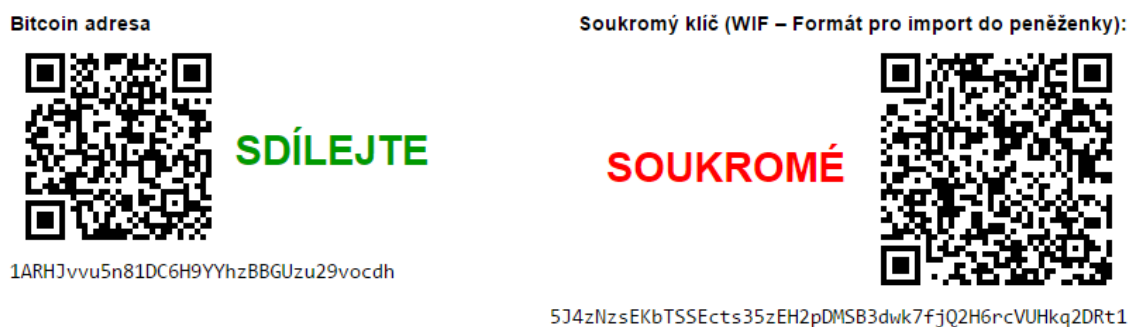
6 Bitcoin jako platební nástroj

V této kapitole uvedu možnosti jak uchovávat bitcoiny v různých typech BTC klientů (peněženkách), dále jak získat bitcoiny a využití Bitcoinu jako platebního nástroje v rámci nákupů za bitcoiny na e-shopech v ČR a v rámci zahraničního platebního styku.

6.1 Jak uchovávat bitcoiny

Dříve, než budeme vlastnit nějaké bitcoiny, je třeba mít peněženku, do které si bitcoiny můžeme „uschovat“. Cílem kapitoly je doporučit nejvhodnější peněženku pro běžného uživatele.

Uživatel komunikuje s bitcoinovou sítí pomocí peněženky. Jedná se o software, který generuje adresy a příslušné klíče, zobrazuje jejich zůstatky a umožňuje oznámení transakcí. Nejjednodušší a nejrychlejší způsob, jak vytvořit Bitcoin peněženku, je za pomoci některého z online generátorů, jako je například Bitaddress.org. Tato služba je open source, dostupná ve dvanácti jazycích včetně češtiny, a generování adres probíhá v JavaScriptu lokálně na počítači uživatele. Na bitaddress.org (viz obr. 11) se vygeneroval pár klíčů po náhodném hýbání s myší a zadání náhodných znaků do příslušného pole. Veřejný klíč je tzv. bitcoinová adresa (něco jako číslo účtu), na kterou nám ostatní uživatelé mohou posílat bitcoiny, a soukromý klíč nám garantuje přístup k bitcoinům na této adrese. Pro zabezpečení peněženky je důležité provést zálohu soukromého klíče a jeho uschování na bezpečném místě. Při ztrátě soukromého klíče ztrácíme přístup ke svým bitcoinům jednou provždy.



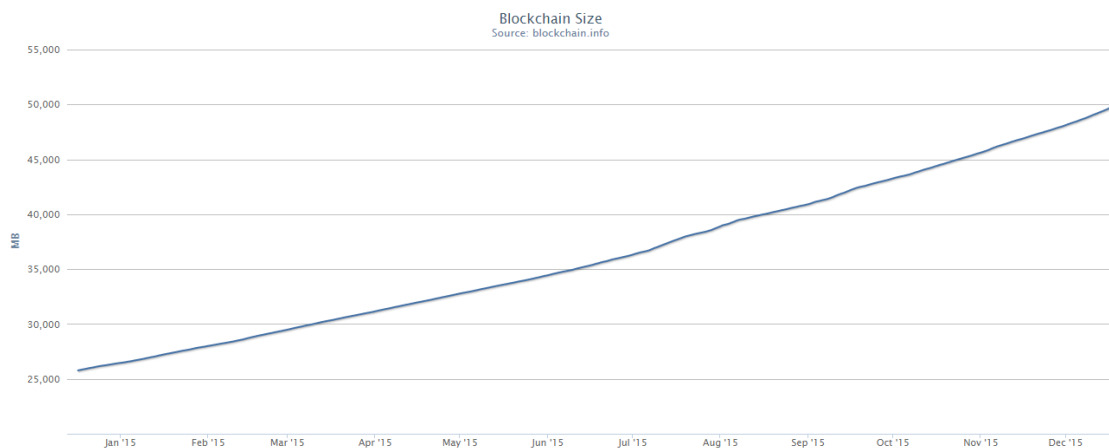
Obr. 11 Generátor Bitaddress
Zdroj: Bitaddress.org, 2015

6.2 Softwarová peněženka

Rozlišujeme 4 základní typy softwarových peněženek, podle toho, kde budeme mít uložené bitcoiny a odkud k nim budeme mít přístup. U každého typu uvedu jeden praktický příklad té nejznámější peněženky, i když jich může být více druhů.

6.2.1 Základní softwarová peněženka

Bitcoin Core (dříve Bitcoin QT) je oficiální bitcoinová peněženka, pro kterou je charakteristické, že uchovává celý Blockchain (full klient). Momentálně je dostupná pro operační systémy Windows, Linux, Ubuntu a Mac OsX. Je velmi náročná na internetové připojení a vyžaduje poměrně velký prostor na pevném disku, který se bude logicky zvětšovat, protože se Blockchain zvětšuje. V době psaní této práce (12/2015) má velikost zhruba 50 GB a za poslední rok rostl rychlostí přibližně 2GB za měsíc, ale podle exponenciální křivky jde vidět, že roste čím dál rychleji, viz obr. 12. Už první synchronizace (stažení blockchainu) může trvat podle rychlosti připojení řádově i dny. Při každém přihlášení do peněženky se stahují nové části blockchainu od poslední synchronizace, což zabere další čas a prostor na pevném disku. Další nevýhodou full klienta je to, že můžeme mít jen jednu peněženku. Pro účely pouhé peněženky na občasné transakce je tento typ peněženky nevhodný.



Obr. 12 Velikost blockchainu
Zdroj: blockchain.info, 2015

6.2.2 Odlehčená softwarová peněženka

MultiBit je opensource program dostupný také pro operační systémy Windows, Linux a Mac OS X. Nestahuje celý Blockchain, ale jen hlavičky transakcí (header only klient), takže je mnohem úspornější a instalace trvá pár minut. S tímto počítal už od začátku Nakamoto ve svém úvodním dokumentu a tento mechanismus nazval „Zjednodušená platební kontrola“ („Simplified Payment Verification“, SPV), který prokazuje, že transakce skutečně byla zařazena do bloku, aniž bychom museli stahovat celý blok. Kromě toho MultiBit umožňuje vytváření nejen dalších adres, ale i vytváření dalších samostatných peněženek přímo v programu. Vytvoření peněženky mi trvalo asi 10 min, přičemž bylo nutné si na začátku zapsat na papír „datestamp“ a „wallet words“, a tento papír dobře uschovat, tyto 2 údaje potřebuji pro obnovu peněženky, v případě, že se mi stane něco s počítačem. Po ověření, že jsem si údaje správně zapsala, si zvolím dostatečně silné heslo, které budu potře-

bovat při posílání bitcoinů, MultiBit následně provede automaticky zálohu a vytvoří se tak nová peněženka. Další „odlehčenou“ peněženkou je například Electrum.

6.2.3 Online peněženka

Coinbase je jedna z nejoblíbenějších platforem na světě, kde můžeme nakupovat, prodávat i uchovávat bitcoiny v reálném čase. Výhodou online peněženek (thin klient) je, že jsou jednoduché, přehledné, máme k nim přístup kdykoli a kdekoli na světě, dají se používat synchronizovaně na více zařízeních, nemusíme se starat o zálohování, na druhou stranu ale nemáme plnou kontrolu nad svými bitcoiny, je potřeba důvěry v poskytovatele, protože má plný přístup k našim bitcoinům, doporučuje se mít na online peněžence jen malý obnos na drobné nákupy v obchodech, restauracích, apod. a hlavní část bitcoinů mít na počítači, nebo při větších částkách v hardwarové peněžence, ke které se ještě dostaneme. Coinbase se snaží o mimořádnou ochranu svých vkladatelů a snaží se maximum bitcoinů odpojit od internetu, aby zamezila při případném prolomení ochrany kompletní ztrátě. V praxi tedy 98 % všech bitcoinů jsou uchovávány na odpojených discích i papírových zálohách ve fyzické šifrované podobě. Riziko se snaží rozkládat i tak, že jsou jednotlivé zálohy rozmístěny v různých částech celého světa, čímž snižují jak geopolitické riziko, tak i riziko nastání přírodní katastrofy. (coinbase.com, 2015)

Od konce listopadu 2015 spustila na americkém trhu dokonce vlastní platební karty SHIFT, kterými lze platit jako běžnou debetní kartou. Jediným poplatkem ze začátku je 10 USD, které slouží k autorizaci a aktivaci karty, a také k pojištění proti zneužití, žádný roční poplatek už nemá a nabití pomocí domácí platby (v rámci USA) je bezplatné. V zahraničí se platí poplatek 3 % z transakce a za výběr z bankomatu 2,5 USD. (Bedřich, 2015) Další důvěryhodná online peněženka je na platformě Blockchain.info. Jsou to taky všechny peněženky založené na různých směnárnách a burzách.

6.2.4 Mobilní peněženka

Mycelium je mobilní bitcoin peněženka oceněna prestižním oceněním *Best Mobile App* od Blockchain.info v roce 2014. Mycelium je hodnocen jako třetí nejbezpečnější bitcoin aplikace a peněženková platforma u *Open Bitcoin Privacy Project*, hlavně protože poskytuje uživatelům 100 % kontrolu nad svými soukromými klíči, které nikdy neopustí zařízení, s výjimkou exportování. (Young, 2015) Je velmi praktická v tom, že nahrazuje klasickou peněženku, jelikož mobil nosíme vždy u sebe. Díky fotoaparátu, který má dnes každý chytrý telefon, mohou platby jednoduše probíhat naskenováním QR kódu, který poskytne obchodník. Peněženka se dá stáhnout bezplatně na trhu aplikací, je to otázka několika sekund. U mobilních peněženek je nejdůležitější vytvořit si zálohu, tzn. vyexportovat soukromý klíč, opsat si ho na papír, nebo rovnou vytisknout v podobě QR kódu a pečlivě uschovat. V případě, že bychom telefon ztratili, stačí znovu stáhnout mobilní peněženku a naskenovat QR kód, telefon si „přečte“ Blockchain a bitcoiny se objeví v peněžence. U peněžen-

ky Mycelium slouží jako záloha „master seed“, jedná se o soubor anglických slov, mají stejnou funkci jako „wallet words“ u MultiBitu. Mezi další mobilní peněženky patří Bitcoin Wallet, Blockchain, Coinbase, KnC Wallet.

6.2.5 Papírová peněženka

Podle Coindesk (2016) je papírová peněženka (obr. 13) dokument, který obsahuje kopie veřejného a soukromého klíče, často má i QR kódy, tudíž je můžeme jednoduše oskenovat a přidat klíče do softwarové peněženky pro provedení transakce. Výhodou papírových peněženek je to, že klíče nejsou uloženy nikde digitálně, a tak je nemůže nikdo „hacknout“. Ten, kdo drží peněženku ve svém vlastnictví, drží i možnost manipulace s penězi. Peněženku lze libovolně předávat, tedy měnit vlastníka bez záznamu v Blockchain, stejně jako u hotovosti. Jejich nevýhodou je, že papír i inkoust mohou degradovat a papír je navíc relativně křehký. Mimo to, pokud ztratíme papírovou peněženku, už se k bitcoinům nikdy nedostaneme.

Public Key:

Used to receive Bitcoins

Share this with anyone you wish

Private Key:

Used to spend Bitcoins

Never share this with anyone



Obr. 13 Papírová peněženka
Zdroj: bitcoinhelp.net, 2014

6.2.6 Hardwarová peněženka

Trezor (obr. 14) je produkt české značky SatoshiLabs, jejíž spoluzakladatelem je Marek „Slush“ Palatinus (také vynálezce konceptu těžících poolů). Jedná se o samostatnou počítačovou jednotku, hardwarovou peněženku, ve které je uložen privátní klíč. Jeho cena je nyní 99 USD, platí se bitcoiny. Trezor funguje tak,

že se transakce zadávají na obrazovce počítače, potvrzení soukromým klíčem však probíhá mimo počítač, a to několikanásobným ověřením správnosti bitcoin adresy a pouze jednosměrnou cestou, tedy pouze z Trezoru do počítače, to nás chrání před zavírovaným počítačem. Tím, že je zařízení izolované od PC a také jednostranné, nehrozí „přečtení“ hesla keyloggerem⁶. Navíc se transakce potvrzují mechanicky – tedy stisknutím tlačítka přímo na zařízení, což za nás žádný hacker neudělá. Instalace je sice zdouhavější, berme to ale jako daň za bezpečnost už při instalaci. K vytvoření zálohy vytváří tzv. recovery seed, který funguje na stejném principu, jako seed u mobilních peněženek, tzn. při poškození, či ztrátě Trezoru jsem schopna pomocí seed obnovit privátní klíč a tím celou historii transakcí z blockchainu. Trezor je chráněn taky PINem, bez kterého nejde odeslat transakci. PIN je zadáván na speciální numerické klávesnici, Trezor ukazuje devět čísel, na obrazovce PC se mezitím ukazuje mřížka s devíti otazníky. Postavení čísel na displeji Trezoru se pokaždé náhodně mění a na počítači je třeba je zadávat pohybem kurzoru na monitoru namísto otazníků – opět výborná ochrana proti keyloggeru. (Fillner, 2014) Vyzkoušela jsem i tuto hardwarovou peněženku, jde opravdu o nejbezpečnější variantu, někteří lidé vlastní i více trezorů.



Obr. 14 Bitcoin Trezor
Zdroj: satoshilabs.com, 2016

6.2.7 Závěr kapitoly

V této kapitole jsou shrnuty možnosti uchovávání bitcoinů v bitcoin peněženkách. Po osobním vyzkoušení doporučuji pro běžného uživatele si nainstalovat odlehčenou softwarovou peněženku typu MultiBit do počítače, která není tak náročná na

⁶ Keylogger je útočný program, který zaznamenává činnost klávesnice.

paměť jako Bitcoin Core, protože nestahuje celý Blockchain, ale jen hlavičky transakcí. U Bitcoin Core jsem nechala stahovat Blockchain přes 12 hod., i tak nebyla stažená ani půlka. Blockchain má v době psaní této práce velikost 50 GB, která bude růst čím dál rychleji dle exponenciální křivky. Výhoda MultiBitu je také uživatelské rozhraní v češtině a celková přehlednost pro uživatele. Papírová peněženka je podle mě nutná vždy k jakékoli peněžence, je bezpečná, protože je offline, ideálně jich mít víc na různých místech. Její nevýhodou je životnost papíru a inkoustu při špatném skladování, doporučuje se uschovat ve folii v sejfu proti požáru.

V běžném životě ocení uživatel mobilní peněženku, jedná se o aplikaci v telefonu, díky které můžeme platit bitcoiny např. v kavárnách, restauracích velmi rychle a jednoduše načtením QR kódu obchodníka a potvrzením transakce. Online peněženky patří k nejpoužívanějším peněženkám pro jejich snadné používání, dostupnost, rychlost registrace. Nemusíme řešit zabezpečení, což je sice pohodlné, na druhou stranu má poskytovatel služby přístup ke všem našim bitcoinům, je tedy nutná důvěra v třetí stranu, ačkoli poskytovatel nemusí mít nekalé úmysly, bývá často terčem útoků hackerů, viz kapitola 5.6 *Vývoj Bitcoinu*. Pokud však uživatel trvá na online peněžence, pak se doporučuje na ní mít jen malý obnos a vybrat si důvěryhodnou platformu, jako je např. Coinbase, která 98 % bitcoinů uchovává offline. Pro větší majetek v bitcoinech doporučuji hardwarovou peněženku, která je ze všech peněženek úplně nejbezpečnější, v této práci jsem se zaměřila konkrétně na český produkt Trezor. Je ochráněn před viry díky tomu, že se jedná o samostatnou počítačovou jednotku s jednosměrným zadáváním z Trezoru do počítače (naopak to nejde), PIN se zadává kurzorem myši na speciální klávesnici na obrazovce, která pokaždé náhodně mění postavení čísel – ochrana před keyloggerem. V neposlední řadě je vysoce bezpečné potvrzování transakcí mechanickým způsobem (stisknutím tlačítka na Trezoru), což hacker není schopen udělat.

6.3 Jak získat bitcoiny

V současnosti máme i v České republice poměrně široké možnosti jak zakoupit či prodat bitcoiny. Cílem kapitoly je porovnat jednotlivé možnosti získání bitcoinů a doporučit nejvýhodnější variantu dle požadavků běžného uživatele.

6.3.1 Mining

Co je mining jsme si již vysvětlili v kapitole 5.3.4 *Mining*. Dříve se bitcoiny těžily pomocí procesoru počítače (CPU), později se k těžbě využívaly grafické karty (GPU). V současnosti se těžba vyplatí provádět jedině pomocí specializovaných zařízení, tzv. ASIC jednotek. ASIC (Application Specific Integrated Circuit neboli integrovaný obvod pro zvláštní využití) je momentálně nejvýkonnější zařízení a zároveň spotřebuje nejméně elektrické energie při těžbě. (Vítek, 2012)

V roce 2010 přišel český programátor Marek Palatinus alias Slush na koncept těžení v poolu, jedná se o seskupení těžařů, kteří společně těží bitcoiny a při nalezení bloku si mezi sebou odměnu včetně transakčních poplatků od uživatelů rozdě-

lí poměrně k výpočetnímu výkonu, který každý poskytl. Slush's pool si nárokuje 2 % z vytěžených bitcoinů a transakčních poplatků.

V dnešní době při tak velkém výkonu počítačové sítě se těžít vyplatí pouze velkým investorům, kteří mají velmi nízké náklady na elektřinu, jelikož mívají vazbu přímo na výrobce elektřiny a platí za elektřinu i částky kolem 0,80 Kč/kWh, v tomto případě se to vyplatí i s obrovskými náklady na ASIC zařízení.

6.3.2 Bitcoin směnárny

V současnosti funguje na českém trhu několik online směnáren, které se liší zejména kurzem. Některé nabízejí výhodnější výkupní kurz a prodávají velmi drah (např. Coin Hub), jiné zase prodávají relativně za dobrou cenu, výkup bitcoinu už ale příliš výhodný není. „... Světlou výjimkou mezi českými projekty je online bitcoinová směnárna SimpleCoin.cz, která nabízí vysoce konkurenční kurz bitcoinu a zároveň je nákup a prodej velmi jednoduchý a rychlý. Směnárna funguje zpravidla od rána do pozdních večerních hodin včetně víkendů a poskytuje služby od listopadu 2013.“ (Laciga, 2015) Mezi českými směnárnami jsou poměrně velké rozdíly, které se projevují v jejich okamžité likviditě, rychlosti vyřízení obchodu a přístupu k AML/KYC procedurám (Anti Money Laundering (= zákon proti praní špinavých peněz)/Know your customer (= poznej svého zákazníka). Výhodami nákupu a prodeje bitcoinů prostřednictvím online směnáren jsou jednoduchost a pohodlnost nákupu, žádné poplatky, bitcoiny i peníze jsou po vyřízení obchodu ihned k dispozici, nákup přímo v Kč, tedy žádné kurzové rozdíly. Nevýhodou je větší rozpětí mezi nákupní a prodejní cenou (= spread) oproti online burzám. V tab. 2 jsou uvedeny aktuální kurzy směnáren v ČR k 18. 12. 2015 23:35.

