Univerzita Hradec Králové
Fakulta informatiky a managementu
Katedra informatiky a kvantitativnich metod

Kryptoměny

Bakalářská práce

Autor: Mikoláš Zítko
Studijni obor: Informační management

Vedoucí prace: Ing. Monika Borkovcová

Hradec Králové Duben 2015

Prohlášení:

Prohlašuji, že jsem bakalářskou práci zpracoval samostatně a s použitím uvedené literatury.

Podpis

V Hradci Králové dne Jméno a příjmení

Poděkování

Rád bych poděkovat Ing. Monice Borkovcové za odborné rady, trpělivost, a především čas věnovaný vedení této práce.

Anotace

Bakalářská práce se zaměřuje na kryptoměny. Nejvíce prostoru je věnováno Bitcoinu, který je nejvyužívanější kryptoměnou. Teoretická část postupně popisuje základy kryptografie, systém fungování kryptoměn a další prvky související s kryptoměnami. V této části je také věnován prostor pro současný legislativní pohled na kryptoměny. Praktická část je zaměřena výhradně na Bitcoin a klade za cíl prozkoumat parametry a využití kryptoměn. Jsou zde porovnány různé vlastnosti a souvislosti, které mohou ovlivňovat Bitcoin. Z hlediska využití jsou kromě klasických burz, kde se obchodují bitcoiny s různými světovými měnami, analyzovány také ilegální tržiště a další možnosti užití Bitcoinu pro nelegální účely.

Annotation

Title: Cryptocurrency

This bachelor thesis deals with a topic of cryptocurrency. The thesis deals mostly with a Bitcoin, which is the most used cryptocurrency. The theoretical part describes gradually the basics of cryptography, the system of functioning of cryptocurrency and other elements related to them. This part also deals with an issue of current legislative attitude to cryptocurrency. The practical part is focused specifically on Bitcoin and main aim is to explore the parameters and the use of cryptocurrency. There are compared various attributes and connections, which can influence Bitcoin. Regarding the use there are common stock markets where is doing trade with bitcoins for various world currcencies, but there are also analysed illegal markets and other options for the use of Bitcoin for illegal aims.

Obsah

Úvod

Bakalářská práce je věnována poměrně aktuálnímu tématu kryptoměn. Kryptoměny jsou forma digitálně vytvářených platidel s řadou odlišností oproti klasickým měnám. Toto téma je v současnosti velmi aktuální a využívání kryptoměn se stále rozšiřuje. Jelikož první kryptoměna bitcoin byla vytvořena teprve před přibližně pěti lety, jedná se o velmi mladý projekt, ale na druhou stranu s každým přibývajícím rokem je mnohem využívanější a populárnější. Kryptoměny s bitcoinem v čele se vyznačují přímými a levnými transakcemi od uživatele k uživateli. Tyto transakce v dnešní době slouží nejen k nákupu v internetových obchodech, ale například ve Spojených státech se již rozrůstá sít bankomatů, bitcoiny je také možné využít například k platbě za kávu v řetězci Starbucks. Bitcoiny je tak možné využít k placení i na místech, kde by většina uživatelů ještě před pár lety nevěřila, že se kdy rozšíří.

Kromě kryptoměn existuje řada jiných možností pro placení na internetu. Společnosti jako PaayPal a další nabízejí pouze zprostředkování a finance jsou drženy v klasických měnách, jako jsou například dolary. Další společnosti nabízejí určitou formu digitálních peněz, ale ta je využitelná pouze u dané společnosti. Bitcoin a další kryptoměny, však vytvářejí vlastní formu mincí, který má, jak je vidět, určitou hodnotu a je s nimi možno zaplatit komukoli, kdo si zařídí speciální peněženku. Kromě platebních možností, je mechanismus ověřování plateb založený na řadě uživatelů, také možné využít k dalším účelům, jako je ověřování dokumentů a dalších odlišných způsobů.

V současnosti, je možné v řadě odvětví, pozorovat nárůst významu společností nabízejících decentralizované služby, neboli služby, které nejsou provozovány jedním subjektem. Takovéto služby mají zpravidla značnou uživatelskou základnu, která zajišťuje fungování služby. Řada výrobců nabízí své výrobky napřímo bez pomoci obchodníků. Další služby fungující na bázi mnoha uživatelů, nabízejí pronájem či sdílení aut nebo pokojů. Bitcoin a další kryptoměny jsou také příkladem decentralizovaného principu. Jsou také založena na síti tvořené množstvím uživatelů, kteří zabezpečují fungování celého systému, bez potřeby a také možnosti centrálních regulací. Toto téma jsem si vybral, protože myšlenka možnosti vytvoření peněz, které nebudou závislé na státu,mi přišla velmi zajímavá.

Cílem teoretické části práce je seznámit čtenáře se základními principy a systémem fungování kryptoměn. Tato část tak bude postupně pokrývat základní principy kryptografie, které jsou nutné pro pochopení určitých funkcí, které využívají kryptoměny. Následně se bude věnovat celému systému fungování, vlastnostem a dalším souvisejícím informacím. V neposlední řadě bude představen současný pohled na kryptoměny z hlediska legislativy.

Praktická část si klade několik podcílů.

U nejstarší měny, Bitcoinu se jedná o pouze pět let starý projekt, který již zažil značné cenové výkyvy. Kryptoměny se vyznačují nemožnostmi přímé regulace ceny ze strany vlád a centrálních institucí. Také mají značné problémy s různými snahami vlád o zákaz, zdanění či jinou regulaci. Prvním cílem porovnání parametrů kryptoměn s oficiálními měnami.

Dalším podcílem je prozkoumání cenových vlivů dopadajících na kryptoměny. Tyto měny se v mnohém odlišují od standarního chápaní peněz a je tedy možné se domnívat, že také cenové vlivy budou jiné než u klasických měn. V této části budou porovnány možnosti vlivu rozšířenosti kryptoměn, oblíbenosti a dalších podobných aspektů na cenu. V této části bude také věnován prostor finančním burzám. Přesto již existuje řada společností, které se umožňují obchodování bitcoinů a dalších kryptoměn za ostatní klasické měny. V této části tak budou také porovnány možnosti obchodování které tyto burzy nabízejí.