Tab. 2 Kurzy BTC směnáren v ČR k 18. 12. 2015 23:35

Směnárna	Výkupní cena [Kč]	Prodejní cena [Kč]	Spread [Kč]
Coin Hub	10 602	12 323	1 721
First Bitcoin	11 206	11 943	737
Simple Coin	11 051	11 984	933
Rubi Coin	10850	11 882	1032

Zdroj: coinhub.cz, firstbitcoin.cz, simplecoin.cz, rubicoins.cz, 2015

Vybrala jsem si směnárnu Rubi Coin, protože prodává bitcoiny za aktuálně nejlepší cenu z uvedených směnáren, vzhledem k tomu, že je nechci prodat zpět, tak jsem neřešila spread. Vyplnila jsem formulář, kde jsem vyplnila počet bitcoinů, svůj e-mail a bitcoin adresu. Pro zaslání SMS o vyřízení můžete vyplnit i telefonní číslo, toto pole je nepovinné, já jsem ho však vyplnila. Koupila jsem 0,025 BTC (25mBTC)

za 299 Kč. Poté jsem potvrdila formulář tlačítkem „koupit“ a téměř okamžitě mě došel e-mail o potvrzení objednávky s platebními instrukcemi. Rubi Coin vlastní 4 korunové bankovní účty a 2 cizoměnové (pro eura a dolary). Pro převod se volí vždy účet vedený u stejné banky, jako je bankovní účet, ze kterého budu platbu realizovat. Pokud budu převádět peníze z jiné banky, zvolím primární účet pro danou měnu (např. zde je pro koruny primární účet vedený u Fio banky). Zvolila jsem účet vedený u stejné banky (KB) a platbu potvrdila přes internetové bankovníctví v 23:50. Následující den jsem v 7:55 obdržela e-mail od Rubi Coin, ve kterém bylo potvrzeno přijetí mé platby s dovětkem, že objednávku vyřídí během chvíle. V 8:06 mi došla SMS s oznámením, že je má objednávka vyřízena, v 8:10 byla potvrzena transakce a bitcoiny připsány na mou mobilní peněženku v Myceliu. V podrobnostech můžu vidět ID transakce, počet potvrzení (k 19. 12. 2015 13:03 se jedná o 27 potvrzení), číslo bloku, ve kterém byla potvrzena transakce, vstupy, výstupy z adresy směnárny a poplatek sítě 0.08456 mBTC. Nákup proběhl opravdu jednoduše a rychle, je to otázka pár minut. Na Blockchain.info se dá vyhledat jakákoli transakce, adresa, hash, atd. Na obr. 15 je výsledek po zadání mé bitcoin adresy.

Bitcoin Address Addresses are identifiers which you use to send bitcoins to another person.

Summary		Transactions	
Address	1DFTT2qtUAP56c3b2dfz6DCZqEHdhPAGJQ	No. Transactions	1
Hash 160	865d6946cc35c20f4bb560808132c7496f10de80	Total Received	0.025 BTC
Tools	Taint Analysis - Related Tags - Unspent Outputs	Final Balance	0.025 BTC

Request Payment Donation Button

Transactions (Oldest First) Filter

Transaction ID	Amount	Time
25b5b2458be932299812282945d74f09e4d60cace5bb8ab6403f3f4e1d3b072	0.025 BTC	2015-12-19 07:05:52
3EkDAHyoqeYQWIBuzodUSJQE2TU7q9AAbf	0.025 BTC	

29 Confirmations 0.025 BTC

Obr. 15 Nákup bitcoinů
Zdroj: blockchain.info, 2015

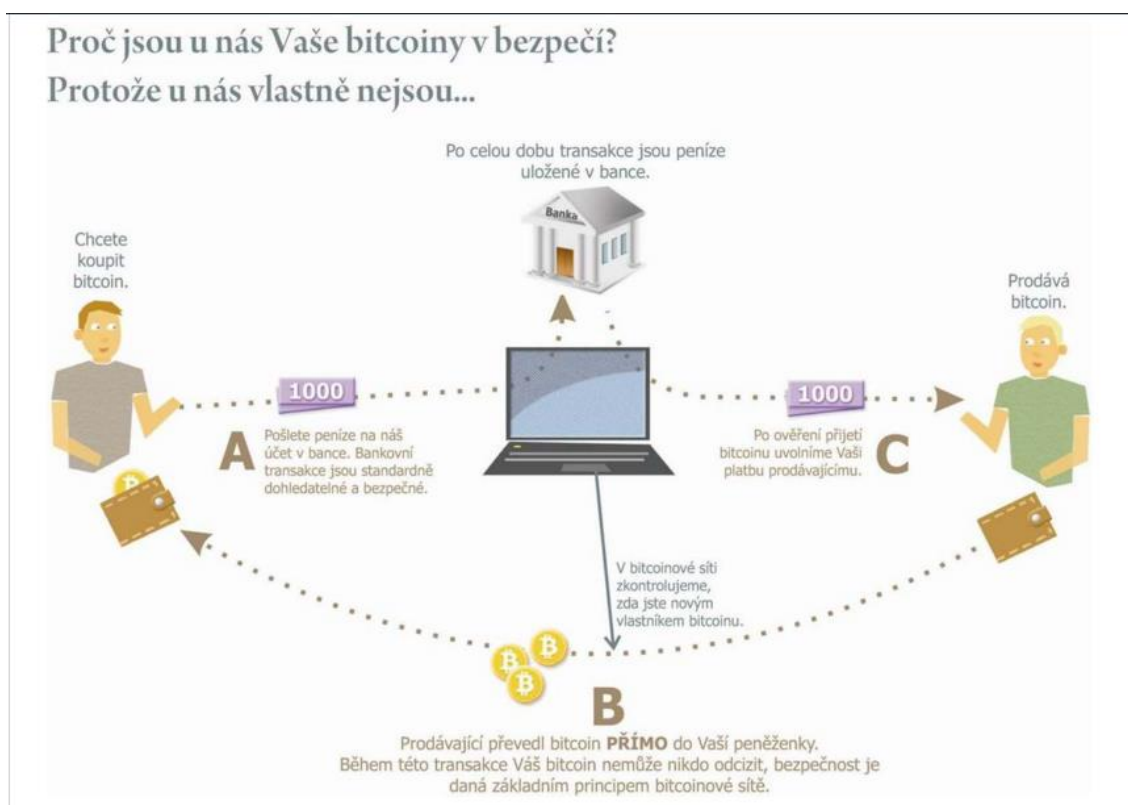
6.3.3 Bitcoin burzy

Rozdíl mezi burzou a směnárnou je zjednodušeně řečeno to, že směnárna nabízí vlastní pevný kurz, kdežto na burze se párují nabídky a poptávky uživatelů, a podle toho se vytváří aktuální tržní cena.

V České republice působí v současné době jediná burza BitStock, která na rozdíl od ostatních burz nadržuje bitcoiny, jak znázorňuje obr. 16. Ani to však nezaručí 100 % bezpečnost, protože hacker může napadnout převod např. v e-mailu, kdy si myslíte, že posíláte bitcoiny tam, kam máte, přitom ale prostředky posíláte na adresu útočníka. Výhodou obchodování na BitStocku oproti zahraničním burzám je možnost obchodovat za české koruny. Nevýhodou je, že se jedná o poměrně

malý trh. V porovnání se zahraničními burzami má BitStock o něco vyšší poplatek, ve výši 0,5 % z každého obchodu (např. burza BitStamp si účtuje poplatek 0,25 %). Poplatek se snižuje se zvyšujícím se objemem transakcí. Při prodeji je nutné složit nejdříve zálohu ve výši 1000 Kč/1 BTC, to znamená, že pokud bude chtít prodejce prodat např. 0,1 BTC, pak se na jeho burzovním účtu zablokuje částka 100 Kč. Po uzavření obchodu a zaslání bitcoinů je celá částka opět uvolněna a prodávající s ní může bez omezení dále manipulovat. Pokud nedojde po uzavření obchodu k zaslání bitcoinů, je 70 % ze zálohy připsáno na burzovní účet kupujícího a 30 % propadá burze jako administrativní poplatek. V případě neobdržení bitcoinů tedy kupující nejen že prodávajícímu nic nezaplatí, ale naopak dokonce obdrží finanční odškodnění. (bitstock.com, 2015)

Při registraci vyžaduje kromě e-mailu i telefonní číslo na zaslání tokenu. Ověření identity je nutné až při obchodování nad obrat 25 000 Kč. Pro vložení finančních prostředků je třeba mít zaregistrovaný alespoň jeden bankovní účet, přičemž musím být majitelem tohoto účtu.



Obr. 16 Burza BitStock
Zdroj: bitstock.com, 2015

Mezi nejznámější a nejstarší burzy patří britská burza Bitstamp, která má sídlo na Slovinsku a i když měla v minulosti velký bezpečnostní problém (v důsledku hackerského útoku přišla o 19 000 BTC), problémy ustála a je považována za spolehlivou. V březnu 2014 poprvé prošla auditem na 100 %. Na Bitstampu se

zaslané prostředky v eurech konvertují na dolary a za depozit není účtován žádný poplatek.

U zahraničních burz je pro českého uživatele nevýhoda, že bývají v EUR nebo USD. Doporučuje se mít účet v eurech nebo dolarech, protože SEPA/SWIFT platby stojí další poplatky, na které se podrobněji podíváme v kapitole 6.5 *Převod finančních prostředků*. Laciga (2015) doporučuje burzu Kraken zkušenějším obchodníkům, kteří se umí na burzách pohybovat a využijí pokročilejší burzovní příkazy známé z tradičních trhů. Poplatek z objemu obchodu na burze Kraken je 0,35 % a s vyšším objemem obchodů se snižuje. Nejzkušenější obchodníci v poslední době používají zejména čínské burzy, nejen kvůli nízkým poplatkům, ale i kvůli velkému objemu obchodů. Největšími burzami podle objemu obchodů jsou v současnosti OKCoin, BTCChina a Huobi. Na bitcoinwisdom.com můžete sledovat vývoj ceny bitcoinu na největších burzách.

6.3.4 Bitcoinmaty

Bitcoinmat je skvělý způsob, jak okamžitě získat bitcoiny. V České republice je aktuálně do 10 automatů, z toho je 5 v Praze a po jednom v Brně, v Ostravě a v Plzni. Můžou být jednosměrné (koupím bitcoiny) i obousměrné (koupím i prodám bitcoiny).

Vyzkoušela jsem obousměrný automat od GeneralBytes, což je česká firma. GeneralBytes na rozdíl od Robocoinu, který zprostředkovává WBTCB např. v Brně ve Vaňkovce, nevyžaduje osobní údaje a má nižší poplatek. Kurz se počítá od kurzu na burze BitStamp + 3 %, Robocoin + cca 7 %. Při koupi bitcoinů stačí zadat „koupit bitcoiny“, naskenovat QR kód své peněženky, pokud ještě žádnou peněženku nemám, tak si můžu vygenerovat novou peněženku na malém přístroji, kdy mě vyjde něco jako účtenka s oběma klíči (papírová peněženka), vložím hotovost, okamžitě jsem viděla bitcoiny na své mobilní peněžence, i když ještě nepotvrzené. U prodeje bitcoinů si zvolím „prodat bitcoiny“, cenu v korunách a vyjde mi účtenka s adresou, kde mám zaslat bitcoiny. Tato účtenka má platnost asi 30 min, po cca 10 minutách, kdy se potvrdí transakce v blockchainu, si oskenuju účtenku a automat mi vydá hotovost.

6.3.5 Localbitcoins

Jednou ze zajímavějších služeb pro občany České republiky je LocalBitcoins.com, která sdružuje jednotlivce, kteří chtějí nakupovat či prodávat bitcoiny, a dělí je podle lokace. Uživatelé tak mohou snadno najít prodejce ve svém městě a domluvit se s ním na platbě. LocalBitcoins si za zprostředkování obchodu účtuje 1 % z transakce. Výhody této služby jsou jednoznačné, uživatelé mohou snadno a rychle zaplatit v lokální měně, platebními prostředky obvyklými pro danou oblast, dokonce i platba v hotovosti je možná. Mezi nevýhody patří oproti směnárnám velice malý trh, kde je menší množství nabídek a s tím spojené problémy. Jsou zde přítomny nástroje na hodnocení jednotlivých uživatelů, takže v případě nákupu od renomovaného obchodníka s řadou pozitivních hodnocení je šance podvodu mini-

mální. (Huřák, 2013) Služba funguje tak, že poptávající zaplatí nabízejícímu korunu, či jinou měnu za dohodnutou částku za bitcoiny, v hotovosti, či na účet dle dohody, po jeho potvrzení přijetí platby pošle Localbitcoins poptávajícímu bitcoiny, které jim zaslal nabízející. Funguje to jako u klasických burz.

6.3.6 Vlastní služby

Celosvětově je nyní více než 100 000 akceptačních míst, tedy prodejen, podniků a služeb, kde je bitcoin přijímán jako platební metoda. V České republice jsme zatím přibližně na počtu 100, čísla však stále rostou. Platba je velmi jednoduchá a v menší kamenné prodejně pro ni stačí jednoduchá aplikace v mobilu. Zákazník načte QR kód, který se vygeneruje po zadání požadované částky – dá se to přirovnat k čárovému kódu, nebo bezkontaktní platební kartě. Větším prodejnám, nebo eshopům se vyplatí spíše implementace řešení platební brány – například americké BitPay. Platby, které se načtou od zákazníka, jsou instantně převedeny do lokální měny a odpadá tak obava z vysoké volatility a kurzových rozdílů. U menších on-line prodejnách stačí příjmová bitcoin adresa, na kterou zákazník pošle platbu a po ověření v blockchainu odesíláte zboží, nebo poskytnete službu. (Fillner, 2014)

6.3.7 Závěr kapitoly

V této kapitole jsem shrnula možnosti získání bitcoinů v České republice. Pro jednotlivce se dnes už nevyplatí těžit bitcoiny kvůli vysokým nákladům na elektrinu. V ČR existuje několik BTC směnárén, kde je možno koupit či prodat bitcoiny. Rozdíl mezi směnárnou a burzou je takový, že směnárna nabízí svůj vlastní fixní kurz, kdežto na burze je kurz v tržní ceně. Výhodou směnárén je jednoduchost a rychlost obchodování, nevýhodou je velký spread mezi výkupní a prodejní cenou. V dnešní době existuje pouze jedna česká burza BitStock. Výhodou je obchodování v českých korunách, a tudíž nemusím řešit SEPA převody, jako u zahraničních burz, i když tam jsou nižší poplatky. Nevýhodou je nevýhodná cena oproti zahraničním burzám právě kvůli malému trhu. Další možností získání bitcoinů je služba LocalBitcoins.com, která shromažďuje uživatele, kteří chtějí nakupovat či prodávat bitcoiny a dělí je podle lokace, funguje jako klasická burza. Výhodou je opět lokální měna a výběr metody platby i v hotovosti, nevýhodou je velmi malý trh. Další možností získání bitcoinů je Bitcoinmat (něco jako bankomat), který je taktéž velmi jednoduchý a rychlý, fungují i obousměrné, to znamená, že krom nákupu bitcoinů můžu v bitcoinmatu i prodat bitcoiny za koruny. Nevýhodou je, že těchto automatů je v ČR jen pár, z toho většina je v Praze, a po jednom v Brně, Ostravě a Plzni. Další možností je za své zboží či služby akceptovat bitcoiny.

Pokud potřebuje uživatel bitcoiny co nejrychleji, doporučuji bitcoinmat. Pokud se uživatel nenachází v jednom z uvedených měst, kde se bitcoinmat nalézají nebo jednoduše by si raději bitcoiny nakoupil v pohodlí domova, pak doporučuji jednu ze směnárén, při vedení účtu u stejné banky, jako má směnárna, může získat

bitcoiny téměř okamžitě. Pokud chce nakoupit bitcoiny nejlevněji, pak doporučuji BTC burzu nebo LocalBitcoins.

6.4 Možnosti využití bitcoinů

V této kapitole provedu online nákup za bitcoiny. Dále porovnáím ceny vybraných produktů v BTC na pár příkladech e-shopů s cenami vybraných produktů na ostatních e-shopech v Kč a zjistím, zda se vyplatí platit bitcoiny. Poté porovnáím Bitcoin z hlediska zahraničních odchozích plateb, co se týče nákladovosti a rychlosti se zástupci českých velkých, středních a malých bank, Western Union a službou cash2vn.

6.4.1 Nákup za bitcoiny na e-shopech

Na stránkách mises.cz jsem si objednala knížku *Bitcoin: Peníze budoucnosti*. Knížka stála k 19. 12. 2015 160 Kč (cca 0,017 BTC). Poté mě došel e-mail s žádostí o poslání 0,024 BTC na adresu 1FYZkXvjMBp2UTGUqyrFqHaboqVyomLe1A. Následně jsem na své peněženice na Myceliu klikla na tlačítko „odeslat“, zadala jsem zmíněnou adresu, částku ve vybrané měně a poplatek sítě, kde si můžu zvolit z možností: nízká priorita, ekonomický (u těchto dvou se objeví „potvrzení může chvíli trvat“), běžný a prioritní (zvolila jsem běžný, automaticky se mi nastavilo 0,04371 mBTC), zadala jsem heslo, dala příkaz „odeslat“ a do pár minut byla transakce potvrzena. Platbu jsem odeslala 17:38 a k 19:04 byla transakce 8x potvrzena, opravdu se blok nachází průměrně zhruba jednou za 10 minut. Zajímavé je, že se můžu přímo v Myceliu podívat na ID transakce, vstup či výstupy transakce na Blockchainu.

Zde je pár příkladů e-shopů v ČR, kde akceptují bitcoin: ibit.cz (PC komponenty), g-hosting.cz (webhosting), kleckashop.cz (rostlinná hnojiva a různé pěstební systémy), silver.ag (stříbrné i zlaté a diamantové šperky), gourmetkava.cz (zrnková pražená káva), lukashladecek.cz (weby, grafika, online marketing), golfplanet.cz (cestovní kancelář), gekonis.cz (hosting, prodej hardware a software), pretiko.cz (reklamní tisk a výroba), pams.eu (nášivky), izlato24.cz (šperky, hodinky), odeli.cz (přírodní kosmetika), subreg.cz (domény), msficek.cz (mateřská škola), krtkovo.eu (webdesign, grafika), webstep.net (správa sítě, instalace a správa serverů, apod.). Celosvětový přehled míst, kde akceptují bitcoin, byť neúplný, zobrazuje interaktivní mapa coinmap.org, jejíž tvůrcem je česká firma SatoshiLabs.

Výzkumná otázka č. 1: Vyplatí se na českých e-shopech platba za bitcoiny?

Produkt *Microsoft XBOX 360 4GB* nabízí kromě e-shopu iBit.cz dalších 23 e-shopů na Heuréce s průměrnou cenou včetně dopravy 4795,54 Kč. iBit.cz ho nabízí za 4802 Kč (0,045686 BTC), u svých produktů má dané fixní ceny v BTC, nepoužívá BitPay jako ostatní testované e-shopy akceptující Bitcoin. Bitcoiny koupím na LocalBitcoins (LB) za nejlepší cenu 11665,83 Kč od uživatele Kucci, tento kurz budu používat i u dalších produktů, na koupi 0,045686 budu tedy potřebovat

5329,42 Kč. Už teď se mi nákup prodraží o 10,98 %, oproti ostatním e-shopům je to o 11,13 %. Není však pravidlem, že zvolením platby bitcoiny se nákup musí vždy prodražit. Pokud má firma platební portál BitPay (něco jako PayPal, ale v BTC), může být pro zákazníka i lepší zaplatit produkt bitcoiny. Na následující tab. 3 si ukážeme na 4 příkladech, o kolik % se platby bitcoiny prodraží. Za X považuji vybraný e-shop akceptující Bitcoin (iBit.cz, gourmetkava.cz, g-hosting.cz a subreg.cz). Za Y považuji ostatní e-shopy nabízející stejný produkt (vybranými produkty jsou: herní konzole Microsoft XBOX 360 4GB, termoska 0,5l zn. Renberg a registrace domény CZ).

Tab. 3 Srovnání cen e-shopů

<i>Produkt</i>	<i>Cena X [CZK]</i>	<i>Cena X [BTC]</i>	<i>Nákup BTC na LB [CZK] (1)</i>	<i>Prům. cena Y [CZK](2)</i>	<i>Rozdíl (1)-(2)</i>
iBit.cz					
Konzole	4 802	0,45684	5 329,42	4 785,54	11,13%
gourmetkava.cz					
Termoska	284	0,02178	254,09	307,8	-17,45%
g-hosting.cz					
CZ doména	242	0,02158	251,71	179,01	40,61%
subreg.cz					
CZ doména	175	0,01563	182,49	184,56	-0,01%

Zdroj: iBit.cz, gourmetkava.cz, g-hosting.cz, subreg.cz, heureka.cz, 2015

6.4.2 Závěr kapitoly

Při srovnání cen vybraných 4 produktů v BTC s jejich cenami v Kč na ostatních e-shopech v ČR jsem zjistila, že nemusí být pravidlem, že se nákup za bitcoiny musí vždy prodražit. V některých případech se to může vyplatit i s náklady za prvotní nákup bitcoinů. Nákup přes platební portál BitPay vyšel velmi výhodně.

6.5 Převod finančních prostředků

V této kapitole se zaměřím na zahraniční platební styk, kde porovnám jednotlivé možnosti převodů finančních prostředků nejen v rámci Evropy, ale hlavně do Asie,

konkrétně do Vietnamu. Porovnám banky, cash2vn, Western Union a Bitcoin skrz náklady i rychlost.

Výzkumná otázka č. 2: Jak vychází Bitcoin jako nástroj zahraničního platebního styku?

6.5.1 Banky

Odchozí platby do zahraničí v EHP

Československá obchodní banka (2015) definuje SEPA převod⁷ jako převod, který splňuje následující podmínky:

- převody v EUR,
- převody do/z členských států EU/EHP a Švýcarska,
- převod částky v plné výši bez jakýchkoli srážek poplatků,
- IBAN formát čísla účtu plátce/příjemce,
- BIC formát banky plátce/příjemce,
- kód zpoplatnění SHA (příkazce i příjemce hradí poplatky své banky),
- žádné specifické instrukce či dodatečné informace pro banku.

U SEPA převodů v rámci EHP je povinné uvedení banky příjemce ve formátu BIC a čísla účtu příjemce ve formátu IBAN. Zprostředkující banky ve členských státech EHP jsou oprávněny odmítnout či vrátit platbu v případě neuvedení BIC a IBAN (popř. při uvedení BIC a IBAN v neplatném či nekorektním formátu).

V tab. 4 je přehled poplatků vybraných českých bank včetně lhůt připsání transakce příjemci. Všechny údaje jsou aktuální k 21. 12. 2015 dle sazebníků a obchodních podmínek bank dostupné na webových stránkách bank, nebo po telefonickém kontaktu s bankéři. U více možností bez znaku + se jedná o víc variant podle typu daného produktu v určité bance (AirBank, GE, nebo Zuno). U variant se znakem + se jedná o příplatky, kdy chceme, aby příjemce obdržel platbu dřív, než je standard (ČS nebo KB). Nejsou zahrnuty poplatky navíc při podávání žádostí na pobočkách bank.

Banky jsou seřazeny dle velikosti, žlutou barvou jsou malé nízkonákladové banky (od 50 mld. Kč), modrou barvou jsou střední banky (od 50 mld. Kč do 100 mld. Kč) a zelenou barvou velké banky (nad 100 mld. Kč). Z každého okruhu jsem vybrala 4 zástupce, velikost poplatků i lhůty zpracování transakcí jsou dost podobné v každém z nich. Malé banky nabízejí nejnižší poplatky na úkor delšího trvání vyřízení transakcí (až třetí den po splatnosti), výjimkou je Fio banka, kde je poplatek pouhých 20 Kč při stejné rychlosti jako u ostatních bank. Průměrná doba připsání platby příjemci je následující pracovní den po dnu splatnosti. U velkých bank jako je ČS nebo KB je možnost příplatku ke standardnímu poplatku, když potřebujeme, aby obdržel příjemce peníze co nejdřív.

⁷ SEPA = Single Euro Payments Area (jednotná oblast pro platby v eurech). Zahrnuje členské státy EHP (Evropského hospodářského prostoru), tj. 27 států EU (Evropské unie) + Norsko, Island, Lichtenštejnsko a Švýcarsko.

Většina bank nabízí i vedení účtu v cizí měně, poplatky by nám však zůstaly, protože by se stále jednalo o zahraniční platbu, urychlilo by to ale europlatby, pokud bychom měli účet vedený v EUR. Všechny malé banky krom mBank, která jako jediná banka v ČR nenabízí vedení účtu v cizí měně, tzn. AirBank, Fio Bank i Equa Bank mají vedení účtu v cizí měně zcela zdarma. U středních bank je vhodné si založit spořicí účet v EUR, který je vedený zdarma u všech krom CitiBank, kde je buď zdarma nebo za poplatek 169 Kč/měs. za vedení balíčku služeb Citikonto Plus v případě celkového průměrného zůstatku pod 250 000 Kč nebo v případě, že součet příchozích plateb v daném měsíci nepřesáhne 25 000 Kč. U velkých bank vychází nejlíp UniCredit Bank, protože nabízí tuto službu zdarma, poté Česká spořitelna za poplatek 20 Kč/měs., Komerční banka za poplatek 19-69 Kč/měs. a ČSOB nabízí vedení účtu v cizí měně pouze podnikatelům.

Tab. 4 Poplatky vybraných českých bank za odchozí SEPA platbu

<i>Banka</i>	<i>Poplatek do 50 000 EUR v rozsahu <min;max>[Kč]</i>	<i>Průměrný poplatek [Kč]</i>	<i>Poplatek od 50 000 EUR v rozsahu <min;max>[Kč]</i>	<i>Průměrný poplatek v rozsahu <min;max> [Kč]</i>	<i>Připsání platby na účet příjemce. D+0 = datum splatnosti</i>
mBank	zdarma	36	0,5%, <250;840>	<96;246>	D+3
Air Bank	0/25		0/25		D+3
Fio Bank	20		20		D+1
Equa Bank	99		99		D+1
GE Money Bank	45/75/220	231	1%, <100;1000>	<325;963>	D+1
Sberbank	250		250		D+2
ExpoBank	0,9%, <350;2000>		0,9%, <350;2000>		D+2
CitiBank	250		600		D+1
Česká spořitelna	220/+500/+750	229	1%, <220;1500>	<555;1313>	D+1/D+0/do 4 hod
ČSOB	250		0,7%, <250;750>		D+1
Komerční banka	195/+600		1500/+600		D+1/D+0
UniCredit Bank	250		0,9%, <250;1500>		D+1

Zdroj: Seznam bank a jejich poplatků, 2015

Odchozí platby v rámci zahraničí mimo EHP

V tab. 5 je přehled zástupců českých bank z každé kategorie v rámci SWIFT⁸ odchozích plateb do zahraničí mimo Evropu a výše jejich poplatků a lhůt pro připsání platby na účet banky příjemce. Zde opět platí, že malé banky konkurují nižšími poplatky ovšem na úkor rychlosti připsání na účet příjemci. Střední banky vyjdou v této kategorii nejdráž, velké banky mají nejnižší průměrný minimální poplatek. Průměrná výše poplatku se pohybuje okolo 1 % z odesílané částky, min. zhruba 243 Kč, max. 1500 Kč. U některých bank záleží u výše poplatku také na typ převodu, zda se jedná o SHA, BEN nebo OUR. SHA ("shared") = Plátce hradí poplatky své bance a příjemce poplatky bance své, popř. zprostředkujícím bankám. BEN ("beneficiary") = Poplatky související s mezinárodní platbou hradí příjemce platby, včetně poplatků účtovaných bankou plátce. OUR ("our") = Veškeré poplatky spojené se zahraniční platbou bude hradit plátce (včetně poplatků banky příjemce, případně i zprostředkujících bank).

⁸ SWIFT (Society for Worldwide Interbank Financial Telecommunication – Společnost pro celosvětovou mezibankovní finanční komunikaci) slouží zejména k mezinárodnímu platebnímu styku. V rámci SWIFTu má každá zúčastněná banka svůj jedinečný kód (BIC), kterým se identifikuje.

Tab. 5 Poplatky vybraných českých bank za odchozí SWIFT platbu

<i>Banka</i>	<i>Poplatek v rozsahu <min;max> [Kč]</i>	<i>Průměrný poplatek v rozsahu <min;max> [Kč]</i>	<i>Připsání platby na účet banky příjemce. D+0=datum splatnosti</i>
mBank	0,5%, <250;840>	<287;435>	D+5
Air Bank	100		D+7
Fio Bank	200 (SHA/BEN)/ 500(OUR)		D+3
Equa Bank	299		D+4
GE Money Bank	1%, <100;1000>	0,98%, <300;1500>	D+3
Sberbank	1%, <300;1700>		D+2
Expo Bank	0,9%, <500;2200>		D+3
CitiBank	1%, <300;1100>		D+2
Česká spořitelna	1%, <220;1500>/+250/+500	0,95%, <243;1500>	D+2
ČSOB	1%, <250;1500>		D+2
Komerční banka	0,9%, <250;1500>		D+3
UniCreditBank	0,9%, <250;1500>		D+3

Zdroj: Seznam bank a jejich poplatků, 2015

Příchozí platba ze zahraničí (Vietnam)

Tab. 6 ukazuje přehled sedmi vybraných komerčních bank ve Vietnamu, u kterých se daly dohledat sazebníky pro příchozí platby ze zahraničí. Většina bank spolupracuje s Western Union. U každé banky je možnost výběru peněz na výběr minimálně z měn: USD a VND (vietnamská měna: dong), u některých i EUR, u USD a EUR je další poplatek, který jsem neuvažovala, protože by si občan zcela určitě zvolil možnost výběru hotovosti ve VND. Poplatky jsou u bank téměř totožné. U všech bank je poplatek 0,05 %, průměrný poplatek je 0,05 %, v průměru v rozmezí min. 2 USD, max. 129 USD.

Tab. 6 Poplatky za příchozí zahraniční platbu ve vietnamských bankách

<i>Banka</i>	<i>Poplatek v rozsahu <min;max>[USD]</i>
DongABank	0,05%, <2;100>
OCB	0,05%, <2;100>
VietcomBank	0,05%, <2;150>
EximBank	0,05%, <2;100>
ACB	0,05%, <2;200>
LienVietPostBank	0,05%, <2;150>
AgriBank	0,05%, <2;100>

Zdroj: Seznam bank a jejich poplatků, 2015

6.5.2 Western Union (WU)

Na stránkách InterCash, s. r. o., zástupce WU v České republice, píše: „*Western Union je největší poskytovatel služeb hotovostních převodů peněz na světě. Americká obchodní společnost vznikla v roce 1851 jako telegrafická firma. V roce 1871 byla představena služba převodů peněz a stala se hlavní činností společnosti. Firma postupně expandovala za hranice amerického kontinentu a dnes působí ve více než 200 zemích a na celém světě má více než 470 000 provozoven. Spolehlivost, rychlost a jednoduchost jsou hlavní charakteristiky Western Union Převodů peněz.*“ Western Union je známá tím, že má extrémně drahé poplatky. Zajímají nás poplatky do Vietnamu, který má s Čínou speciální ceník, viz obr. 17. Největší nevýhodou WU je kromě vysokých poplatků maximální limit k zaslání z ČR je 7400 USD (či jiný ekvivalent v ČR). 7400 USD je při aktuálním kurzu k 22. 12. 2015 0:46 cca 184 000 Kč, z toho poplatek činí 3017 Kč. Jedinou výhodou je rychlost vyřízení převodu, peníze si může příjemce vyzvednout téměř okamžitě, záleží však na pracovní době na místě určení. Příjemce žádný poplatek nehradí. Western Union vyplácí příjemci peníze vždy v USD nebo EUR nebo v lokální měně (v případě Vietnamu v USD nebo VND), přičemž převod měny je již započítán do poplatků. Maximální částka, kterou lze poslat, aby si mohl příjemce vyzvednout peníze ve VND, je 4000 USD (při aktuálním kurzu 22532 VND/USD k 22. 12. 2015 15:20 se jedná o 90 128 000 VND).

Vietnam a Čína

Částka (CZK)	Poplatek (CZK)	Částka (USD)	Poplatek (USD)
0,01 - 12 250,00	375,00	0,01 - 500,00	15,00
12 250,01 - 25 000,00	687,00	500,00 - 1 000,00	28,00
25 000,01 - 62 250,00	1 517,00	1 000,01 - 2 500,00	54,00
62 250,01 - 124 000	2 517,00	2 500,01 - 5 000,00	101,00
124 000,01 - 185 000	3 017,00	5 000,01 - 7 500,00	121,00

Poznámka:
Max. částka na zaslání činí 7 400,00 USD nebo její ekvivalent.

Obr. 17 Poplatky Western Union
Zdroj: intercash.cz, 2015

6.5.3 Bitcoin

U Bitcoinu nezáleží na částce, kterou posílám, ale na počtu a velikosti vstupů do transakce, tudíž tady neexistuje zvyšující se poplatek s rostoucí výší objemu peněz. Na obr. 18 je příklad transakce obrovské částky peněz 171 731,43 USD (při aktuálním kurzu k 22. 12. 2015 10:20 se jedná o cca 4 250 000 Kč) za poplatek 0,04 USD, což není ani 1 koruna. Poplatek je dobrovolný, i bez poplatku se transakce potvrdí, ale může to potrvát déle. Počítá se s tím, že se může výše doporučeného poplatku zvýšit v budoucnu, jelikož se těžařům snižuje odměna v nových bitcoinech. Rychlost je nesrovnatelná, do 10 min byla transakce potvrzena (sledovala jsem osobně).

Summary	Inputs and Outputs
Size: 225 (bytes)	Total Input: \$ 171,737.47
Received Time: 2015-12-22 00:30:44	Total Output: \$ 171,737.43
Lock Time: Block: 389573	Fees: \$ 0.04
Included In Blocks: 389585 (2015-12-22 00:44:24 + 14 minutes)	Estimated BTC Transacted: \$ 4,470.62
Confirmations: 48 Confirmations	Scripts: Show scripts & coinbase

Obr. 18 Transakce a poplatek sítě
Zdroj: blockchain.info, 2015

Příjemce si bitcoiny může za dongy směnit na online burze. Ve Vietnamu jsou dvě bitcoinové burzy, jejichž nabídka a poptávka k 22. 12. 2015 14:35 je v tab. 7.

Tab. 7 BTC burzy ve Vietnamu

<i>Burza</i>	<i>Výkupní cena [VND]</i>	<i>Prodejní cena [VND]</i>	<i>Spread [VND]</i>	<i>Poplatek [%]</i>
BitcoinVietNam	9 757 000	10 067 000	310 000	2,5
VBTC	10 200 000	11 100 000	900 000	1

Zdroj: bitcoinvietnam.com.vn, vbtc.vn, 2015

Další možností je služba LocalBitcoins, viz kapitola 6.3.5 *LocalBitcoins*. Pokud nechceme přijímat bitcoiny a následně je prodávat na burze z různých důvodů, např. protože to může být pro někoho příliš složité, existuje služba cash2vn, která zprostředkovává převod v bitcoinech, ale peníze vydává ve VND. Účtuje si poplatek 2 USD, nevýhodou je denní limit maximální částky odeslaných peněz, který je pouhých 1000 USD. V tab. 8 je shrnutá průměrná výše poplatků jednotlivých zástupců a rychlost převodů prostředků. Částky v USD jsem převedla dle aktuálního kurzu USD/CZK na webových stránkách ČNB k 22. 12. 2015.

Tab. 8 Průměrná výše poplatků

<i>Zástupce</i>	<i>10 tis. [Kč]</i>	<i>20 tis. [Kč]</i>	<i>50 tis. [Kč]</i>	<i>100 tis. [Kč]</i>	<i>150 tis. [Kč]</i>	<i>1 mil. [Kč]</i>	<i>Rychlost [dny]</i>
Malé banky	250	250	250	500	840	840	D+5
Střední banky	300	300	490	980	1500	1500	D+3
Velké banky	243	243	475	950	1500	1500	D+3
Western Union	375	687	1517	2517	3017	-	D+0
Cash2vn	50	50	-	-	-	-	D+0
Bitcoin	1	1	1	1	1	1	D+0

Zdroj: Seznam bank a jejich poplatků, intercash.cz, cash2vn.com, 2015

K 22. 12. 2015 14:25 mají banky aktuální devizový kurz CZK/USD, viz tab. 9.

Tab. 9 Devizový kurz CZK/USD vybraných bank

<i>Banka</i>	<i>Devizový kurz CZK/USD</i>	<i>Průměrný devizový kurz CZK/USD</i>
AirBank	25,217	25,2778
mBank	25,445	
Fio banka	25,227	
Equa Bank	25,222	
Expo Bank	25,253	25,3788
Sberbank	25,48	
GE Money Bank	25,458	
Citibank	25,324	
Česká spořitelna	25,263	25,1655
ČSOB	25,183	
Komerční banka	25,102	
UniCredit Bank	25,114	

Zdroj: Kurzovní lístek, 2015

Tab. 10 představuje srovnání českých bank, WU, cash2vn a Bitcoin z hlediska všech nákladů při převodu 10 000 Kč, přičemž jsem pro výpočty kromě výše uvedených údajů v předchozích tabulkách použila také následující kurzy podle České národní banky, Vietnamské centrální banky a burzy First Bitcoin, která nabízela nejvýhodnější kurz na českém trhu 11302,84 Kč/BTC aktuální k 23. 12. 2015 20:00. Můžeme vidět, že nejvýhodnější metodou je Bitcoin, poté WU a poté cash2vn. Banky vyšly nejdraž.