Třetím a posledním podcílem je analýza ilegálního využití kryptoměn. Vzhledem k tomu, že vystopování transakcí u kryptoměn je náročné, jsou často využívány pro ilegální účely. Jedná se především o černé trhy a další podobné využití.

Vzhledem k povaze tématu, které je stále relativně nové, v češtině není moc dostupné literatury, ze které by bylo možné čerpat.Téměř všechny zdroje jak literatura, tak i internetové zdroje jsou tak anglické. U internetových zdrojů jsem se vždy snažil ověřit informaci na více zdrojích a také ověřit autora. Většina citovaných zdrojů je vždy od konkrétních autorů, kteří se tématem zabývají, nebo od předních webových portálů věnovaných kryptografickým měnám. U knižních zdrojů jsem čerpal od renomovaných autorů. Simon Singh, od kterého autor čerpal především pro část věnovanou kryptografii, se dlouhodobě věnuje psaní knih s matematickou tématikou. Andreas M. Antopulos je velmi uznávaným odborníkem přes bitcoin, Jose Pagliery se dlouhodobě věnuje psaní o kyberbezpečnosti a soukromí a podobně.

1 Kryptografie

Celý systém fungování kryptoměn, staví na principech a funkcích kryptografie. Kryptografie zajišťuje bezpečnost a samotné fungování kryptoměn. Využívané funkce jsou velmi složité, a proto v následujícím textu budou uvedeny pouze základní pojmy z kryptografie související se jednotlivými principy kryptoměn a také jednotlivé vývojové etapy kryptografie vedoucí k vytvoření systému, který využívají kryptoměny.

Cílem kryptografie je zajištění bezpečné komunikace mezi subjekty, tak aby nedošlo k vyzrazení přenášených informací třetí straně. Hála, V. [67] definuje kryptografii jako vědu, která se zabývá utajováním tím, že je převádí do podoby, čitelné jen s určitou speciální znalostí. Jak dodává Hála [67] slovo kryptografie vychází ze spojení řeckých slov kryptós - skrytý a gráphein- psát. Někdy je pojem obecněji používán pro vědu o čemkoli spojeném se šiframi a je také alternativou k pojmu kryptologie

Pro pohodlné využívání jakýchkoliv platidel je potřeba řada vlastností. Platby musí být dostatečně bezpečné, aby nebylo jednoduché uživatele oklamat. Placení by mělo být dostatečně rychlé a nemělo by být složité. V případě klasických měn tyto vlastnosti zajišťují banky, které zabezpečují jednotlivé platby. Bez důvěryhodné třetí strany je však potřeba vyřešit řadu problémů.

1.1 Distribuce šifrovacích klíčů

Kryptografie jako taková od začátku narážela na zásadní problém a to s distribucí samotných šifrovacích klíčů. Podle Singha, S. [6], je problémem princip dešifrovacího klíče, který je velmi složité bezpečně předat druhé straně bez vyzrazení. Podle Singha, S. [6], tak vždy než mohou dva lidé sdílet zašifrovanou zprávu, musí sdílet klíč. Takovýto systém je však pro využití nepohodlný, doprava klíče je složitá a není dostatečně bezpečná. Vzhledem k riziku, je také potřeba často měnit dešifrovací klíče.

Problém s distribucí dešifrovacích klíčů přetrvával v kryptografii až do roku 1976, kdy jako první přišli s částečným řešením tohoto problému matematici Martin Hellman a Bailey Diffie, kteří se zabývali jednosměrnými funkcemi a modulární aritmetikou.

1.1.1 Jednosměrné funkce

Matematické funkce je možné rozlišovat na obousměrné a jednosměrné. Jak uvádí Singh, S. [6] :*„většina funkcí je obousměrných a lze je provést v jednom i druhém směru. Tudíž obousměrná funkce je funkce, jejíž jeden stav lze snadno vrátit do stavu původního.“* Příkladem velmi jednoduché obousměrné funkce může být třeba násobení či dělení. Příkladem elementární funkce je například y=10x. I když využité číslo x není známo, lze se velice snadno dopočítat původního čísla, pouze se znalostí výsledeku a využité funkce.

Protikladem obousměrných funkcí jsou jednosměrné funkce. Klíma, V. [79] popisuje jednosměrné funkce jako takové funkce, u kterých je snadné vypočítat výslednou hodnotu, ale postup obrátit a vypočítat z výsledné hodnotypůvodní je velmi složité až nemožné. Pro lepší představu jak fungují jednosměrné funkce, dodává Klíma, V. [79] příklad :*„Je to třeba 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.“*

1.1.2 Modulární aritmetika.

Jak popisuje Bogomolny, A. [29] Modulární aritmetika je neobvykle univerzální nástroj objevený K. F Gaussem roku 1801. V nejjednodušší formě se jedná o aritmetiku s počtem, který se vynuluje pokaždé, když je dosaženo nějakého celého čísla N, většího než jedna. Toto číslo je známé jako modulus (mod). Modulus tedy značí zbytek po celočíselném dělení.

Například:

1. 10 mod 5 = 0
2. 11 mod 5 = 1

Na výhody pocházející z nevyzpytatelnosti funkcí v modulární aritmetice upozorňuje Singh, S. [6]. Právě díky této vlastnosti jsou funkce v modulární aritmetice jednosměrné. Singh, S. Uvádí příklad jednosměrné funkce v modulární aritmetice:*„Výpočet funkce Mod 5 6093 je velmi jednoduchý, ale naopak zjištění původní hodnoty z výsledku je velmi složité. Jediný způsob jak invertovat funkci v modulární aritmetice často spočívá v sestavení tabulky funkcích hodnot pro mnoho hodnot x.“* V modulární aritmetice i se znalostí funkce, která byla využita, nelze snadno vypočítat původní hodnotu. Nejvýrazněji je možné pozorovat rozdíly v porovnání s funkcí z normální aritmetiky, například funkce 3^x. Tato funkce při zvyšující se

proměnné x zvyšuje i výslednou hodnotu. Naproti tomu u funkce 3^x (mod 7) je výsledná hodnota nepředvídatelná a není tedy možné odhadnout její hodnotu.