Tab. 10 Srovnání zástupců při převodu 10 000 Kč

<i>Zástupce</i>	<i>Poplatek odesílatele [Kč]</i>	<i>Prodej Kč [USD]</i>	<i>Nákup BTC [Kč]</i>	<i>Poplatek příjemce [USD]</i>	<i>Prodej BTC [VND]</i>	<i>Výstup [USD]</i>	<i>Výstup [Kč]</i>
Malé b.	250	385,71	-	2	-	383,71	9501,54
Stř. b.	300	382,21	-	2	-	380,21	9414,75
Velké b.	243	387,71	-	2	-	385,71	9551,03
WU	375	-	-	-	-	9625	9625
Cash2vn	49,52	-	0,88035	-	8589593	-	9368,45
Bitcoin	1	-	0,88464	-	9023378	-	9841,57

Zdroj: Seznam bank a jejich poplatků, intercash.cz, cash2vn.com, 2015

V tab. 11 je srovnání zaokrouhlených výstupů pro převod 10 000 Kč, 20 000 Kč, 50 000 Kč, 100 000 Kč, 150 000 Kč a 1 000 000 Kč. V závorce je uvedena vypočtená nákladovost v %. Zeleně jsou označeny nejnižší náklady, žlutě druhé nejnižší a červeně nejvyšší náklady.

Tab. 11 Komparace výstupů

	<i>Malé b.</i>	<i>Střední b.</i>	<i>Velké b.</i>	<i>Western Union</i>	<i>Cash2vn</i>	<i>Bitcoin</i>
<i>Vstup [Kč]</i>	10 000					
<i>Výstup [Kč]/[%]</i>	9 502 (4,98)	9 415 (5,85)	9 551 (4,49)	9 625 (3,75)	9 369 (6,32)	9 842 (1,58)
<i>Vstup [Kč]</i>	20 000					
<i>Výstup [Kč]/[%]</i>	19 298 (3,51)	19 172 (4,14)	19 391 (3,05)	19 313 (3,44)	18 784 (6,08)	19 684 (1,58)
<i>Vstup [Kč]</i>	50 000					
<i>Výstup [Kč]/[%]</i>	48 685 (2,63)	48 257 (3,49)	48 681 (2,64)	48 483 (3,03)	-	49 212 (1,58)
<i>Vstup [Kč]</i>	100 000					
<i>Výstup [Kč]/[%]</i>	97 421 (2,58)	97 043 (2,96)	97 880 (2,12)	98 483 (1,52)	-	98 425 (1,58)
<i>Vstup [Kč]</i>	150 000					
<i>Výstup [Kč]/[%]</i>	146 044 (2,64)	144 819 (3,45)	146 046 (2,64)	146 983 (2,01)	-	147 637 (1,58)
<i>Vstup [Kč]</i>	1 000 000					
<i>Výstup [Kč]/[%]</i>	978 284 (2,17)	973 748 (2,63)	981 999 (1,8)	-	-	984 255 (1,58)

Zdroj: Zdroj: Seznam bank a jejich poplatků, intercash.cz, cash2vn.com, 2015

Podle výsledků vyšel Bitcoin téměř při každé částce nejlevněji (jediná výjimka je u částky 100 000 Kč, kdy vychází nejlépe Western Union, jedná se však pouze o rozdíl 0,06 %). Cash2vn se vůbec nevyplatí jednak nákladově, jednak omezeným denním limitem. Pokud bych nepočítala službu cash2vn, tak střední banky vycházejí nejdráž. Odpovědí na výzkumnou otázku tedy je: Bitcoin vychází nejlevněji i se všemi náklady. Co se týče rychlosti, nejrychlejší je Western Union v rádech minut, po něm hned následuje Bitcoin. Celkově vychází Bitcoin nejlépe.

6.5.4 Závěr kapitoly

V této kapitole jsem porovnala české banky, Western Union, cash2vn a Bitcoin v rámci převodu finančních prostředků z České republiky do Vietnamu, kde jsem porovnala nákladovost a rychlost daných služeb. Nejlevněji vyšel Bitcoin s nákladovostí 1,58 % u libovolné transakce od 10 000 Kč až 1 000 000 Kč. U bank a Western Union se poplatky snižují se zvětšujícím objemem prostředků. Služba cash2vn se nevyplatí vůbec s nákladovostí okolo 6 %. Co se týče rychlosti, tak u bank se peníze převedou zhruba do 3-4 dnů, u Western Union je to v rámci minut, u Bitcoinu taktéž. Bitcoin je dle vypočítaných výsledků nejlepší nástroj, s rychlostí je porovnatelný s Western Union. WU je ale na druhou stranu pohodlnější cesta pro příjemce, jelikož si příjemce může na místě vyzvednout peníze ve VND, kdežto u Bitcoinu musí přijaté bitcoiny ještě směnit na burze nebo LocalBitcoins.

7 Bitcoin jako investiční nástroj

V této kapitole porovnám investici do zlata a do bitcoinu v období mezi 2010-2015. Bitcoin sice vznikl už v roce 2009, do roku 2010 však neměl bitcoin skoro žádnou hodnotu, proto začíná sledované období až po roce 2010. Investice porovnám na základě roční průměrné výnosnosti a rizikovosti investice a Sharpeho poměru. Dále se zaměřím okrajově na volatilitu bitcoinu a zlata, a také korelaci bitcoinu se zlatem. Cílem této kapitoly je formulovat doporučení pro potenciálního investora do bitcoinu.

7.1 Zlato a bitcoin

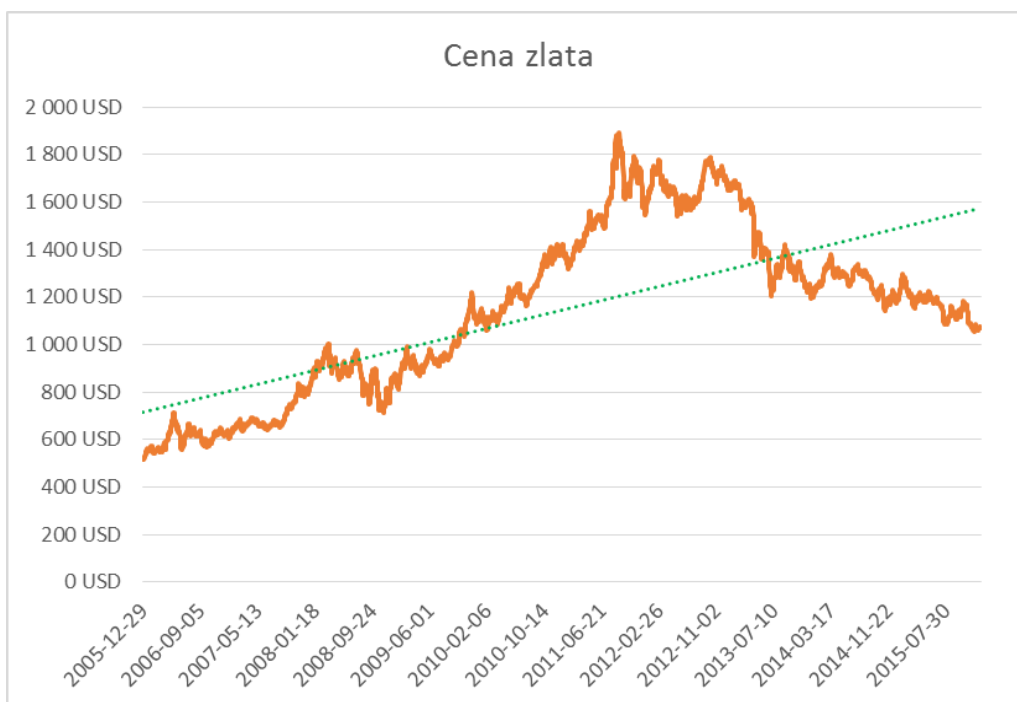
Vybrala jsem zlato pro porovnání, protože má hodně podobných vlastností jako bitcoin. V obou případech se jedná o aktivum, které není možné „tisknout“ ani jinak znásobit na účtech. Obě komodity jsou vzácné, existují v omezeném množství a jsou nezávislé na vlivu vlád. Na základě studií se ukázalo, že zásoby zlata každoročně rostou o přibližně 1,8 %. Toto číslo se víceméně shoduje s celkovým růstem světové populace a tvorbou bohatství a ukazuje na to, že síla zlata je konzistentní přes dlouhé období. Bitcoin je založený na podobném principu, až na to, že se místo podzemní těžby těží na základě matematických vzorců. Dalším společným znakem je, že se zlatem i bitcoiny dá platit. Bitcoin ani zlato nereaguje na inflaci a z tohoto hlediska se dá i bitcoin považovat za uchovatele hodnoty.



Obr. 19 Vývoj ceny zlata a bitcoinu v USD za posledních 5 let
Zdroj: vlastní zpracování podle dat z investexcel.net, a blockchain.info, 2015

Na obr. 20 je znázorněn vývoj ceny zlata za posledních 10 let. Všimněme si dlouhodobě rostoucího trendu zlata znázorněný zelenou přerušovanou čarou, i když

právě v pozorovaném období od roku 2010 cena zlata mírně klesá. K 1. 9. 2010 má unce zlata hodnotu 1245,36 USD, k 1. 9. 2015 je jeho tržní cena 1140,32 USD. Další zajímavostí je, že zatímco rok 2013 byl pro zlato v té době nejhorším rokem od roku 1997, tak pro bitcoin to byl nejlepší rok doposud, kdy tržní cena jednoho bitcoinu dosáhla hodnoty 1 151 USD, čímž se téměř přiblížil ceně zlata, viz obr. 19.



Obr. 20 Vývoj ceny zlata v USD za unci za posledních 10 let
Zdroj: vlastní zpracování podle dat z investexcel.net

7.2 Investování do zlata

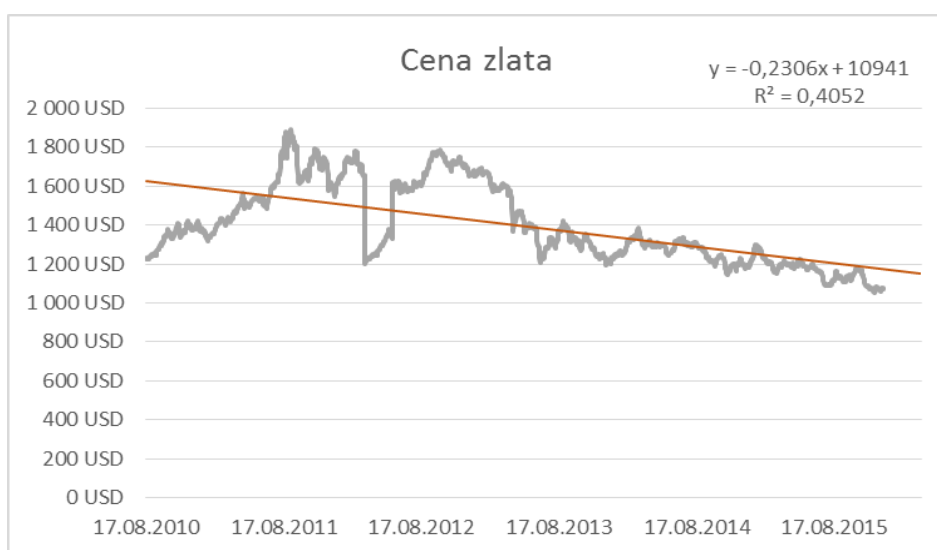
Investiční zlato je podle § 9 zákona o dani z přidané hodnoty

- a) zlato připouštěné na světové trhy zlata ve tvaru uzančných slitků v podobě cihly nebo destičky s
 1. vlastním číslem,
 2. ryzostí nejméně 995 tisícín,
 3. hmotností připouštěnou na těchto trzích a
 4. označením výrobce, ryzosti a hmotnosti,
- b) zlaté mince, které
 1. mají ryzost nejméně 900 tisícín,
 2. byly vyraženy po roce 1800,
 3. jsou nebo byly v zemi svého původu zákonným platidlem a
 4. jsou obvykle prodávány za cenu, která nepřevyšuje volnou tržní hodnotu jejich zlatého obsahu o více než 80 %.

Investiční zlato je dlouhodobě vysoce ceněným finančním aktivem. Po zrušení Brettonwoodského systému sice částečně ztratilo svoji roli jako platidlo, je však stále považováno za významného nositele a uchovatele hodnoty. (Rejnuš, 2014, s. 472)

Jak říkají Studýnka a Struž (2014, s. 36), v kritických okamžicích historie lidstva zlato bylo a vždy bude univerzálním platebním prostředkem. Kdykoli se hroustí měny a hodnoty tohoto světa, lidé ve strachu o svůj majetek utíkají ke zlatu. Zcela zákonitě se vrací (zejména soukromý) zájem o fyzickou držbu zlata, nejlépe pak individuální investice s vlastním neomezeným přístupem a možností jeho přemísťování i prodeje, a to bez potřeby prostředníků.

Obr. 21 znázorňuje cenu zlata v USD ve sledovaném období mezi rokem 2010-2015, kde můžeme sledovat mírně klesající trend.



Obr. 21 Cena za unci zlata v USD v letech 2010-2015
Zdroj: vlastní zpracování podle dat z investexcel.net

Na následujících tabulkách a grafech jsou znázorněny průměrné roční výnosnosti a rizikovosti zlata za posledních 6 let. Při výpočtech jsem vycházela z dat z investexcel.net.

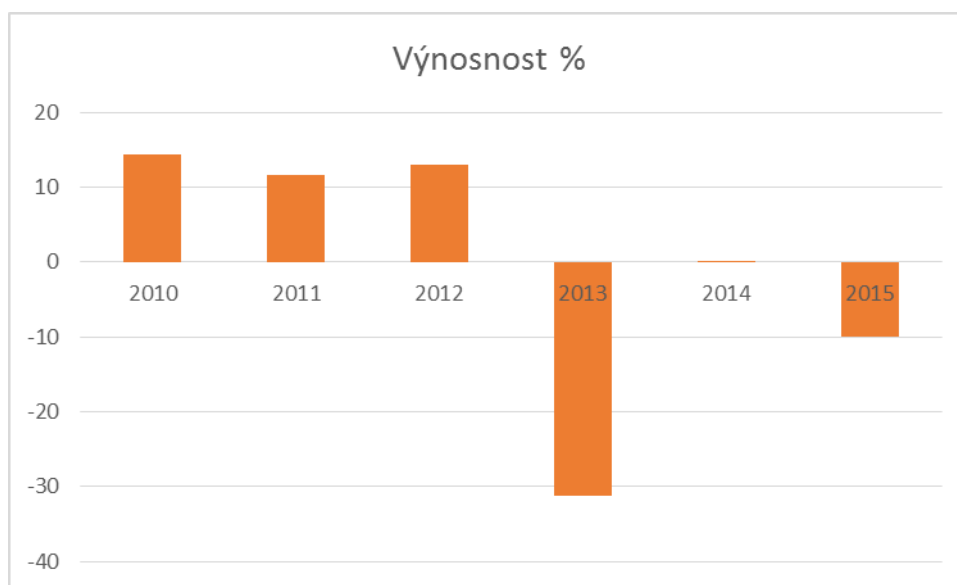
Tab. 12 Roční výnosnost zlata v %

Rok	2010	2011	2012	2013	2014	2015
[%]	14,44	11,66	13,04	-31,27	0,23	-10,04

Zdroj: vlastní zpracování podle dat z investexcel.net

V letech 2010-2012 se roční výnosnost zlata celkem stabilně pohybuje kolem 10 %, v roce 2013 přišel náhlý pokles v podobě záporné výnosnosti

s hodnotou přibližně -31 %. Podle Vencla (2013) klesla cena zlata z několika důvodů. Jeho cena již byla příliš vysoká a ovládaly ji z velké části emoce a ne racionální poptávka. Druhým vysvětlením je změna investičních preferencí a to ze zlata, tedy z bezpečného přístavu, na rizikové, ale výnosnější akcie. Současně politické zprávy ceně zlata moc nepřidaly a ve zlatu zůstali údajně jen dlouhodobí investoři. Cena zlata je stále u dlouhodobých minim a v době psaní této práce má hodnotu 1075 USD k 25. 12. 2015.



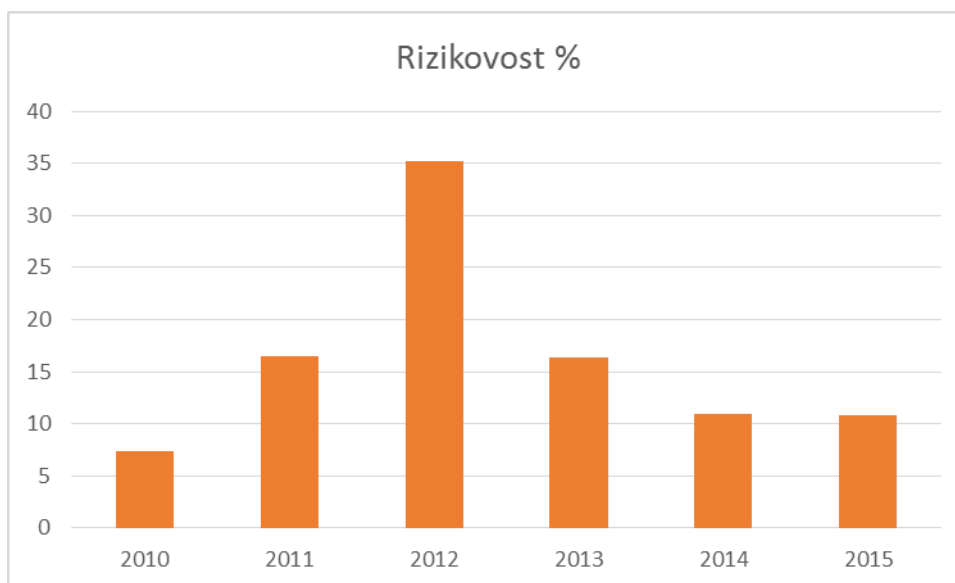
Obr. 22 Grafické znázornění vývoje zlata v %
Zdroj: vlastní zpracování podle dat z investexcel.net

Tab. 13 Roční rizikovost zlata v %

Rok	2010	2011	2012	2013	2014	2015
[%]	7,32	16,51	35,19	16,35	10,9	10,86

Zdroj: vlastní zpracování podle dat z investexcel.net

Rizikovost zlata je nejvyšší v roce 2012 s 35,19 %, od roku 2013 se ale stabilně snižuje.