X	1	2	3	4	5	6
3^x	3	9	27	81	243	729
3^x (mod 7)	3	2	6	4	5	1

Tabulka 1 Nevyzpytatelnost modulární aritmetiky. Zdroj: Singh, S. [6]

Následující tabulka č. 2 uvádí, jak je možné pomocí funkce Y^x (mod P) ustanovit dešifrovací klíč, aniž by se musel odesílat. Uživatelé si zvolí dvě čísla Y a P, která tvoří funkci. Tyto čísla musí splňovat podmínku, že Y musí být menší než P. Tato dvě čísla, stejně jako hodnotu funkce si mohou sdělit veřejně, a přesto ustanovit dešifrovací klíč.

Krok	Alice	Bob
Dohodnutí se na Y a P	Y = 7, P = 11	Y = 7, P = 11
Zvolení tajného čísla (x)	3	6
Vypočítání funkce Y^x(mod P)	7^3(mod 11) = 2	7^6(mod 11) = 4
Odeslání tohoto výsledku druhé osobě (z)	Obdrží 4	Obdrží 2
Vypočítání klíče pomocí původního čísla x a funkce z^x(mod P)	4^3(mod 11) = 9	2^6(mod 11) = 9
Oba dospěli ke stejnému číslu – dešifrovacímu klíči	9	9

Tabulka 2 Jednosměrná funkce Y^x(mod P). zdroj Singh, S. [6], upraveno

1.1.3 Veřejný klíč

Předchozí systém představoval takzvané symetrické šifrování, neboli šifrování kdy mají oba účastníci stejný dešifrovací klíč. Tato metoda sice umožňuje bezpečnou komunikaci, ale neřeší veškeré problémy. Jak uvádí Singh, S. [6], je nutné, aby oba účastníci odeslali svoji část klíče, což je nepohodlné. Skutečným řešením problémů s distribucí klíčů je tak až asymetrická šifra, u které má každý uživatel jiný klíč.

V asymetrické šifře se využívá dvou klíčů, veřejného a privátního. Jak popisuje Mička, P. [88], veřejný klíč může být dostupný komukoliv, zatímco druhý, privátní klíč musí být uschován. Pomocí veřejného klíče se zprávy zašifrují, ale dešifrovat je lze pouze s příslušným soukromým klíčem.

Příkladem asymetrické šifry je Algoritmus RSA (Rivest, Shamir, Adleman) podle Mičky, P. [88] :*„…jedná se o asymetrickou šifru, která je založena na Eulerově větě, a která je použitelná jak pro šifrování, tak pro podepisování dokumentů.“*

Pro lepší zabezpečení, však Bitcoin využívá kryptografii založenou na eliptických křivkách nebo-li ECDSA (Elliptic Curve Digital Signature Algorithm). Tento algoritmus je při stejných délkách klíčů, mnohem bezpečnější než předchozí zmíněná RSA. Podle Sullivana, N. [106] poskytuje 256bitový klíč eliptické křivky stejnou úroveň bezpečnosti jako 3,248-bitový klíč RSA.

Podle Singha, S. [6] tak asymetrická šifra řeší problém s distribucí klíčů. Dva uživatelé tak mohou díky veřejnému šifrovacímu klíči bezpečně komunikovat. Veřejný klíč je jedním ze základních principů, na kterém staví Bitcoin a jiné kryptografické měny.

1.2 Hash funkce

Dalším prvkem využívaným v systému Bitcoinu jsou takzvané hash funkce. Jak popisuje Jansen, C. [77] jedná se o funkce, které z libovolně velké skupiny znaků utvoří projekci s pevně danou délkou - hash. Jansen, C.[77] dodává, že je téměř nemožné zjistit původní data, pokud je známa pouze výsledná hodnota hash funkce. Dalším významným znakem hash funkcí je, že drobná změna vstupních dat vyvolá značnou změnu výsledku.

Hash funkce se také používají k rychlejšímu prohledávání tabulek, nebo pro porovnávání dat – například pro hledání položek v databázi, odhalování duplicitních záznamů ve velkém souboru. Pro potřeby Bitcoinu je dvakrát využívána hash funkce SHA-256, u které podle Ošťádala, R. [92], nebyly zatím nalezeny žádné bezpečnostní problémy. Hodnotu SHA-256 je možné vypočítat například na webové službě Xorbin[113].
Níže je vidět jak drobný rozdíl ve změně jednoho písmena vstupního textu, vyvolá velmi velký rozdíl ve výstupu.

Vstupní data:

> Lorem ipsum dolor sit amet, consectetur adipiscing elit. Integer vel auctor nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Donec lacus purus, venenatis eget lacinia ac, iaculis quis purus.

Výstup SHA-256

> 92d7182777b9cf14e8d1b346d13c20d20f9cf9c49e0e4ee9a4b606f1660e3bb8

Vstupní data:

> **M**orem ipsum dolor sit amet, consectetur adipiscing elit. Integer vel auctor nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Donec lacus purus, venenatis eget lacinia ac, iaculis quis purus.

Výstup SHA-256

> 0c944488fdf201584496214a98447bb3919a979df0650a02f47a540808ef080d

2 Bitcoin

Bitcoin je první digitální měna a platební systém postavený na kryptografických principech a funkcích. Antonopoulos, A. [1] popisuje, že se jedná se o decentralizovanou kryptoměnu, kompletně vytvářenou a drženou elektronicky. V systému představuje Bitcoin samotné principy systému - Peer to peer síť, ve které jednotlivé uzly zaznamenávají jednotlivé transakce. Naproti tomu bitcoin představuje jednotlivé mince. Zkratkou měny je BTC. Celý systém funguje na bázi sítě uživatelů, nové mince jsou uvolňovány těm z nich, kteří využívají výpočetní sílu svých počítačů nebo specializovaného hardware, k ověřování transakcí mezi ostatními uživateli.

2.1 Historie

Podle webové stránky Historyofbitcoin [72] je Bitcoin první decentralizovanou kryptoměnou. Byl stvořen osobou, nebo osobami skrývajícími se pod pseudonymem Satoshi Nakamoto. První krok ke stvoření sahá již do roku 2008, kdy byl publikován teoretický základ nazvaný Bitcoin: A Peer-to-Peer Electronic Cash System. Nakamoto, S. [103] popisuje, že důvodem pro vytvoření Bitcoinu, bylo umožnění obchodovat přímo mezi uživateli, bez využití třetí strany. Dále se zaměřuje na nevýhody vyplívající ze samotného fungovaní finančních institucí. Banky jako důvěryhodní prostředníci si účtují za zprostředkování plateb mezi stranami poplatky a vzhledem k výši těchto poplatků, tak není pro uživatele výhodné provádět malé transakce.

Představa fungování Bitcoinu je založena na uživatelích, kteří propůjčí své počítače pro zajištění funkčnosti systému. Budou, ověřovat transakce a zároveň uvolňovat nové mince do oběhu. Základním prvkem bude takzvaný blockchain, který bude sdružovat ověřené transakce přidávat je do bloků a řadit za sebe. Celý systém, jak popisuje Nakamoto, S. [103], bude veřejný a bude zahrnovat veškeré záznamy o ověřených transakcích a nově uvolněných mincích. Díky tomuto systému nebude potřeba využívat důvěryhodných třetích stran a uživatelé budou moci vzájemně posílat libovlně velké transakce přímo cílovému subjektu. Zároveň také přichází s opatřením, které by teoreticky mělo omezit či zabránit inflaci, jedná se o celkové množství peněz, které dosáhne přesně stanoveného množství. Jak upozorňuje, Pagliery, J. [4], filosofie systému staví na osobní odpovědnosti – díky přístupu, který

nevyužívá důvěryhodnou třetí stranu, jsou platby nevratné, pokud se je uživatelé nerozhodnou poslat zpět.

Jak uvádí Pagliery, J. [4], historie tohoto projektu sahá až do Ledna roku 2009, kdy byla uvolněna první použitelná verze Bitcoinového klienta. V této první verzi byla také nastavena vrchní hranice mincí v oběhu na téměř 21 milionů kusů. Z počátku byla těžba bitcoinů velmi snadná a dala se zvládnout i standardním domácím počítačem. Byla však nastavena tak, aby se s postupem času stávala čím dál složitější. V dnešní době je sice stále možné vytěžit bitcoin s normální sestavou, ale cena spotřebované energie bude výrazně vyšší, než hodnota takto získaných bitcoinů. Efektivní těžení bitcoinů, bez specializovaného hardware, je prakticky vyloučeno. Postupem času se k projektu připojovalo stále více vývojářů a Nakamoto roku 2011 předal projekt Gavinu Andresenovi, aby se tak vzdal vývoje.

Během prvních dvou a půl let existence se z neznámého kryptografického projektu stala malá internetová měna. Za tuto změnu vděčí především online službám, kde uživatelé mohli nakupovat a prodávat bitcoiny za standardní peníze. První z těchto směnáren byl Bitcoinmarket.com následovaný MT.gox. Jak dodává Pagliery, J. [4], začátky byly velmi problematické a plné stížností uživatelů na podvody, přesto však ještě toho roku dosáhl objem obchodovaných bitcoinů přibližně jednoho milion dolarů.

Od svého založení zažil Bitcoin nejen obrovský nárůst popularity, ale také strmé pády. Níže jsou pro větší přehlednost uvedeny významné události v historii Bitcoinu.

2.2 Časová osa historie Bitcoinu

2008

18. Srpen
Zaregistrování webové domény Bitcoin.org.

9. Říjen
Registrace projektu na SourceForge.net.

2009

9. Leden
Vydání verze 0.1. V této verzi bylo zahrnuto, že celkem bude vytvořeno 21 milionu bitcoinů.

12. Leden
První transakce, zahrnutá v bloku 170 provedena mezi uživateli Satoshi a Hal Finney

5. Říjen
Ohodnocení bitcoinu v porovnání s americkým dolarem 1 USD = 1 309,03 BTC. Ohodnocení bylo provedeno podle ceny elektřiny nutné k provozu počítače, který generoval bitcoiny.

2010

17. Červen
Založení směnárny MtGox.

18. Září
Slush's Pool vytěžil první blok přes sdruženou těžbu. Jedná se o metodu, která umožňuje spojení více jednotlivců.

Říjen
Finanční pracovní skupina (FATF) varuje před možností, že digitální měny jsou využívány pro financování teroristických skupin.

8. Prosinec
První mobilní transakce.

2011

28. Leden
Vytvořeno 25% z celkového množství bitcoinů.

9. Únor
Dosažení parity s americkým dolarem. Hodnota bitcoinu se poprvé dostala na 1 USD/BTC.

27. Březen
Otevření Britcoinu první služby pro výměnu bitcoinů za Britské libry.

2. Červen
Cena stoupá na 10 USD/BTC na Mtgox.com.

2012

15. Listopad
WordPress.com začíná přijímat Bitcoin.

2013

Duben
Hodnota Bitcoinu ve směnárnách stoupá na 100 USD/BTC.

2. Květen 2
První bankomat využívající bitcoiny zprovozněn v San Diegu v Kalifornii.

18. Květen 18
Založení online kasina primedice.com, využívajícího Bitcoin.

2. Říjen 2
FBI Zavírá Silk RoadFBI a zabavuje bitcoiny v celkové hodnotě přes 3,6 milionu dolarů.

19. Listopad
Více transakcí poslaných pomocí bitcoinů než přes Western Union.

2014

3. Červenec
Apple povoluje bitcoin aplikaci v obchodě applestore.com.

18. Červenec
Dell začíná přijímat platby bitcoinem.

14. Říjen
Burza Coinbase získává investici 50 milionů dolarů.

11. Prosinec
Microsoft začíná přijímat platby Bitcoinem.

2.3 Princip funkce

Celý princip fungování Bitcoinového systému je odlišný od normálních forem peněz. V případě Amerického dolaru, Eura či dalších podobných měn existují fyzické formy mincí, kterými lze platit a v případě bankovního konta je vždy ukládána aktuální hodnota účtu. Jak uvádí Antonopoulos, A [1], u Bitcoinu však žádné fyzické mince neexistují a nejsou reprezentovány ani digitálním souborem, který by uchovával jejich hodnotu.

Veškeré transakce se však zapisují do veřejně dostupné knihy a celkový zůstatek konta u Bitcoinu je vypočítáván jako rozdíl přijatých a odeslaných transakcí.

Princip fungování staví na kryptografických funkcích, veřejně dostupných transakcích a na takzvaném těžení, které slouží pro ověřování transakcí.

2.3.1 Veřejný a privátní klíč

Pro využívání Bitcoinu jsou potřeba 2 matematicky provázané klíče. První je privátní a slouží k podepisování transakcí. Druhý je veřejný a umožňuje ostatním ověřit, že uživatel skutečně vlastní privátní klíče, bez jejich vyzrazení. Zároveň slouží jako adresa, na kterou je možné uživateli poslat bitcoiny.