Obr. 23 Grafické znázornění roční rizikovosti zlata v %
Zdroj: vlastní zpracování podle dat z investexcel.net

Na základě údajů z tab. 12 a tab. 13 je vypočítaná průměrná roční výnosnost, průměrná roční rizikovost a Sharpeho poměr, viz tab. 13. Jako bezrizikovou úrokovou míru jsem použila pětiletou úrokovou míru amerických státních dluhopisů, která je 1,75 %. (Bloomberg, 2015)

Tab. 14 Srovnání ukazatelů u zlata

	<i>Průměrná výnosnost</i>	<i>Průměrná rizikovost</i>	<i>Sharpeho poměr</i>
[%]	-0,32	16,19	-0,13

Zdroj: vlastní zpracování podle dat z investexcel.net

7.3 Investování do bitcoinu

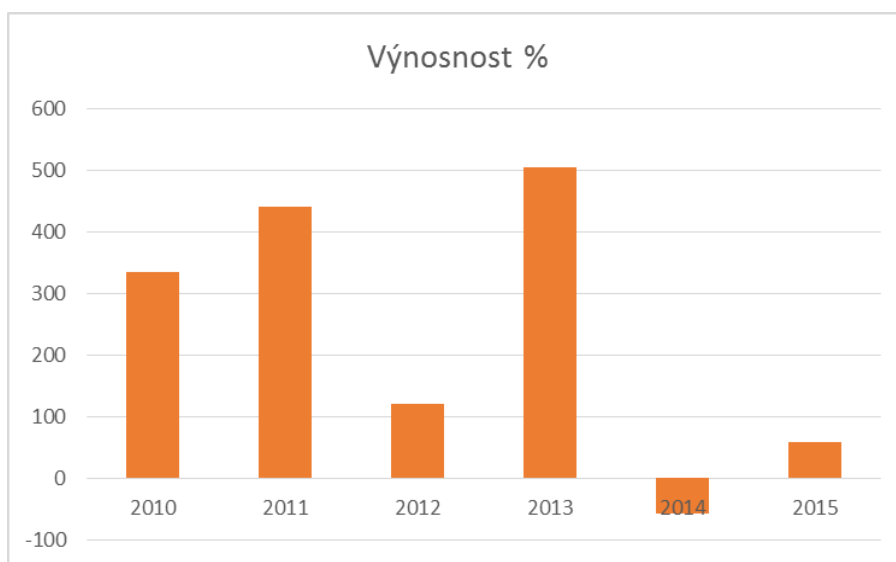
Vývoj ceny bitcoinu v sedmi letech jeho existence jsme si již ukázali v kapitole 5.6 *Vývoj Bitcoinu*, pojdme si tedy ukázat na následujících tabulkách a grafech, jak se bitcoinu vedlo, co se týče jeho výnosnosti a rizikovosti.

Rok 2013 je pro bitcoin nejlepším rokem, kdy na konci tohoto roku dosáhl rekordní ceny 1151 USD/BTC. Na obr. 24 jsou vidět obrovské výkyvy mezi jednotlivými ročními výnosnostmi. Největší výnosnosti dosáhl v roce 2013 s 504 %, hned následující rok se ale objevila záporná výnosnost, a to téměř -60 %. Lidé, kteří do bitcoinu investovali před rokem 2013, na něm mohli velmi dobře vydělat, kdežto ti, kteří čekali a investovali až koncem roku 2013, prodělali i víc než polovinu vkladu.

Tab. 15 Roční výnosnost bitcoinu v %

Rok	2010	2011	2012	2013	2014	2015
[%]	335,27	440,81	120,22	503,88	-58,5	59,12

Zdroj: vlastní zpracování podle dat z blockchain.info

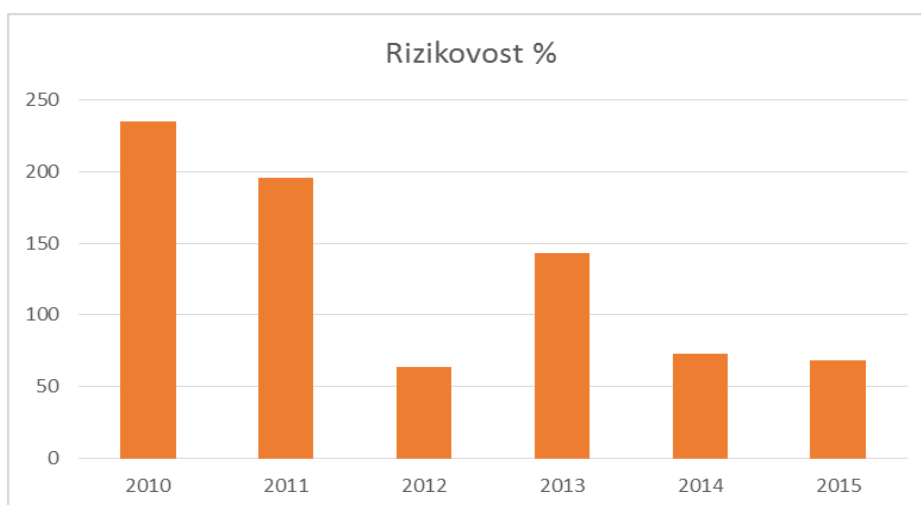


Obr. 24 Grafické znázornění roční výnosnosti bitcoinu v %
Zdroj: vlastní zpracování podle dat z blockchain.info

Tab. 16 Roční rizikovost bitcoinu v %

Rok	2010	2011	2012	2013	2014	2015
[%]	234,96	195,75	63,62	143,05	72,91	68,6

Zdroj: vlastní zpracování podle dat z blockchain.info



Obr. 25 Grafické znázornění roční rizikovosti bitcoinu v %
Zdroj vlastní zpracování podle dat z blockchain.info

Porovnáním rizikovosti a výnosnosti investice do bitcoinů je vidět, jak při investicích platí investiční trojúhelník, tedy čím vyšší výnosnost, tím vyšší rizikovost investice. Na základě údajů z tab. 15 a tab. 16 je vypočítaná průměrná roční výnosnost, rizikovost a Sharpeho poměr investice do bitcoinu za posledních 5 let, viz tabulka 17. Jako bezriziková úroková míra je opět použita průměrná úroková míra pětiletých amerických státních dluhopisů, která je 1,75 %. (Bloomberg, 2015)

Tab. 17 Srovnání ukazatelů u bitcoinu

	<i>Průměrná výnosnost</i>	<i>Průměrná rizikovost</i>	<i>Sharpeho poměr</i>
[%]	233,47	129,82	1,78

Zdroj: vlastní zpracování podle dat z blockchain.info

Hodnota Sharpeho poměru vyšla vysoké číslo, což je způsobené vysokými hodnotami průměrné roční výnosnosti k rizikovosti této investice. K 30. 12. 2015 má bitcoin hodnotu 431 USD/BTC, pojďme se podívat, jaká by byla výnosnost investice jednoho bitcoinu, pokud by si investor koupil bitcoin před jedním až čtyřmi roky a prodal ho 30. 12. 2015. Jak jde vidět z tab. 18, velmi dobře na bitcoinu mohl vydělat investor koupí bitcoinu do roku 2012. Rok 2013, kdy se o bitcoinu nejvíce psalo, o příbězích milionářů, kteří ze dne na den zbohatli díky bitcoinu, by se ale investovi podle dnešních dat určitě nevyplatil se ztrátou okolo 40 % původního vkladu.

Tab. 18 Porovnání výnosnosti investice při nákupu bitcoinu v daných letech

<i>Datum</i>	30. 12. 2011	30. 12. 2012	30. 12. 2013	30. 12. 2014
<i>Nákupní cena [USD]</i>	4,3	13,57	739,1	313,09
<i>Výnosnost investice [%]</i>	9923,26	3076,12	-41,69	37,66

Zdroj: vlastní zpracování podle dat z blockchain.info

7.4 Porovnání investice do bitcoinu a zlata

Pro lepší porovnání zachycuje následující souhrnná tab. 19 vypočítaná data z předchozích 2 kapitol. Ve výpočtech nejsou zahrnuté transakční ani daňové náklady. Už se samotnou koupí zlata se pojí vysoké transakční poplatky, k čemuž se přidává i vysoký spread kolem 20-25 %. Při koupi vznikají náklady na kontrolu pravosti, měření ryzosti, na dopravu, dále skladování a pojištění proti krádeži, to vychází na cca 15 % k čistému zlatu. (Zdražil, 2015) Bitcoin má taky vysoký spread, a to okolo 15 %. U bitcoinu ale není potřeba zabezpečit skladování, pojištění, ani kontrolu pravosti. I transakční poplatky jsou zanedbatelné a ještě dlouho budou. Z tohoto pohledu má bitcoin výhodu oproti zlatu.

Tab. 19 Srovnání investice do bitcoinu a zlata

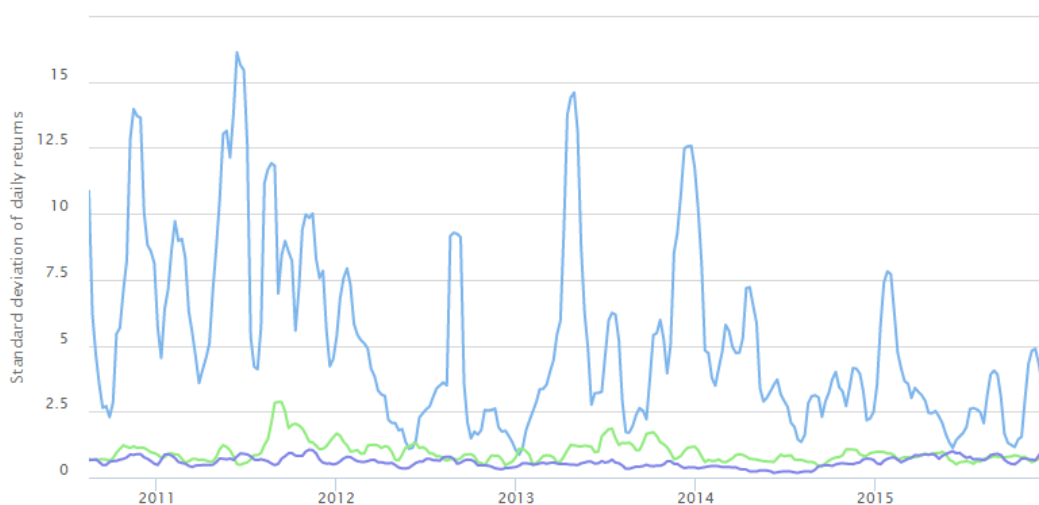
<i>Investice</i>	<i>Průměrná rizikovitost [%]</i>	<i>Průměrná výnosnost [%]</i>	<i>Sharpe Ratio [%]</i>
Bitcoin 2010-2015	129,82	233,47	1,78
Zlato 2010-2015	16,19	-0,32	-0,13

Zdroj: vlastní zpracování podle dat z blockchain.info

Na základě historických údajů je zřejmé, že se investicím do bitcoinu skutečně dařilo a to hlavně v roce 2013. Když se zaměříme čistě jen na výnosnost a rizikovitost těchto investic, můžeme říct, že je výnos i riziko do bitcoinu mnohonásobně větší než do zlata. Investoři, kteří vsadili na bitcoin, mohli na investici vydělat až kolem 500 % zhodnocení, museli ale podstoupit riziko až přibližně 143 %. Proto jsou bitcoiny vhodnější pro agresivnější investory s menší averzí k riziku. Oproti tomu se výnosnost a rizikovitost zlata pohybuje maximálně v desítkách procent. Tato investice byla sice méně výnosná, ale také méně riziková, proto se doporučuje spíše pro konzervativnější typy. Průměrná výnosnost investice zlata vyšla negativně, ale hned bych investici do zlata nezavrhovala. Je to zrovna vybraným obdobím,

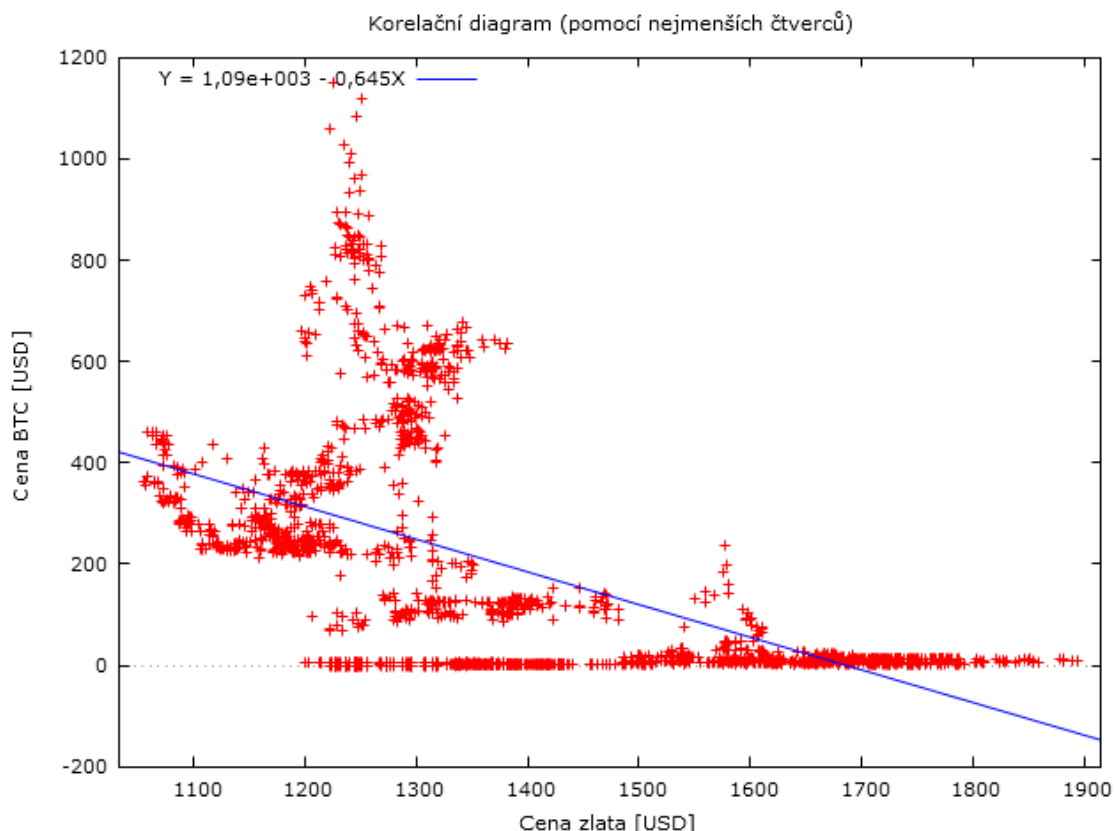
kteřé není pro zlato příliš příznivé, dlouhodobě však cena zlata roste, jak jde vidět z obr. 20, který ukazuje vývoj ceny zlata za posledních 10 let, a z toho vyplývá i rostoucí výnosnost. Zlatu se ale obecně daří spíše v dobách ekonomického poklesu.

Co se týče Sharpeho poměru, bitcoin jako investice vyšla v daném období mnohem výnosnější a rizikovější, což také vypovídá o jeho vyšší volatilitě, kterou si ukážeme na obr. 26, který srovnává třicetidenní průměrnou volatilitu bitcoinu (světle modrá), zlata (zelená) a eura (tmavě modrá) za posledních 5 let. Svislá osa představuje standardní odchylku denních výnosů. Volatilita zlata je oproti bitcoinu velmi nízká, pro srovnání jsem do grafu zařadila extrémně nízkou volatilitu kurzu EUR/USD. Všimněme si však, že se i volatilita bitcoinu postupně snižuje od letošního roku 2015. Bitcoin je známý svou obrovskou volatilitou, dá se ale říct, že to není nic nezvyklého pro nové projekty v začátcích.



Obr. 26 Volatilita bitcoinu, zlata a eura v USD
Zdroj: btcvol.info, 2015

Na obr. 27 můžeme vidět znázorněnou korelaci ceny zlata s bitcoinem, která vyšla $-0,57$. Jde o silně negativní závislost, což znamená, že při růstu ceny zlata klesá cena bitcoinu a naopak. Cena bitcoinu samozřejmě nemůže být záporná, je v grafu uvedena pouze kvůli lepšímu znázornění klesajícího trendu. Záporný koeficient spočítal program Gretl korelační maticí. Tato korelace je na základě dat mezi roky 2010-2015.



Obr. 27 Korelace ceny zlata s bitcoinem

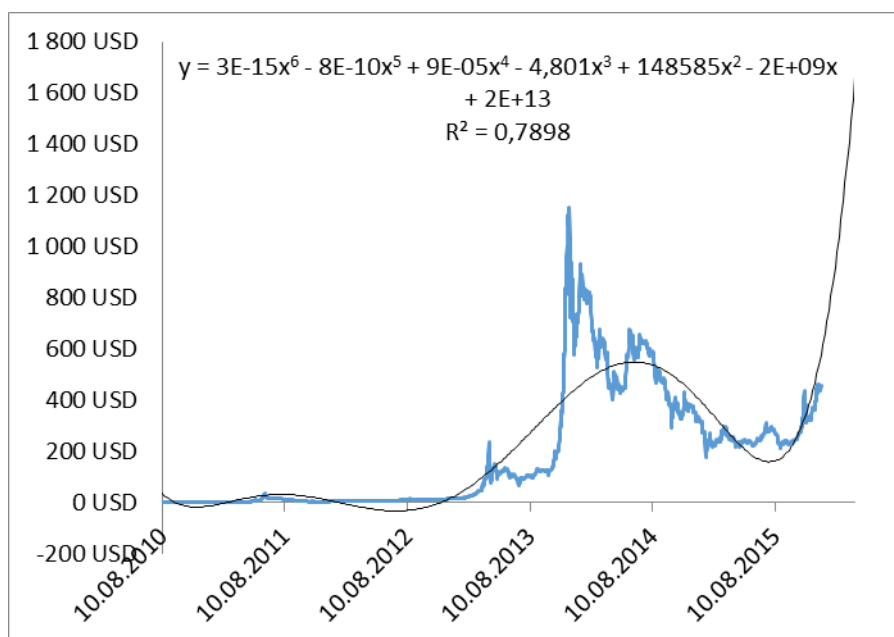
Zdroj: vlastní zpracování podle dat z investexcel.net a blockchain.info (Gretl)

7.5 Závěr kapitoly

V této kapitole jsem porovnala investici do zlata a bitcoinu v letech 2010-2015 pro některé podobné vlastnosti bitcoinu a zlata, mimo jiné to, že jsou obě „komodity“ vzácné, jsou v omezeném množství, nepodléhají inflaci a jsou nezávislé na vlivu vlád. Z krátkodobého hlediska byla v letech 2010-2015 podle dosažených výsledků určitě lepší investice do bitcoinu. Investice do bitcoinu měla v tomto období průměrnou výnosnost neuvěřitelných 233,47 % a průměrnou rizikovost až 129,82 %, oproti tomu zlatu vyšla průměrná výnosnost záporně, a to -0,32 a průměrná rizikovost 16,19 %. Záporná výnosnost je dána nepříznivým zvoleným obdobím pro zlato, neznamená to ale, že je investice do zlata vždy ztrátová. Sharpeho poměr vyšel u bitcoinu 1,78 a u zlata -0,13. Volatilita bitcoinu je oproti zlatu velmi silná, avšak od roku 2015 se snižuje. Koeficient korelace mezi zlatem a bitcoinem vyšel záporně, -0,57, což znamená, že při růstu ceny zlata klesá cena bitcoinu a naopak. Na krátkodobé investice a spekulace se tedy hodí určitě více bitcoin pro jeho vysokou volatilitu, na dlouhodobější investice doporučuji spíše zlato, které je sice méně výnosné, zato mnohem méně riskantní.