2.3.2 Transakce

Pro převádění peněz mezi uživateli slouží transakce. Uživatel zvolí adresu, množství peněz a poté je nutné transakci zabezpečit digitálním podpisem. Pro vytvoření digitálního podpisu se využívá privátní klíč. Jak uvádí Moreno, M. [89], tento klíč je 256bitové číslo, které je přiřazené právě jedné adrese a slouží pouze uživateli, jenž vlastní tuto adresu. Pomocí matematické funkce, která využívá privátní klíč a údaje o transakci se vytváří digitální podpis, který odlišný pro každou transakci.

Driscoll, S. [54] uvádí, že pro ověření pravosti transakce je nutné zjistit, zda uživatel má práva využívat adresu, ze které posílá peníze. K tomuto se využije složité matematické funkce, která využije data transakce, veřejný klíč a digitální podpis pro ověření, že uživatel skutečně vlastní pravý privátní klíč. To vše se děje bez vyzrazení privátního klíče. Po potvrzení je transakce odeslána do Bitcoinové sítě a čeká na přijmutí. Pro ověření, že uživatel opravdu vlastnil mince, které plánuje utratit, musí dokázat, že je skutečně vlastnil. Jak uvádí Driscoll, S. [89], pokud chce Alice poslat 5 BTC Bobovi, musí odkázat na ostatní transakce, během kterých obdržela 5 nebo více BTC. Takto odkázané transakce se nazývají vstupy. Ostatní uzly v síti

pak mohou využít tyto transakce a ověřit tak, že Alice skutečně vlastnila 5 nebo více bitcionů a smí je tedy utratit.

2.3.3 Těžení

Jak již bylo uvedeno systém Bitcoinu funguje na principu veřejných transakcí, ze kterých se vypočítává celkový zůstatek. Aby bylo možné takto kontrolovat jednotlivé platné transakce, musí být někde zaznamenávány. Proces rozhodování, které transakce budou zapsány, a které nikoliv, se nazývá těžení. Do těžení se může zapojit každý uživatel, takový to uživatel se nazývá miner neboli těžař. Težaři přidávají transakce do bloků a poté se snaží ověřit tento blok a zařadit ho za předchozí bloky do takzvaného blockchainu.

Během těžení jsou transakce potvrzovány a zařazovány do řetězce za sebou jdoucích bloků. Podle Hracha, J. [75] je pro zajištění dostatečné bezpečnosti nutné prokázat, že uživatel vlastní dostatek výpočetního výkonu. K tomuto slouží koncept Proof of work, který musí těžaři vyřešit. Jak popisuje James, M. [76] proof of work je výsledek složité úlohy, který bylo složité vyprodukovat tak, aby splňoval určité požadavky. Naopak však musí být triviální zkontrolovat, jestli výsledná data splňují zadané požadavky.

Vytváření proof of work by tedy měl být náhodný proces s nízkou pravděpodobností. Proto je nutné vykonat řadu neúspěšných pokusů, než bude vygenerován platný proof of work. Bitcoin, jak popisuje web Hashcash [69], využívá proof of work Hashcash.

Těžaři tedy hledají hodnotu hash funkce aktuálního bloku, která splňuje požadavky na složitost. Jak uvádí Hrach, J. [75] požadavkem je, aby výsledná hodnota byla menší než aktuální target hodnota. Target je číslo, které značí složitost výpočtu a pravidelně se mění, podle výkonu, kterým disponuje celá Bitcoinová síť. Aktuální hodnotu targetu je možné zjistit například na webu Blockexplorer [22]. Těžař využije hash posledního bloku spojí ho s hash hodnotou transakcí a přidá nějaké číslo takzvané Nonce. Poté vypočítá hodnotu hash funkce a porovná, jestli je menší než hodnota target. Jak bylo popsáno výše, těžení využívá principu proof of work, díky tomuto principu uživateli v podstatě nezbývá nic jiného než zkoušet jednotlivé hodnoty, porovnávat je s hodnotou target dokud nebudou splněny požadavky. Pokud nejsou splněny požadavky, musí zkoušet jinou hodnotu nonce, dokud nenajde takovou, která požadavky splňuje. Težení tedy využívá principu jednosměrných funkcí, kdy je složité zjistit vstupní data, ale je velmi jednoduché zkontrolovat zda jsou správná. Když těžař najde blok mohou ostatní težaři snadno zkontrolovat zda jeho řešení je správné. Pokud se více jak

polovina z nich shodne že ano, získá těžař, který jako první zkompletoval blok, získá odměnu v podobě nově vygenerovaných mincí, které jsou tímto uvolněny do oběhu. Z tohoto principu plyne motivace uživatelů k tomu, aby využívali svůj výpočetní výkon a drželi tak systém v provozu. Podle Buterina, V. [33] byl při začátku projektu počet vygenerovaných mincí za nový blok stanoven na 50 BTC, ale každých 210 tisíc bloku se tato hodnota půlí. V době psaní tohoto textu bylo celkem vytěženo přibližně 340 tisíc bloku a odměna za nově objevený blok tak byla 25 BTC. Odměna za ověřené bloky bude tedy postupem času klesat, v budoucnu se přiblíží až k nule.

Těžba je také navržena tak, aby byla dostatečně složitá a její náročnost se upravovala vzhledem k výpočetní síle uživatelů, kteří těží bitcoiny díky tomu zůstává množství ověřených bloků stabilní a síť se tak udržuje bezpečná. Podle webu Bitcoinwisdom [17] dochází k úpravě obtížnosti těžby každých 2016 bloků, což je přibližně třikrát za měsíc

2.3.4 Blockchain

Jednotlivé transakce jsou tedy zaznamenávány do veřejné knihy, kde se sdružují do bloků. Takovéto bloky vždy obsahují odkaz na předešlý blok. Tímto se vytváří řetězec navazujících bloků, který se nazývá blockchain.

Jak popisuje Bonadonna, E. [30], blockchain slouží k odlišení skutečných transakcí od pokusu o double spend, neboli snahu utratit stejné mince vícekrát. Jak již bylo uvedeno, systém staví na uživatelích, kteří ověřují transakce. K tomuto vždy potřebují mít staženou kopii tohoto blockchainu. Jelikož je systém decentralizovaný a působí v něm velké množství uživatelů, kteří mohou mít v jeden okamžik odlišné kopie záznamu blockchainu. Pro rozhodnutí, který blok bude zařazen, se využívá většiny Bitcoinové sítě, pokud některý z těžařů vyřeší úlohu a většina sítě se shodne, že řešení je správné právě tento blok je zařazen do blockchainu. Bonadonna, E. [30] dodává, že rozhodování na bázi většiny může být do budoucna problémem, pokud by někdo ovládal většinu sítě mohl by tohoto systému zneužít.

2.3.5 Sdružené těžení

Většina uživatelů již nemá dostatečně vysoké množství výkonu, aby se jim vyplácelo samostatné těžení. Řešením je takzvané pooled mining nebo-li sdružené těžení. Jak popisuje web Bitcoinmining [15], sdružené těžení spočívá ve spojení jednotlivých těžařů do skupiny, ve které tak spolupracují. Pokud naleznou blok, celková odměna se rozdělí mezi jednotlivé těžaře

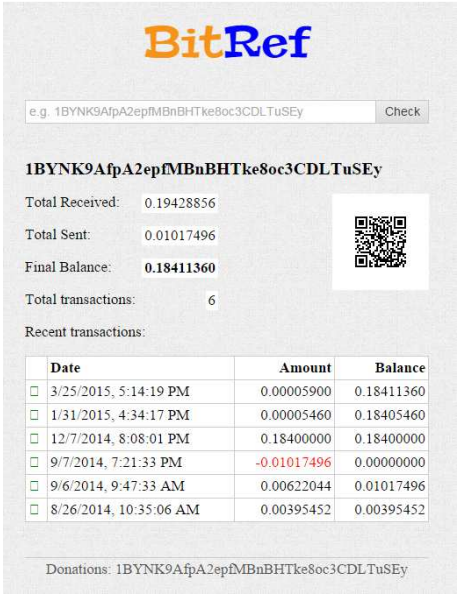
podle množství poskytovaného výkonu jednotlivými uživateli. Mezi nejvýznamnější provozovatele sdruženého těžení patří F2pool, Ghash.io a další.

2.3.5.1 Multipool

Jedná se o sdružené těžení, kde je možno těžit více než jeden typ mince. Takovýto pool se tak podle různých parametrů rozhoduje, kterou minci bude nejvýnosnější těžit. Při výběru tak záleží na náročnosti těžení, výpočetním výkonu a ceně.

2.3.6 Stav konta

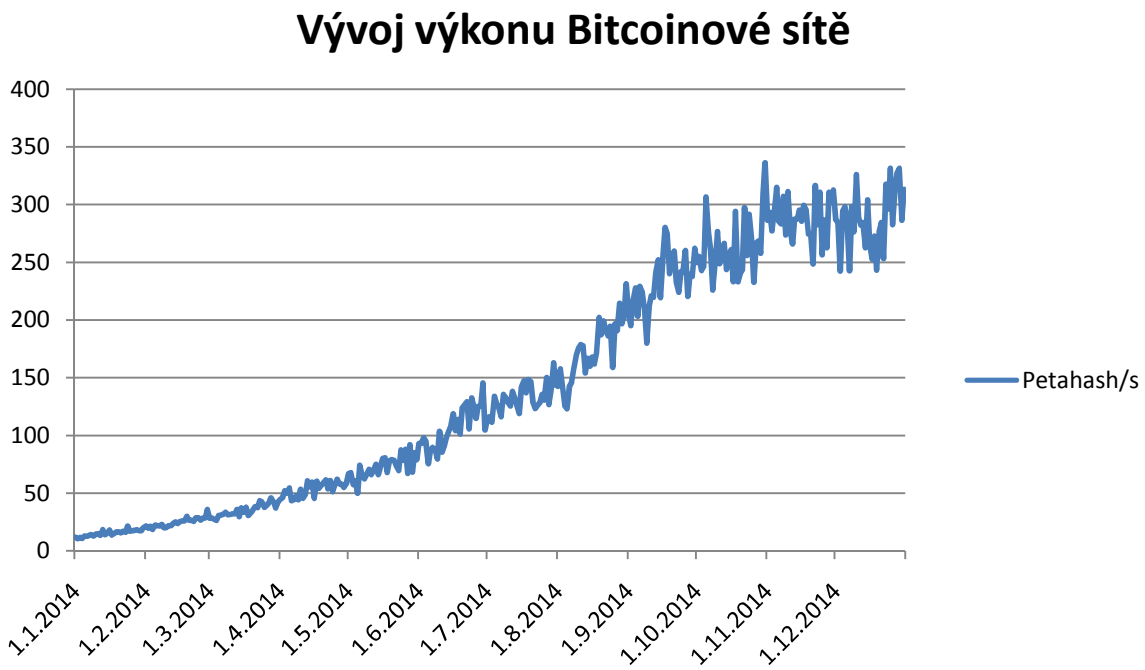
Všechny transakce jsou veřejné a je možné prozkoumat, například na webu blockhain.org či blockexplorer. Vzhledem k tomuto principu je možné například pomocí webové stránky bitref.com dopočítat celkový stav konta na libovolné adrese.



Obrázek 1 Kalkulace celkového stavu adresy. Zdroj: BitRef [19]

2.3.7 Hash rate

S rostoucí počtem těžařů zapojených do procesu roste také jejich celkový výpočetní výkon. Celkový výkon se měří pomocí hash rate, Bitcoin.org [13] definuje hash rate jako jednotku výkonu Bitcoinové sítě. Hash rate 1/Phs, znamená, že celá síť dokáže za sekundu provést 10^{15} výpočtů.



Obrázek 2 Vývoj hash rate v čase. Zdroj: Blockchain [25]

2.4 Parametry Bitcoinu

2.4.1 Decentralizace a inflace

U klasických měn existují centrální instituce, které spravují měnu, a které tak mohou svými intervencemi do jisté míry ovlivňovat cenu a množství peněz v ekonomice.

U Bitcoinu žádná instituce, která by mohla takto ovlivňovat cenu, neexistuje. Vzhledem k tomu, že zde nefiguruje žádná centrální autorita, mohlo by se tak zdát, že hodnota je přisouzena pouze důvěrou v ně. Podle Coxe, J. [29] však jejich hodnotu zaštituje cena elektrické energie, která je potřeba k vytvoření nových mincí (viz kapitola těžení).