8 Předpověď budoucího vývoje Bitcoinu

V této kapitole se podíváme na budoucí vývoj kurzu bitcoinu. Z kapitoly 5.6 *Vývoj Bitcoinu* je patrné, že je cena bitcoinu extrémně citlivá na to, co se o bitcoinu napíše v médiích. Negativní zprávy, jako je krádež bitcoinů na burzách se okamžitě projeví poklesem ceny bitcoinu, naopak pozitivní zprávy, jako je třeba vyhlášení Evropského soudního dvoru, že jsou bitcoin transakce osvobozené od DPH, se projeví růstem ceny bitcoinu. Hodně s kurzem hýbe dění v Číně, či další regulace jiných zemí. Na obr. 28 je znázorněno, jak jsem přidala do grafu vývoje ceny bitcoinu polynomický trend 6. stupně a nastavila předpověď na 100 dnů, podle které má cena bitcoinu rostoucí trend.

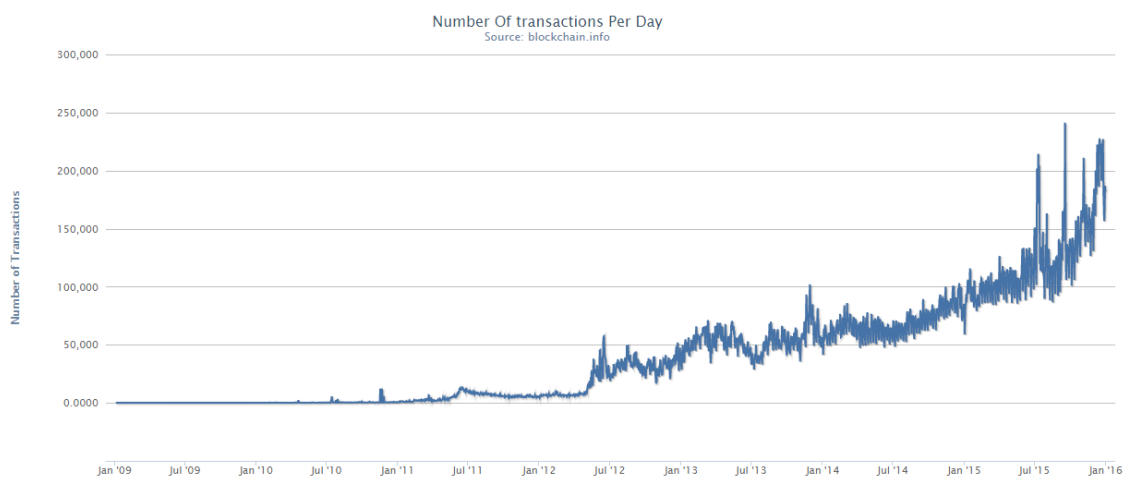


Obr. 28 Předpověď budoucího vývoje kurzu BTC/USD
Zdroj: vlastní zpracování podle dat z blockchain.info

Jak říká Rojko (2015), předpovídání ceny jakéhokoliv aktiva je ošemetná věc. A odhad ceny vysoce volatilního bitcoinu, který je navíc mnohem víc, než jen finančním nástrojem, se téměř blíží magii. Jeden den vyrostete o 10%, aby hned následující den o 5 % poklesl. Proto se Rojko z Cointelegraph zeptal odborníků na jejich názor na cenu bitcoinu na konci roku 2016. Někteří odmítali odpovědět, ovšem ti, co odpověděli, se shodli na tom, že kurz poroste, někteří odhadují dokonce hodnotu 1800-2000 USD/BTC. Vorhees a Gupta (2015) se opírají o fakt, že koncem roku 2016 se bude půlit odměna za vytěžený blok na 12,5 BTC a to by mohlo ovlivnit nárůst ceny bitcoinu, jako se tomu stalo v roce 2012 při prvním půlení, kdy se cena bitcoinu znásobila až osmkrát. Dixon (2015) tvrdí, že nevidí důvod, proč by se bitcoin při býčím trhu nedostal přes nová maxima na úrovni 1200 USD, tentokrát však s trvalejším supportem po dobu několika měsíců a při podstatně vyšším ob-

jemu obchodů, než dnes. Sonnenshein (2015) navíc předpokládá i narůstající institucionální zájem, který povede k dalšímu uvědomění, adopci bitcoinu a jeho používání.

Následující obr. 29 představuje počet uskutečněných transakcí za den od počátku Bitcoinu. Můžeme vidět, že má rostoucí trend, což svědčí o zvyšujícím se zájmu lidí o bitcoin. Denně roste také počet míst akceptujících bitcoin. Čím bude více akceptačních míst, tím bude víc lidí používat bitcoin.



Obr. 29 Počet transakcí za den
Zdroj: blockchain.info, 2015

9 Diskuse

Hlavním cílem bakalářské práce bylo na základě analýzy Bitcoinu jako platebního systému a zhodnocení rizikovosti a výnosnosti investice formulovat doporučení pro potenciálního uživatele a investora do bitcoinu. Pro naplnění prvního cíle, analýzy Bitcoinu jako platebního systému, byly vytyčeny 2 výzkumné otázky.

Výzkumná otázka č. 1: Vyplatí se na českých e-shopech platba za bitcoiny?

Tab. 20 Srovnání cen e-shopů

Produkt	Cena X [CZK]	Cena X [BTC]	Nákup BTC na LB [CZK] (1)	Prům. cena Y [CZK](2)	Rozdíl (1)-(2)
iBit.cz					
Konzole	4 802	0,45684	5 329,42	4 785,54	11,13%
gourmetkava.cz					
Termoska	284	0,02178	254,09	307,8	-17,45%
g-hosting.cz					
CZ doména	242	0,02158	251,71	179,01	40,61%
subreg.cz					
CZ doména	175	0,01563	182,49	184,56	-0,01%

Zdroj: iBit.cz, gourmetkava.cz, g-hosting.cz, subreg.cz, heureka.cz, 2015

Tabulka 20 ukazuje na 4 příkladech, o kolik % se platby bitcoiny prodraží. Za X považuji vybraný e-shop akceptující Bitcoin (iBit.cz, gourmetkava.cz, g-hosting.cz a subreg.cz). Za Y považuji ostatní e-shopy nabízející stejný produkt (vybranými produkty jsou: herní konzole Microsoft XBOX 360 4GB, termoska 0,5l zn. Renberg a registrace domény CZ). Předpokládala jsem, že se platba bitcoiny na českých e-shopech musí vždy prodražit kvůli nákladům obchodníka při zavedení této platební možnosti. Velkým omezením výzkumu byl malý vzorek zkoumaných dat, kdy jsem srovnávala jen 4, resp. 3 vybrané produkty. Bylo to dáno tím, že ještě v ČR není tolik e-shopů s možností platby bitcoiny, kde by se daly koupit produkty, které se dají srovnat. Např. jsem sice našla 2 e-shopy, které nabízely šperky s možností platby bitcoinu, ale tady nešlo srovnat konkrétní stejný produkt u jiných ob-

chodníků. Výsledek mě překvapil, jelikož se v některých případech opravdu nákup na daném e-shopu za bitcoiny vyplatil spíše než nákup produktu na klasickém e-shopu. Zajímavá byla termoska 0,5 l zn. Renberg, která vycházela při kurzu v době výzkumu na samém e-shopu levněji při platbě bitcoiny o cca 30 Kč. U nabídky registrace CZ domény byly odlišné výsledky způsobené tím, že jsem do výpočtu zahrнула i akční ceny na e-shopech, i když zrovna stránka subreg.cz tuto službu v akci neměla a stála o 67 Kč méně než u g-hosting.cz. Na stránce iBit.cz byla cena konzole přímo dána v bitcoinech, což se velmi prodražilo kvůli pohyblivému kurzu. Ostatní vybrané e-shopy s možností platby bitcoinu používají platební bránu Bit-Pay a fungovaly tak, že měly u produktů ceny v českých korunách a až na konci při výběru metody platby se cena převedla na bitcoinu dle aktuálního kurzu, proto tam byl malý rozdíl. Průměrně se tedy nákup za bitcoiny mohl prodražit o 8,57 %, nedá se to však říct jako pravidlo, protože byl výzkum proveden na malém množství vzorku.

Výzkumná otázka č. 2: Jak vychází Bitcoin jako nástroj zahraničního platebního styku?

Tabulka 21 srovnává zaokrouhlené výstupy pro převod 10 000 Kč, 20 000 Kč, 50 000 Kč, 100 000 Kč, 150 000 Kč a 1 000 000 Kč. V závorce je uvedena vypočtená nákladovost v %. Zeleně jsou označeny nejnižší náklady, žlutě druhé nejnižší a červeně nejvyšší náklady.

Co se týče nákladů v Kč, tak byl Bitcoin nejlevnější včetně nákladů při směně bitcoinů za lokální měnu. Vždy jsem si myslela, že má Western Union předražené poplatky, ale ve výsledku je ještě levnější a mnohem rychlejší než banky. Banky mají spoustu skrytých poplatků a devizové kurzy také dost ovlivnily konečný výstup. Služba cash2vn vyšla nejdráž, po ní hned střední banky. V tab. 21 je shrnutá průměrná výše poplatků jednotlivých zástupců a rychlost převodů prostředků. Částky v USD jsem převedla dle aktuálního kurzu USD/CZK na webových stránkách ČNB k 22. 12. 2015. Podle tabulky můžeme vidět, že co se týče rychlosti, tak je na tom nejlépe Bitcoin a Western Union (cash2vn funguje také přes Bitcoin), které peníze doručí v rámci minut. Střední banky vychází nejdráž, malé banky mají v některých případech nižší poplatky, které jsou ale vykompenzovány delší dobou doručení.

Shrnula bych to tak, že je Bitcoin porovnatelný s Western Union co se týče rychlosti i nákladů. WU vychází sice o něco dráž, ale příjemce ve Vietnamu dostane rovnou peníze v lokální měně a nemusí řešit prodej bitcoinů za dongy, což pro ne-technicky zaměřeného člověka není zrovna jednoduchá záležitost. Je ale na zvážení, pokud by se jednalo o pravidelné platby, nevyplatilo by se mu se o bitcoinu trochu doučit a ušetřit tak za poplatky ve WU?

Tab. 21 Komparace výstupů

	<i>Malé b.</i>	<i>Střední b.</i>	<i>Velké b.</i>	<i>Western Union</i>	<i>Cash2vn</i>	<i>Bitcoin</i>
<i>Vstup [Kč]</i>	10 000					
<i>Výstup [Kč]/[%]</i>	9 502 (4,98)	9 415 (5,85)	9 551 (4,49)	9 625 (3,75)	9 369 (6,32)	9 842 (1,58)
<i>Vstup [Kč]</i>	20 000					
<i>Výstup [Kč]/[%]</i>	19 298 (3,51)	19 172 (4,14)	19 391 (3,05)	19 313 (3,44)	18 784 (6,08)	19 684 (1,58)
<i>Vstup [Kč]</i>	50 000					
<i>Výstup [Kč]/[%]</i>	48 685 (2,63)	48 257 (3,49)	48 681 (2,64)	48 483 (3,03)	-	49 212 (1,58)
<i>Vstup [Kč]</i>	100 000					
<i>Výstup [Kč]/[%]</i>	97 421 (2,58)	97 043 (2,96)	97 880 (2,12)	98 483 (1,52)	-	98 425 (1,58)
<i>Vstup [Kč]</i>	150 000					
<i>Výstup [Kč]/[%]</i>	146 044 (2,64)	144 819 (3,45)	146 046 (2,64)	146 983 (2,01)	-	147 637 (1,58)
<i>Vstup [Kč]</i>	1 000 000					
<i>Výstup [Kč]/[%]</i>	978 284 (2,17)	973 748 (2,63)	981 999 (1,8)	-	-	984 255 (1,58)

Zdroj: Seznam bank a jejich poplatků, intercash.cz, cash2vn.com, 2015

Tab. 22 Průměrná výše poplatků

<i>Subjekt</i>	<i>10 tis. [Kč]</i>	<i>20 tis. [Kč]</i>	<i>50 tis. [Kč]</i>	<i>100 tis. [Kč]</i>	<i>150 tis. [Kč]</i>	<i>1 mil. [Kč]</i>	<i>Rychlost [dny]</i>
Malé banky	250	250	250	500	840	840	D+5
Střední banky	300	300	490	980	1500	1500	D+3
Velké banky	243	243	475	950	1500	1500	D+3
Western Union	375	687	1517	2517	3017	-	D+0
Cash2vn	50	50	-	-	-	-	D+0
Bitcoin	1	1	1	1	1	1	D+0

Zdroj: Seznam bank a jejich poplatků, intercash.cz, cash2vn.com, 2015

Pro naplnění druhého cíle, kdy jsem měla na základě zhodnocení rizikovosti a výnosnosti investice do bitcoinu formulovat doporučení pro potenciálního uživatele a investora, byla vytyčena

Výzkumná otázka č. 3: Byla v letech 2010-2015 lepší investice do bitcoinu než do zlata?

Vybrala jsem zlato pro porovnání, protože má hodně podobných vlastností jako bitcoin. Zlato i bitcoin jsou decentralizované „komodity“, to znamená, že žádná vláda nemůže ovládat množství zlata a bitcoinu v oběhu, nedají se zfalšovat či namnožit, jako u standardní fiat měny, kvůli omezenému množství jsou vzácné, nepodléhají inflaci a předpokládá se růst jejich ceny s postupem času.

Tab. 23 Srovnání investice do bitcoinu a zlata

<i>Investice</i>	<i>Průměrná rizikovost [%]</i>	<i>Průměrná výnosnost [%]</i>	<i>Sharpe Ratio [%]</i>
Bitcoin 2010-2015	129,82	233,47	1,78
Zlato 2010-2015	16,19	-0,32	-0,13

Zdroj: vlastní zpracování podle dat z blockchain.info

Z krátkodobého hlediska byla v letech 2010-2015 podle dosažených výsledků určitě lepší investice do bitcoinu. Investice do bitcoinu měla v tomto období průměrnou výnosnost neuvěřitelných 233,47 % a průměrnou rizikovost až 129,82 %, oproti tomu zlatu vyšla průměrná výnosnost záporně, a to -0,32 a průměrná rizikovost 16,19 %. Záporná výnosnost je dána nepříznivým zvoleným obdobím pro zlato. Sharpeho poměr vyšel u bitcoinu 1,78 a u zlata -0,13. Neznamena to však, že je investice do zlata rizikovější, to je právě nevýhoda Sharpeho poměru, který neumí rozlišovat mezi chtěnou „vrchní“ volatilitou (směrodatná odchylka chtěných výnosů) a negativní volatilitou (směrodatná odchylka výnosů/ztrát pod hodnotou bezrizikového výnosu R_f). Kvůli tomu bych navrhovala jako ukazatel výkonnosti investic použít spíše Sortino Ratio. Je to vlastně modifikace Sharpe ratio s tím rozdílem, že pracuje s volatilitou výnosů pod požadovanou hodnotou výnosu (obvykle bezrizikový výnos) a ztrát (jinými slovy směrodatnou odchylkou nedostatečných výnosů a ztrát).

Když se zaměříme čistě jen na výnosnost a rizikovost těchto investic, můžeme říct, že je výnos i riziko do bitcoinu mnohonásobně větší jak do zlata. Investoři, kteří vsadili na bitcoin, mohli na investici vydělat až kolem 500 % zhodnocení, museli ale podstoupit riziko až přibližně 143 %. Proto jsou bitcoiny vhodnější pro agresivnější investory s menší averzí k riziku. Oproti tomu se výnosnost a rizikovost zlata pohybuje maximálně v desítkách procent. Tato investice byla sice méně výnosná, ale také méně riziková, proto se doporučuje spíše pro konzervativnější typy. Průměrná výnosnost investice zlata vyšla negativně, ale hned bych investici do zlata nezavrhovala. Je to zrovna vybraným obdobím, které není pro zlato příliš příznivé, dlouhodobě však cena zlata roste. Jelikož je bitcoin velmi mladá technologie a vyznačuje se vysokou volatilitou, doporučuji do bitcoinu investovat maximálně tolik, kolik si můžete dovolit ztratit. U bitcoinu člověk neví, co s ním bude za měsíc, natož za rok. Zlato je naopak větší jistota, i když z krátkodobého hlediska není držba zlata tak výnosná, jako držba bitcoinů.

I když je Bitcoin stále jakýsi experiment a nikdo s jistotou neví, jak to s ním dopadne, já osobně si myslím, že má velmi nadějnou budoucnost. Když jsem pracovala s bitcoinem ať už při odesílání nebo přijetí transakce, či placení jednoduše načtením QR kódu, přišla mi jeho technologie geniální transparentností všech

transakcí, nízkými náklady, rychlostí realizace plateb. Překvapilo mě při sledování blockchainu, že ještě tolik transakcí posílají lidé bez poplatku. Věřím, že se v budoucnu bude běžně platit bitcoiny, stejně jako dnes běžně používáme internet, kterému před 20 lety také rozuměli jen „IT nadšenci“.

10 Závěr

Hlavním cílem bakalářské práce bylo na základě analýzy Bitcoinu jako platebního systému a zhodnocení rizikovosti a výnosnosti investice formulovat doporučení pro potenciálního uživatele a investora do bitcoinu. K dosažení hlavního cíle bylo využito několika dílčích cílů. V rámci literární rešerše odborných zdrojů byly analyzovány základy kryptografie, principy fungování Bitcoinu a jeho základní vlastnosti.

Jedním z dílčích cílů bylo identifikovat stav právní regulace Bitcoinu v jednotlivých zemích, kde jsem došla k následujícímu závěru. V současnosti je postoj zemí vůči Bitcoinu velmi různorodý. V žádné zemi není Bitcoin považován za národní měnu, ale například v Německu je považován za účetní jednotku, což spadá pod finanční instrumenty a veškeré regulace finančních instrumentů se tedy týkají i bitcoinů. Evropská unie zaujímá neutrální postoj, virtuální měny nepodporuje, ani nezakazuje. Od října 2015 se na bitcoinová transakce nevztahuje DPH. Česká republika stejně jako EU nepovažuje virtuální „měny“ za měny a v současné době neuplatňuje žádná zvláštní zákonná opatření proti virtuálním měnám, která by je zakazovala, nebo omezovala. ČNB nevykonává dohled nad subjekty, které obchodují s virtuálními měnami. V Rusku se v dubnu 2015 na konferenci o bitcoinu projednával návrh na zákaz kryptoměn, zatím však není nic oficiálně platné. V USA jsou bitcoiny považovány za komoditu vedle např. zlata a ropy. Stát New York vydal v červnu 2015 BitLicence, tedy předpisy, podle kterých se musí řídit všechny firmy, které obchodují s virtuálními měnami. Pro Čínu je Bitcoin zajímavý nejen ze spekulativního hlediska. V zemi jsou totiž relativně tvrdá opatření určená k tomu, aby nebylo možné místní měnu juan vyvážet. V Číně je proto finanční instituce zakázané obchodování s bitcoiny. Bitcoin je velmi citlivý na události na čínském trhu. Další země, které zaujímají nepřátelský postoj k virtuálním měnám s částečným až úplným zákazem, jsou Ekvádor, Taiwan, Bolívie, Bangladéš, Ekvádor, Island, Kyrgyzstán, Thajsko a Vietnam.