Systém fungování bitcoinu je také navržen tak, že celkové množství jednotlivých mincí v oběhu je omezené a není tedy principiálně možné do nekonečna uvolňovat nové mince do oběhu. Cox, J. [29] popisuje uvolňování peněz do oběhu jako asymptotický růst. Jedná se o opak růstu exponenciálního, kdy s každým dalším rokem se celkové množství uvolněných peněz zmenšuje. Nároky na složitost potřebných výpočtů tak rostou a s nimi klesá množství uvolňovaných peněz do oběhu. Po první 4 roky bylo vytvořeno 10,5 milionu bitcoinů a toto množství se každé čtyři roky sníží o polovinu. Na 5,25 milionu 2,625 milionu a tak dále. Celkové množství se bude přibližovat 21 milionům, a jak dodává Cox, J. [29] většina mincí bude v oběhu již roku 2030, roku 2140 bude vytěžen poslední bitcoin. Vzhledem k omezení maximálního počtu mincí uvádí Winters, T. [111], že je možné jednotlivé bitcoiny dělit na menší částky a to až na 8 desetinných míst.

2.4.2 Nenávratné transakce

Dalším významným rozdílem je nevratnost plateb. V případě problému s platbou provedenou přes kreditní kartu je možné se obrátit na provozovatele a platbu tak reklamovat. U Bitcoinu jsou však veškeré převody peněz principiálně nevratné a nelze je tedy reklamovat. Jak uvádí web Bitrated [18] nenávratnost transakcí je možné řešit využitím takzvaných multisignature transakcí a webových služeb jako právě Bitrated, které slouží jako arbitr. V takovýchto transakcích figurují 3 subjekty a k úspěšnému dokončení transakce je potřeba schválení transakce od dvou z nich. V případě problému se jak kupující tak prodávající mohou obrátit na tohoto arbitra, který slouží jako důvěryhodná stranu. Ovšem v případě standardních transakcí, mezi uživateli, podle webové stránky Bitcoin [14] platí,že k navrácení peněz platícímu může dojít, pouze pokud se je příjemce rozhodne vrátit.

2.4.3 Anonymita

Využívání Bitcoinu nevyžaduje žádné osobní údaje, ovšem v jistých případech nemusí být tak anonymní, jak by se mohlo zdát. Bradbury, D. [32] považuje Bitcoinovou síť za pseudoanonymní. Vzhledem k celkovému systému Bitcoinu, kdy je každá transakce dohledatelná, se může bitcoin jevit jako ne příliš anonymní. Na druhou stranu pro využívání nevyžaduje od uživatelů žádná soukromá data. V systému jsou uživatelé reprezentováni pouze pomocí veřejné adresy, kterých si navíc může každý vygenerovat libovolné množství. Dokud

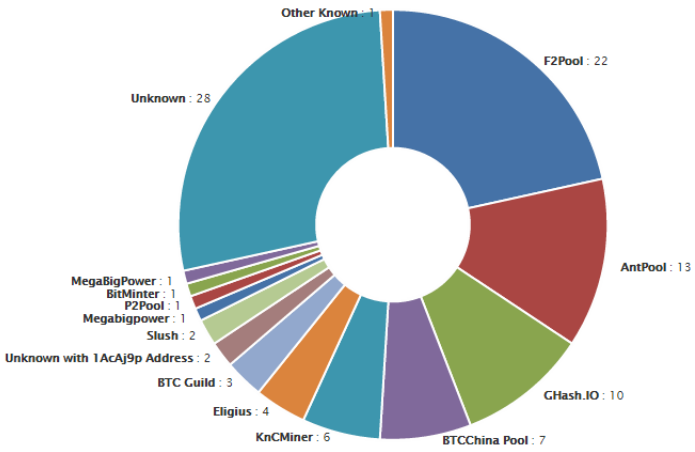
tedy nedojde k provázání adresy uživatele s objednávkou, které by obsahovala jeho osobní data je systém anonymní. Podle oficiálního webu Bitcoinu.org [14], je toto důvod, proč by měly být adresy využívány vždy pouze jednou.

2.4.4 Bezpečnost

Podle Higginse, S. [71] roste počet kybernetických útoků na uživatele bitcoinu. Higgins dodává, že množství útoků úzce souvisí i s cenou bitcoinu. Jak uvádí web Bitcoin.org[14], celý systém je sice chráněn silným šifrováním, ale závisí především na uživateli, jak budou jeho peníze v bezpečí. Light, J. [81] tak považuje za důležité především důsledné zabezpečení peněženky pomocí silného hesla s využitím dvoufázové ochrany. Bezpečnostní riziko také závisí na volbě peněženky, ve které budou bitcoiny uloženy. Jednotlivým typům peněženek je věnováno více prostoru v kapitole Bitcoin a software.

2.4.4.1 51 attack

Jak již bylo popsáno výše, o tom, která transakce bude zařazena do blockchainu a uznána jako platná se v systému Bitcionu rozhoduje na bázi většina výpočetní síly. V případě, že by někdo disponoval většinou (více jak 50% celkového výpočetního výkonu), mohlo by to pro celkový systém znamenat několik problémů. Capkun, V. [35] předpokládá, že síť je z většiny tvořena poctivými jedinci a žádný z nich nebude mít takové množství výpočetní síly. V případě takzvaného sdruženého těžení se však může stát, že některá taková to skupina skutečně dosáhne většího než polovičního množství výkonu. V době psaní tohoto textu se podle webu Blockchain [25] držel největší podíl na výkonu těžařské sdružení F2Pool, které sdružovalo 22% celkového výkonu sítě.