Dalším dílčím cílem bylo doporučit vhodnou peněženku na „úschovu“ bitcoinů. Po osobním vyzkoušení doporučuji pro běžného uživatele si nainstalovat odlehčenou softwarovou peněženku typu MultiBit do počítače, která není tak náročná na paměť jako Bitcoin Core, protože nestahuje celý Blockchain, ale jen hlavičky transakcí. U Bitcoin Core jsem nechala stahovat Blockchain přes 12 hod, i tak nebyla stažená ani půlka. Blockchain má v době psaní této práce velikost 50 GB, bude růst čím dál rychleji dle její exponenciální křivky. Papírová peněženka je podle mě nutná vždy k jakékoli peněženke, je bezpečná, protože je offline, ideálně jich mít víc na různých místech. Její nevýhodou je životnost papíru a inkoustu při špatném skladování, doporučuje se uschovat ve folii v seifu proti požáru. V běžném životě ocení uživatel mobilní peněženku, jedná se o aplikaci v telefonu, díky které můžeme platit bitcoiny např. v kavárnách, restauracích velmi rychle a jednoduše načtením QR kódu obchodníka a potvrzením transakce. Online peněženky patří k nejpoužívanějším peněženkám pro jejich snadné používání, dostupnost, rychlost registrace a nemusíme řešit zabezpečení. Je to sice pohodlné, na druhou stranu má po-

skytovatel služby přístup ke všem našim bitcoinům, je tedy nutná důvěra v třetí stranu. Ačkoli poskytovatel nemusí mít nekalé úmysly, bývá často terčem útoků hackerů. Pokud uživatel trvá na online peněžence, doporučuje se na ní mít jen malý obnos a vybrat si důvěryhodnou platformu, jako je např. Coinbase, která 98 % bitcoinů uchovává offline. Pro větší majetek v bitcoinech doporučuji hardwarovou peněženku, která je ze všech peněženek úplně nejbezpečnější, v této práci jsem se zaměřila konkrétně na český produkt Trezor. Je ochráněn před viry díky tomu, že se jedná o samostatnou počítačovou jednotku s jednosměrným zadáváním z Trezoru do počítače (naopak to nejde), PIN se zadává kurzorem myši na speciální klávesnici na obrazovce, která pokaždé náhodně mění postavení čísel – ochrana před keyloggerem. V neposlední řadě je vysoce bezpečné potvrzování transakcí mechanickým způsobem (stisknutím tlačítka na Trezoru), což hacker není schopen udělat.

Dalším dílčím cílem bylo doporučit nejlepší způsob získání bitcoinů v České republice. Došla jsem k závěru, že se pro jednotlivce dnes už nevyplatí těžit bitcoiny kvůli vysokým nákladům na elektřinu. V ČR existuje několik BTC směnárén, kde je možno koupit či prodat bitcoiny. Výhodou směnárén je jednoduchost a rychlost obchodování, nevýhodou je velký spread mezi výkupní a prodejní cenou. V dnešní době existuje pouze jedna česká burza BitStock. Výhodou je obchodování v českých korunách, a tudíž nemusíme řešit SEPA převody, jako u zahraničních burz, i když tam jsou nižší poplatky, nevýhodou je nevýhodná cena oproti zahraničním burzám právě kvůli malému trhu. Další možností získání bitcoinů je služba LocalBitcoins.com, která shromažďuje uživatele, kteří chtějí nakupovat či prodávat bitcoiny a dělí je podle lokace, funguje jako klasická burza. Výhodou je opět lokální měna a výběr metody platby i v hotovosti, nevýhodou je velmi malý trh. Další možností získání bitcoinů je Bitcoinmat (něco jako bankomat), který je taktéž velmi jednoduchý a rychlý, fungují i obousměrné, to znamená, že krom nákupu bitcoinů můžu v bitcoinmatu i prodat bitcoiny za koruny. Nevýhodou je, že těchto automatů je v ČR jen do deseti kusů, z toho většina je v Praze, a po jednom v Brně, Ostravě a Plzni. Pokud potřebuje uživatel bitcoiny co nejrychleji, doporučuji bitcoinmat. Pokud se uživatel nenachází v jednom z uvedených měst, kde se bitcoinmat nalézá nebo jednoduše by si raději bitcoiny nakoupil v pohodlí domova, pak doporučuji jednu ze směnárén, při vedení účtu u stejné banky, jako má směnárna, může získat bitcoiny téměř okamžitě. Pokud chce uživatel nakoupit bitcoiny za co nejlevněji, pak doporučuji LocalBitcoins nebo burzu.

Jedním z hlavních cílů bylo analyzovat Bitcoin jako platební nástroj na základě následujících dvou výzkumných otázek:

Výzkumná otázka č. 1: Vyplatí se na českých e-shopech platba za bitcoiny?

Při srovnání cen vybraných 4 produktů v BTC s jejich cenami v Kč na ostatních eshopech v ČR jsem zjistila, že není pravidlem, že se nákup v bitcoinech musí vždy prodražit. V některých případech se to může vyplatit i s náklady na prvotní nákup

bitcoinů. Výsledek je ovšem diskutabilní vzhledem k malému vzorku zkoumaných dat.

Výzkumná otázka č. 2: Jak vychází Bitcoin jako nástroj zahraničního platebního styku?

Zde jsem porovnála české banky, Western Union, cash2vn a Bitcoin v rámci převodu finančních prostředků z České republiky do Vietnamu, kde jsem porovnála nákladovost a rychlost daných služeb. Nejlevněji vyšel Bitcoin s nákladovostí 1,58 % u libovolné transakce od 10 000 Kč až 1 000 000 Kč. U bank a Western Union se poplatky snižují se zvětšujícím objemem prostředků. Služba cash2vn se nevyplatí vůbec s nákladovostí okolo 6 %. Co se týče rychlosti, tak u bank se peníze převedou zhruba do 3-4 dnů, u Western Union je to v rámci minut, u Bitcoinu taktéž. Bitcoin je dle vypočítaných výsledků nejlepší nástroj, s rychlostí je porovnatelný s Western Union. WU je ale na druhou stranu pohodlnější cesta pro příjemce, jelikož si může na místě vyzvednout peníze ve VND, kdežto u Bitcoinu musí přijaté bitcoiny ještě směnit na burze nebo LocalBitcoins.

Druhým hlavním cílem bylo zhodnotit rizikovost a výnosnost investice do bitcoinu a formulovat doporučení pro potenciálního investora do bitcoinu. K tomuto cíli se vztahuje

Výzkumná otázka č. 3: Byla v letech 2010-2015 lepší investice do bitcoinu než do zlata?

Zde jsem porovnála investici do zlata a bitcoinu v letech 2010-2015 pro některé podobné vlastnosti bitcoinu a zlata, jako je to, že jsou obě „komodity“ vzácné, jsou v omezeném množství, nepodléhají inflaci a jsou nezávislé na vlivu vlád. Z krátkodobého hlediska byla v letech 2010-2015 podle dosažených výsledků určitě lepší investice do bitcoinu. Investice do bitcoinu měla v tomto období průměrnou výnosnost neuvěřitelných 233,47 % a průměrnou rizikovost až 129,82 %, oproti tomu zlatu vyšla průměrná výnosnost záporně, a to -0,32 a průměrná rizikovost 16,19 %. Záporná výnosnost je dána nepříznivým zvoleným obdobím pro zlato, neznámá to ale, že je investice do zlata vždy ztrátová. Sharpeho poměr vyšel u bitcoinu 1,78 a u zlata -0,13. Znamená to, že investice do bitcoinu byla lepší než investice do zlata ve zkoumaném období. Neznámá to však, že je investice do zlata vždy rizikovější, tato hodnota vyšla kvůli záporné výnosnosti u zlata, je to z nedostatku Sharpeho poměru, který neumí rozlišovat mezi chtěnou „vrchní“ volatilitou (směrodatná odchylka chtěných výnosů) a negativní volatilitou (směrodatná odchylka výnosů/ztrát pod hodnotou bezrizikového výnosu R_f). Volatilita bitcoinu je oproti zlatu velmi vysoká, avšak od roku 2015 se snižuje. Korelace mezi zlatem a bitcoinem vyšla -0,57, což je silně negativní závislost. Na krátkodobé investice a spekulace se tedy hodí určitě více bitcoin pro jeho vysokou volatilitu, na dlouhodobější investice doporučuji spíše zlato, které je sice méně výnosné, zato

mnohem méně riskantní. Na závěr bych tedy pro potenciálního investora do bitcoinu doporučila investovat jen tolik, kolik si může dovolit ztratit, protože zatím u bitcoinu nikdo netuší, co s ním bude za měsíc, natož za rok.

Posledním dílčím cílem bylo nastínit možný budoucí vývoj Bitcoinu. Předpovídat cenu jakéhokoli aktiva je ošemetná věc, obzvlášť u Bitcoinu, který má velmi krátkou historii, je vysoce volatilní a velmi citlivý na to, co o něm kdo v médiích napíše. Dle spojnice trendu grafu z dosavadních dat předpovídá Excel růst ceny bitcoinu, v čemž se shodují také odborníci v oboru. Zdůvodňují to nejčastěji očekávaným halvingem (půlením odměny pro těžaře v roce 2016). Podle dat na blockchain.info se den ode dne zvyšuje počet uskutečněných transakcí, zvyšuje se také počet akceptačních míst. Čím víc lidí bude přijímat bitcoin, tím víc ho budou lidé používat. Bitcoin přežije, pokud mu budou lidé věřit. I když je Bitcoin stále jakýsi experiment a nikdo s jistotou neví, jak to s ním dopadne, já osobně věřím, že se v budoucnu bude běžně platit bitcoiny, stejně jako dnes běžně používáme internet, kterému před 20 lety také rozuměli jen „IT nadšenci“.

11 Literatura

- 5-letá úroková míra amerických státních dluhopisů [online]. 2015 [cit. 2015-12-29]. Dostupné z: <http://www.bloomberg.com/markets/rates-bonds/government-bonds/us>
- ANTONOPOULOS, Andreas M. *Mastering bitcoin*. Sebastopol: O'Reilly Media, c2015. ISBN 978-144-9374-044
- ASCHENBECK-FLORANGE, Tanja. *Regulation of Bitcoins in Germany: First comprehensive statement on Bitcoins by German Federal Financial Supervisory Authority (BaFin)*. Bitcoinmagazine.com [online]. 2014 [cit. 2016-05-02]. Dostupné z: <https://bitcoinmagazine.com/articles/regulation-bitcoins-germany-first-comprehensive-statement-bitcoins-german-federal-financial-supervisory-authority-bafin-1391637959>
- BACK, Adam. *Hashcash - A Denial of Service Counter-Measure* [online], 2002 [cit. 2015-12-27]. Dostupné z: <http://www.hashcash.org/papers/hashcash.pdf>
- BARSKI, Conrad a Chris WILMER. *Bitcoin for the befuddled*. San Francisco, CA: No Starch Press, 2014. ISBN 978-1-59327-573-0
- BEDŘICH, Václav. *S touhle debetní platební kartou můžete kdekoliv na světě platit v bitcoinech* [online]. CzechCrunch 2015 [cit. 2016-05-05]. Dostupné z: <http://www.czechcrunch.cz/2015/11/s-touhle-debetni-platebni-kartou-muzete-kdekoliv-na-svete-platit-v-bitcoinech/>
- Bitcoin Regulation*. Coin.co [online]. [cit. 2016-05-02]. Dostupné z: <https://coin.co/bitcoin-guide/regulations>
- BITCOINHELP. *How To Send Bitcoins From A Paper Wallet* [online]. 2014 [cit. 2016-05-05]. Dostupné z: <https://bitcoinhelp.net/know/more/send-from-paper-wallet>
- BITCOINVIETNAM. *Mua và bán Bitcoin với Đồng!* [online]. [cit. 2015-12-18]. Dostupné z: <https://www.bitcoinvietnam.com.vn/>
- BITCOINWIKI. *Proof of Work* [online]. 2015 [cit. 2016-05-08]. Dostupné z: https://en.bitcoin.it/wiki/Proof_of_work
- BITSTOCK. *Bitcoin burza* [online]. [cit. 2015-12-18]. Dostupné z: <http://bitstock.com/>
- BLOOMBERG NEWS. *China Bans Financial Companies From Bitcoin Transactions*. Bloomberg [online]. 2013 [cit. 2016-05-03]. Dostupné z: <http://www.bloomberg.com/news/articles/2013-12-05/china-s-pboc-bans-financial-companies-from-bitcoin-transactions>
- BUDIŠ, Petr. *Elektronický podpis a jeho aplikace v praxi*. Olomouc: ANAG, 2008. Právo (ANAG). ISBN 978-80-7263-465-1.
- CASH2VN. *Send money to Vietnam. Cheap and simple*. [online]. [cit. 2015-12-18]. Dostupné z: <https://www.cash2vn.com>

- CFTC. *CFTC Orders Bitcoin Options Trading Platform Operator and its CEO to Cease Illegally Offering Bitcoin Options and to Cease Operating a Facility for Trading or Processing of Swaps without Registering* [online]. [cit. 2016-05-03]. Dostupné z: <http://www.cftc.gov/PressRoom/PressReleases/pr7231-15>
- CLINCH, Matt. *Baidu division now accepting bitcoins*. CNBC [online]. 2013 [cit. 2016-05-03]. Dostupné z: <http://www.cnbc.com/2013/10/16/baidu-division-now-accepting-bitcoins.html>
- COINBASE. *Bitcoin Wallet - Coinbase* [online]. [cit. 2016-05-05]. Dostupné z: <https://www.coinbase.com/>
- COINDESK. *How to Make a Paper Bitcoin Wallet* [online]. [cit. 2016-05-05]. Dostupné z: <http://www.coindesk.com/information/paper-wallet-tutorial/>
- COINHUB. *Bitcoin směnárna* [online]. [cit. 2015-12-18]. Dostupné z: <http://www.coinhub.cz/>
- ČNB. *Obchodování s bitcoiny* [online]. 2014 [cit. 2016-05-02]. Dostupné z: https://www.cnb.cz/cs/faq/obchodovani_s_bitcoiny.pdf
- ČSOB. *SEPA* [online]. 2015 [cit. 2015-12-18]. Dostupné z: https://www.csob.cz/portal/lide/produkty/ucty-a-platby/platby/zahranicni-a-tuzemske-devizove-platby#vse-o-platbach|shkv_3
- DAS, Samburaj. *Bitcoin Declared Illegal in Taiwan*. CryptocoinsNews[online]. 2015 [cit. 2015-12-07]. Dostupné z: <https://www.cryptocoinsnews.com/bitcoin-declared-illegal-in-taiwan/>
- DHAKA TRIBUNE. *Bitcoin illegal in Bangladesh* [online]. 2014 [cit. 2016-05-04]. Dostupné z: <http://www.dhakatribune.com/bangladesh/2014/sep/16/bitcoin-illegal-bangladesh>
- DONNELLY, Jacob. *Bitcoin Price Hits 2015 Highs Led by Chinese Exchanges*. Bitcoin-Magazine [online]. 2015 [cit. 2016-05-05]. Dostupné z: <https://bitcoinmagazine.com/articles/bitcoin-price-hits-highs-lead-by-chinese-exchanges-1446498909>
- DUŠEK, Jiří. *DPH 2015: zákon s přehledy*. Praha: Grada, 2015, ^^^sv. Účetnictví a daně (Grada). ISBN 978-80-247-5434-5.
- EBA. *Varování pro spotřebitele týkající se virtuálních měn*. [online]. [cit. 2016-05-02]. Dostupné z: https://www.eba.europa.eu/documents/10180/598420/EBA_2013_0103000_0_CS_TRA.pdf
- ECB. *Virtual currency schemes – a further analysis* [online]. 2015 [cit. 2015-12-05]. ISBN 978-92-899-1560-1. Dostupné z: <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf>
- ECB. *Virtual currency schemes* [online]. Frankfurt-on-Main: European Central Bank, 2012 [cit. 2015-12-05]. ISBN 978-928-9908-627. Dostupné z: <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>

- FAÚ. *Metodický pokyn o přístupu povinných osob k digitálním měnám* [online]. 2013 [cit. 2016-05-10]. 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
- FBI. *Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Detering Illicit Activity* [online]. 2012 [cit. 2016-05-03]. Dostupné z: http://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf
- FILLNER, Karel. *Bitcoin Trezor – recenze: Jak mít bitcoiny v bezpečí*. BtcTip [online]. 2014 [cit. 2016-05-05]. Dostupné z: <http://btctip.cz/bitcoin-trezor-recenze/>
- FILLNER, Karel. *Je bitcoin legální? Hrozí mu zákaz?* BtcTip [online]. 2014 [cit. 2015-12-03]. Dostupné z: <http://btctip.cz/je-bitcoin-legalni>
- FILLNER, Karel. *Vlastnosti btc, výhody i nevýhody*. Btctip[online]. 2014 [cit. 2015-11-18]. Dostupné z: <http://btctip.cz/vlastnosti-btc-vyhody-i-nevyhody>
- FILLNER, Karel. *Jak na bitcoin krok za krokem: Ověřené postupy, tipy a triky jak ihned získat a používat vaše nové digitální peníze - bitcoiny*. 2. vydání. Praha, 2014.
- FINANCE MAGNATES. *Bitcoin deemed illegal in Kyrgyzstan* [online]. 2014 [cit. 2016-05-04]. Dostupné z: <http://www.financemagnates.com/forex/brokers/bitcoin-deemed-illegal-in-kyrgyzstan/>
- FINCEN. *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies* [online]. 2013 [cit. 2016-05-03]. Dostupné z: https://www.fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html
- FIRSTBITCOIN. *Bitcoin směnárna* [online]. [cit. 2015-12-18]. Dostupné z: <http://www.firstbitcoin.cz/>
- FRANCO, Pedro. *Understanding Bitcoin: cryptography engineering and economics*. Wiley, 2014. ISBN 978-1-119-01916-9
- Generátor Bitaddress* [online]. [cit. 2015-12-10]. Dostupné z: <http://bitaddress.org/>
- G-HOSTING. [online]. [cit. 2015-12-18]. Dostupné z: <http://g-hosting.cz/>
- GOURMET KÁVA. [online]. [cit. 2015-12-18]. Dostupné z: <http://gourmetkava.cz/>
- GUTTMANN, Benjamin. *The Bitcoin Bible gold edition*. Norderstedt: Books on demand, 2014. ISBN 978-3-7322-9696-5
- HEUREKA. [online]. [cit. 2015-12-18]. Dostupné z: <http://heureka.cz/>
- History of Bitcoin* [online]. [cit. 2015-12-15]. Dostupné z: <http://historyofbitcoin.org/>
- HRUSKA, Joel. *One Bitcoin group now controls 51% of total mining power, threatening entire currency's safety*. ExtremeTech [online]. 2014 [cit. 2016-04-14]. Dostupné z: <http://www.extremetech.com/extreme/184427-one-bitcoin-group-now-controls-51-of-total-mining-power-threatening-entire-currencys-safety>

- HUŘTÁK, Petr. *Analýza virtuální měny Bitcoin*. Praha, 2013. Bakalářská práce. Vysoká škola ekonomická v Praze. Vedoucí práce Ing. Radim Brixí.
- IBIT. *Bitcoin e-shop* [online]. [cit. 2015-12-18]. Dostupné z: <http://ibit.cz/>
- JACKSON, Ian. *Bitcoin Around the World: Germany* [online]. 2015 [cit. 2015-12-07]. Dostupné z: <http://insidebitcoins.com/news/bitcoin-around-the-world-germany/29737>
- JIROTKA, Tomáš. *Elektronický podpis pro začátečníky*. Digipodpis - odborník na elektronický podpis [online]. 2009 [cit. 2016-03-31]. Dostupné z: <http://www.digipodpis.cz/zaciname.php>
- KHAN, Samir. *Historical Gold and Silver Prices in Excel* [online]. 2015 [cit. 2015-12-26]. Dostupné z: <http://investexcel.net/historical-gold-silver-prices-excel/>
- KHAOSAN, Venzen. *Ecuador Bans Bitcoin In Favor Of Own National Cryptocurrency* [online]. 2014 [cit. 2016-05-04]. Dostupné z: <https://www.cryptocoinsnews.com/ecuador-bans-bitcoin-favor-own-national-cryptocurrency/>
- KLÍMA, Vlastimil. *Hašovací funkce, principy, příklady a kolize*. Cryptoworld [online], 2005 [cit. 2015-12-01]. Dostupný z: http://cryptoworld.info/klima/2005/cryptofest_2005.htm
- KUCCI. *LocalBitcoins.com* [online]. [cit. 2015-12-24]. Dostupné z: <https://localbitcoins.com/ad/133252/purchase-bitcoin-bank-cs-kb-airbank-ge-unicredit-fio-mbank-equa-czech-republic>
- Kurzovní lístek* [online]. [cit. 2015-12-22]. Dostupné z: <http://www.kurzy.cz/kurzy-men/kurzovni-listek/>
- LACIGA, Marek. *Jak výhodně koupit a prodat bitcoiny* [online]. 2015 [cit. 2015-12-18]. Dostupné z: <http://btctip.cz/jak-vyhodne-koupit-a-prodat-bitcoiny>
- LocalBitcoins. *Buy and sell bitcoins near you* [online]. [cit. 2016-05-10]. Dostupné z: <https://localbitcoins.com/>
- MÁLEK, Petr. *Bitcoin pro začátečníky*. Mises.cz [online]. 2013 [cit. 2016-05-02]. Dostupné z: <http://www.mises.cz/clanky/bitcoin-pro-zacatecniky-1014.aspx>
- MALONE, J. Anthony. *Glossary of Bitcoin Terms and Definitions*. NoHoMedia, 2015. ISBN 978-1-312984158
- NÁDENÍČEK, Petr. *Pravdy o elektronickém podpisu a šifrování*. Svět sítí [online], 2003 [cit. 2016-03-31]. Dostupné z: <http://www.svetsiti.cz/clanek.asp?cid=Pravdy-o-elektronickem-podpisu-a-sifrovani-3-digitalni-podpis--duveryhodna-komunikace-1952003>
- NAKAMOTO, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System*. Bitcoin [online], 2008 [cit. 2015-12-02]. Dostupné z: <https://bitcoin.org/bitcoin.pdf>
- NYDFS. *BitLicence* [online]. New York, 2015 [cit. 2016-05-03]. Dostupné z: <http://www.dfs.ny.gov/legal/regulations/adoptions/dfsp200t.pdf>

- PALMER, Daniel. *Bank of Thailand Suggests Bitcoin Not Illegal But Warns Against its Use* [online]. 2014 [cit. 2016-05-04]. Dostupné z: <http://www.coindesk.com/bank-thailand-says-bitcoin-illegal-warns-use/>
- PEREZ, Yessi Bello. *Bitcoin is Exempt from VAT, Rules European Court of Justice*. *Coindesk* [online]. 2015 [cit. 2016-05-02]. Dostupné z: <http://www.coindesk.com/bitcoin-is-exempt-from-vat-says-european-court-of-justice/>
- PHIL. *Legality of Bitcoin in Vietnam* [online]. 2015 [cit. 2016-05-04]. Dostupné z: <http://www.bitcoinvietnam.com.vn/blog/tinh-hop-phap-cua-bitcoin-tai-vietnam-legality-of-bitcoin-in-vietnam/>
- POLOUČEK, Stanislav a kol. *Peníze, banky, finanční trhy*. Praha: C. H. Beck, 2009. ISBN 978-80-7400-152-9
- PONSFORD, Matthew P. *A Comparative Analysis of Bitcoin and other Decentralized Virtual Currencies: Legal Regulation in the People's Republic of China, Canada, and the United States*. JOLT Digest [online]. [cit. 2015-12-13]. Dostupné z: <http://jolt.law.harvard.edu/digest/bitcoin/a-comparative-analysis-of-bitcoin-and-other-decentralized-virtual-currencies-legal-regulation-in-the-peoples-republic-of-china-canada-and-the-united-states>
- REJNUŠ, Oldřich. *Finanční trhy*. 4., aktualiz. a rozš. vyd. Praha: Grada, 2014, 760 s. Partners. ISBN 978-80-247-3671-6.
- RILEY, Charles a Sophia YAN. *China Bitcoin crackdown hits major exchange*. CNN-Money [online]. 2013 [cit. 2016-05-03]. Dostupné z: <http://money.cnn.com/2013/12/18/technology/bitcoin-china-exchange/>
- RIZZO, Pete. *Bolivia's Central Bank Bans Bitcoin* [online]. 2014 [cit. 2016-05-03]. Dostupné z: <http://www.coindesk.com/bolivias-central-bank-bans-bitcoin-digital-currencies/>
- ROJKO, Martin, Erik VORHEES, Simon DIXON, Vishal GUPTA a Michael SONNENSHEIN. *Expect Bitcoin Price to Reach US \$1,200 or More Next Year, Experts Say* [online]. 2015 [cit. 2016-05-09]. Dostupné z: <http://cointelegraph.com/news/expect-bitcoin-price-to-reach-us1200-or-more-next-year-experts-say>
- RUBICOIN. *Bitcoin směnárna* [online]. [cit. 2015-12-18]. Dostupné z: <http://www.rubico.in.cz/>
- SATOSHILABS. *TREZOR User Manual* [online]. [cit. 2016-05-05]. Dostupné z: https://doc.satoshilabs.com/trezor-user/advanced_features.html
- SCOTT, Allen. *Russian Ministry of Finance: Anti-Bitcoin Law 'Will Finally Be Passed This Year'*. Cointelegraph [online]. 2015 [cit. 2016-05-02]. Dostupné z: <http://cointelegraph.com/news/russian-ministry-of-finance-anti-bitcoin-law-will-finally-be-passed-this-year>
- SCHNEIER, Bruce. *Applied cryptography, second edition: protocols, algorithms, and source code in C*. New York: John Wiley, c1996. ISBN 04-711-1709-9.

- SIMPLECOIN. *Bitcoin směnárna* [online]. [cit. 2015-12-18]. Dostupné z: <http://www.simplecoin.cz/>
- SINGER, Miroslav. *Bezpečnost internetových plateb a virtuální „měny“ z pohledu ČNB* [online]. 2015 [cit. 2015-12-14]. Dostupné z: http://www.cnb.cz/miranda2/export/sites/www.cnb.cz/cs/verejnost/pro_media/konference_projevy/vystoupeni_projevy/download/singer_20150421_zlata_koruna.pdf
- SLÍŽEK, David. *Marek Palatinus: Pád Mt. Gox je pro bitcoin dobrá zpráva.* LUPA [online]. 2014 [cit. 2016-05-05]. Dostupné z: <http://www.lupa.cz/clanky/marek-palatinus-pad-mt-gox-je-pro-bitcoin-dobra-zprava/>
- STROUKAL, Dominik. *Kryptoměna bitcoin se v Rusku stala veřejným nepřítelem.* Ekonomický deník [online]. 2015 [cit. 2016-05-02]. Dostupné z: <http://ekonomicky-denik.cz/kryptomena-bitcoin-se-v-rusku-stala-verejnym-nepritelem/>
- STUDÝNKA, Bohumil a Jan STRUŽ. *Zlato: příběh neobyčejného kovu. 2., aktualiz. a dopl. vyd.* Praha: Grada, 2014, 344 s. ISBN 978-80-247-5210-5.
- SUBREG. [online]. [cit. 2015-12-18]. Dostupné z: <http://subreg.cz/>
- The bitcoin volatility index* [online]. [cit. 2015-12-20]. Dostupné z: <https://btcvol.info/>
- VBTC. *Sàn giao dịch Bitcoin lớn nhất Việt Nam* [online]. [cit. 2015-12-18]. Dostupné z: <https://vbtc.vn/>
- Velikost blockchainu* [online]. [cit. 2015-12-10]. Dostupné z: <https://blockchain.info/charts/blocks-size>
- VENCL, Jiří. *Vývoj ceny zlata v roce 2013: Zlato uzavírá nejhorší rok* [online]. 2013 [cit. 2015-12-29]. Dostupné z: <http://www.tradeportal.cz/aktualni-prilezitosti/vyvoj-ceny-zlata-v-roce-2013-zlato-uzavira-nejhorsirok.html>
- VÍTEK. *Technologie těžení bitcoinů* [online]. 2012 [cit. 2015-12-18]. Dostupné z: <http://blog.bitcoin.cz/2012/09/technologie-tezeni-bitcoinu/>
- Vývoj kurzu USD/BTC* [online]. 2016 [cit. 2016-05-05]. Dostupné z: https://blockchain.info/charts/market-price?timespan=all&showDataPoints=false&daysAverageString=1&show_header=true&scale=0&address
- WESTERN UNION. *Poplatky* [online]. [cit. 2015-12-18]. Dostupné z: <http://www.intercash.cz/poplatky.asp>
- WESTERN UNION. *Profil společnosti* [online]. [cit. 2015-12-18]. Dostupné z: <http://www.intercash.cz/profil-spolecnosti.asp>
- WILCOX, Devon. *Bitcoin Beginner's Guide: Everything You Need To Know To Become Rich With Bitcoins.* ClydeBank Media, 2015. ISBN 978-1500644383.

YOUNG, Joseph. *Top Bitcoin Wallets 2016* [online]. NEWSBTC 2015 [cit. 2016-05-05]. Dostupné z: <http://www.newsbtc.com/2015/11/30/most-secure-bitcoin-wallets-2016/>

ZDRAŽIL, Tomáš. *Zlato: Vyplatí se do něj investovat?* Investree [online]. 2015 [cit. 2015-12-30]. Dostupné z: <http://investree.cz/zlato-vyplati-se-do-nej-investovat/>

Seznam bank a jejich poplatků

ČESKÁ SPOŘITELNA. *Ceník pro zahraniční platební styk pro soukromou klientelu* [online]. 2015 [cit. 2015-12-21]. Dostupné z: <http://www.csas.cz/banka/nav/osobni-finance/zahranicni-platebni-styk-d00022725>

ČESKÁ SPOŘITELNA. *Informace České spořitelny, a. s.: K platebním službám* [online]. 2015 [cit. 2015-12-21]. Dostupné z: http://www.csas.cz/static_internet/cs/Komunikace/Otevrena_komunikace/Ostatni/Prilohy/informace_o_platebnich_sluzbach_21.10.2015_cz.pdf

ČSOB. *Obchodní podmínky pro účty a platební styk* [online]. 2015 [cit. 2015-12-21]. Dostupné z: <https://www.csob.cz/portal/documents/10710/174462/obchodni-podminky-pro-ucty-a-platebni-styk.pdf>

EXPOBANK. *Standardní sazebník odměn a poplatků pro osobní bankovníctví* [online]. 2015 [cit. 2015-12-21]. Dostupné z: <https://www.expobank.cz/wp-content/uploads/2015/07/expobank-sazebnik-osobni-20150701.pdf>

EXPOBANK. *Podmínky pro provádění platebního styku Expobank CZ a.s.* [online]. 2015 [cit. 2015-12-21]. Dostupné z: <https://www.expobank.cz/wp-content/uploads/2015/06/expobank-podminky-pro-provadeni-platebniho-styku-20140110.pdf>

FIO BANKA. *Ceník finančních operací a služeb pro fyzické a právnické osoby* [online]. 2015 [cit. 2015-12-21]. Dostupné z: http://www.fio.cz/docs/cz/cenik_bankovni_sluzby.pdf

FIO BANKA. *Informace o obecných podmínkách pro provádění převodů peněžních prostředků, typech podporovaných plateb a lhůtách zúčtování* [online]. 2015 [cit. 2015-12-21]. Dostupné z: http://www.fio.cz/docs/cz/Informace_prevody.pdf

GE MONEY BANK. *Sazebník poplatků za produkty a služby pro fyzické osoby nepodnikatele* [online]. 2015 [cit. 2015-12-21]. Dostupné z: <https://legacy.gemoney.cz/documents/cz/sazebniky-uroky/1595.pdf>

GE MONEY BANK. *Základní produktové podmínky běžného účtu a Základní produktové podmínky platebního styku* [online]. 2015 [cit. 2015-12-21]. Dostupné z: <https://www.gemoney.cz/documents/10667/1394026/gemb-pp-bu-ppps-2015-12-01.pdf/2b24e3b9-6a87-43a6-b75d-b0185a9b733e>

- KOMERČNÍ BANKA. *Úhrady v tuzemsku, ze a do zahraničí* [online]. 2015 [cit. 2015-12-21]. Dostupné z: <http://www.sazebnik-kb.cz/cs/obcane/platebni-styk/uh rady-v-tuzemsku-ze-a-do-zahranici.shtml>
- KOMERČNÍ BANKA. *Časy pro přijetí a zpracování zahraničních plateb, a.s.* [online]. 2015 [cit. 2015-12-21]. Dostupné z: <http://www.kb.cz/file/cs/obcane/dokumenty-ke-stazeni/kb-lhuty-zuctovani-zahranicnich-plateb.pdf?201506>
- MBANK. *Sazebník bankovních poplatků mBank* [online]. 2015 [cit. 2015-12-21]. Dostupné z: http://www.mbank.cz/informace-k-produktum/sazebnik/osobni-finance/Sazebnik_mBank_CZ_2015_03_01.pdf
- MBANK. *Všeobecné obchodní podmínky pro zakládání a vedení účtů fyzických osob* [online]. [cit. 2015-12-21]. 2015 Dostupné z: <http://www.mbank.cz/informace-k-produktum/obchodni-podminky/vseobecne-podminky-fyzicke-osoby.pdf>
- AGRIBANK. *Dịch vụ chuyển tiền ra nước ngoài qua hệ thống ngân hàng* [online]. 2010 [cit. 2015-12-21]. Dostupné z: <http://www.agribank.com.vn/61/995/khach-hang-ca-nhan/dich-vu-chuyen-tien/dich-vu-chuyen-tien-ra-nuoc-ngoai-qua-he-thong-ngan-hang.aspx>
- EQUA BANK. *Podmínky platebního styku* [online]. 2015 [cit. 2015-12-21]. Dostupné z: <https://www.equabank.cz/files/doc/353-podminky-platebniho-styku-010114-1.pdf>
- Banky v ČR* [online]. [cit. 2015-12-21]. Dostupné z: <http://www.banky.cz/prehled-bank>
- AIR BANK. *Ceník a poplatky* [online]. 2015 [cit. 2015-12-21]. Dostupné z: <https://www.airbank.cz/cs/bezny-ucet/cenik-a-poplatky/cenik/>
- AIR BANK. *Obchodní poplatky* [online]. 2015 [cit. 2015-12-21]. Dostupné z: <https://www.airbank.cz/cs/vse-o-air-bank/dokumenty/pro-uzivatele/obchodni-podminky/Contents/0/FF8E0C93B3D71382C10983EE77B59931/resource.pdf>
- CITI BANK. *Informační leták* [online]. 2015 [cit. 2015-12-21]. Dostupné z: http://www.citibank.cz/czech/gcb/corporate_banking/czech/pdf/Informacni_letak_2015.pdf
- CITI BANK. *Sazebník poplatků* [online]. 2015 [cit. 2015-12-21]. Dostupné z: http://www.citibank.cz/czech/gcb/corporate_banking/czech/pdf/Sazebnik_poplatku_2015.pdf
- ČSOB. *Zahraniční platby: Sazebník* [online]. 2015 [cit. 2015-12-21]. Dostupné z: <https://www.csob.cz/portal/podnikatele-firmy-a-instituce/produkty/ucty-a-platebni-styk/zahranicni-platby#sazebnik>
- EQUA BANK. *Sazebník – účty* [online]. 2015 [cit. 2015-12-21]. Dostupné z: <https://www.equabank.cz/files/doc/738-cz-sazebnik-ucty-03102015.pdf>

- SBERBANK. *Sazebník poplatků* [online]. 2015 [cit. 2015-12-21]. Dostupné z: <https://www.sberbankcz.cz/sazebnik>
- SBERBANK. *Obchodní podmínky* [online]. 2015 [cit. 2015-12-21]. Dostupné z: <https://www.sberbankcz.cz/o-bance/obchodni-podminky>
- UNICREDIT BANK. *Sazebníky* [online]. 2015 [cit. 2015-12-21]. Dostupné z: https://www.unicreditbank.cz/content/dam/cee2020-pws-cz/cz-dokumenty/dokumenty-produkty/sazebniky/Sazebnik_CZ_retail_IND_02_2016.pdf
- DONGABANK. *Thanh toán quốc tế* [online]. [cit. 2015-12-21]. Dostupné z: <http://www.dongabank.com.vn/service/128>
- OCB. *Dịch vụ chuyển tiền quốc tế* [online]. 2014 [cit. 2015-12-21]. Dostupné z: <http://www.ocb.com.vn/vi-VN/Khach-hang-ca-nhan/Bieu-phi/Dich-vu-chuyen-tien-quoc-te.htm#.VnXDAct61if>
- VIETCOMBANK. *Biểu phí* [online]. 2009 [cit. 2015-12-21]. Dostupné z: <http://www.vietcombank.com.vn/Personal/OnlineBanking/Bieu%20phi%20KHCN.%20update%2013012014.pdf?21>
- EXIMBANK. *Biểu phí nhận tiền kiều hối* [online]. [cit. 2015-12-21]. Dostupné z: https://www.eximbank.com.vn/home/static/cn_bieuphi_nhantienkieuhoi.aspx
- ACB. *Biểu phí* [online]. [cit. 2015-12-21]. Dostupné z: <http://acb.com.vn/wps/portal/Home/fee>
- LIENVIETPOSTBANK. *Biểu phí* [online]. [cit. 2015-12-21]. Dostupné z: http://www.lienvietpostbank.com.vn/sites/default/files/file_download/Bieu_phi_KHCN.pdf