Obrázek 3 Rozdělení výpočetního výkonu. Zdroj Blockchain [25]

V případě, že by některý subjekt dosáhl nad zmíněnou hranici 50%, mohl by podle Bořánka, R. [31] zabránit potvrzování transakcí a těžení bloků. Jako největší problém se v takovém případě jeví takzvaný Double-spend, nebo-li snaha o utracení stejných peněz vícekrát. Jak uvádí Bořánek, R. [31] :*„Pokud by jeden subjekt měl většinu výpočetního výkonu sítě, může transakce potvrzovat ve svůj prospěch“*. Bořánek, R. [31] ovšem dodává, že žádný pool (skupina sdružených těžařů) nemá pro provedení takovéhoto útoku důvod, jelikož by se tím připravil nejen o poplatky z ověřovaných transakcí, ale také o důvěru těžařů. Důvodem pro provedení takovéhoto útoku, se tak může jevit snaha poškodit či zničit celý projekt, bez ohledu na enormní finanční náklady nutné na získání potřebného množství výkonu. V případě hrozícího nebezpečí je i v tomto případě podle Andresena, G. [8], hlavního vývojáře Bitcoinu možné řešení v podobě úpravy kódu, ke které by došlo při bezprostředně hrozícímu útoku.

2.4.4.2 Likvidita bitcoinu

Jak popisuje web banky Saxo [104], pojem likvidita představuje schopnost zajistit peněžní prostředky ze svých aktiv a tím dostát svým závazkům. Čím je tedy likvidita vyšší tím rychleji je společnost či jednotlivec schopný získat peněžní prostředky.

Bitcoin zdaleka není tak rozšířený, aby se dal využívat podobně jako skutečné peníze. Samotná Bitcoinová transakce trvá přibližně 10 minut než je zařazena do bloku a tím potvrzená. Bloky na sebe navazují, s každým dalším blokem se transakce dostává hlouběji a hlouběji. Řada směnáren vyžaduje různý počet potvrzení, například směnárna Coinbase [40]

vyžaduje 3 potvrzení a směnárna Bitstamp [20] šest potvrzení.. Převedení bitcoinů do některé ze směnáren je tedy otázkou řádově desítek minut. Ovšem poté je třeba ještě převést bitcoiny ze směnárny do banky. Převod může trvat dva až pět dní, v závislosti na výběru směnárny a na státu, ve kterém sídlí banka.

2.4.4.3 Využití Bitcoinu k ilegálním aktivitám

Celá základní myšlenka systému Bitcoinu se jeví jako zajímavá alternativa platebních prostředků. Systém umožňující anonymní využívání, který je neregulovaný a nezávislý na centrálních autoritách, však činí z Bitcoinu atraktivní prostředek také pro ilegální využití. Podle Fagana, E. J. [60] Bitcoin do značné míry eliminuje zprostředkovatele a tím umožňuje jednotlivcům provádět transakce, aniž by podléhaly kontrolám praní špinavých peněz, což z něj činí atraktivní měnu pro zločince. Fagan dodává, že zločinci zapojení do nadnárodní trestné činnosti potřebují bankovní účty, možnost mezinárodních transakcí a především anonymitu. Vzhledem k provádění přímých transakcí od uživatele k uživateli, tak použití Bitcoinu umožňuje provádění ilegálních transakcí v obrovském měřítku.

2.5 Bitcoin, software a aplikace

2.5.1 Peněženky

Pro využívání Bitcoinu jako platidla slouží takzvané peněženky. Tyto peněženky umožňují odesílat a přijímat bitcoiny, spravovat adresy, privátní klíče. Jednotlivé peněženky se nejvýrazněji liší, podle toho pro jaké využití jsou určeny a také mají odlišnou a také podle zařízení. Jednotlivé typy peněženek popisuje web Coindesk [41].

2.5.1.1 Desktopové peněženky

Verze Bitcoinové peněženky instalované přímo do počítače. Hlavní výhodou těchto peněženek oproti webovým peněženkám je, že nezapojují do procesu třetí stranu. Jak popisuje Jackman, J. T. [3] některé desktopové peněženky, například oficiální klient, také často vyžadují stažení celé kopie blockchainu se všemi předchozími transakcemi. V době psaní tohoto textu tato velikost podle webu Blockchain [23] dosahovala přes 27GB dat

2.5.1.2 Mobilní aplikace

Peněženky v podobě mobilních aplikací se nejvíce odlišují od těch desktopových ve využitém systému. Vzhledem ke kapacitě mobilních zařízení není možné, aby takovéto peněženky uchovávaly celou kopii blockchainu. Podle Hardy, P. a Zaman, M. [68] z tohoto důvodu

využívají mobilní aplikace zjednodušené ověřování transakcí (SPV), které vychází z malé části dat z blockchainu. Platby pomocí bitcoinů jsou stále hlavní doménou internetových obchodů. Nejsou však omezené pouze na internet, ale podle Pagliery, J. [93] je s nimi možno v některých kamenných obchodech. Mobilní peněženky mohou být vhodnou volbou v případě, kdy uživatel potřebuje mít peněženku stále při sobě.

2.5.1.3 Webová aplikace

Peněženky fungující v rámci webového rozhraní bývají pro uživatele nejjednodušší a také nejpohodlnější na využívání. Uživatel nemusí instalovat žádné programy a stačí mu pouze webový prohlížeč. Nadruhou stranu je tato jednoduchost vykoupena nižší bezpečností, protože uživatelé vkládají důvěru do provozovatele, který je zapojen do procesu. Podle Hardyho a Zaman [68], jsou webové peněženky vystaveny několika potencionálním problémům. Například provozovatel takovéto peněženky může být považován za finanční instituci a podléhat regulacím ze strany státních úřadů.

2.5.1.4 Offline uložení bitcionů coldstorage

Cold storage peněženky fungují na principu zamezení přístupu k privátním klíčům z internetu, kde by se jinak vystavovali největšímu nebezpečí. Podle Apodaca, R. [9], se jedná o speciálně vytvořené offline prostředí, které slouží pro využívání všech operací, zahrnujících privátní klíče. Vzhledem k tomuto přístupu zůstávají privátní klíče mimo síť a nevystavují se tak případným útokům z její strany. Jak uvádí web Bitzuma [9], proces začíná vygenerováním nepodepsané transakce v online prostředí. Takováto transakce je následně přesunuta pomocí USB disku či jiné metody do offline prostředí, kde dojde k jejímu podepsání. Po podepsání může být transakce opět přesunuta zpět a může tak být bezpečně odeslána. Podle Davida Perry[96]musí cold storage splňovat základní parametry.Nesmí být nikdy připojeno k internetu nebo veřejné síti.Mělo by umožňovat uložení privátních klíčů, které by se neměly využít k podepisování plateb přes internet. Do systému by tak měli vstupovat pouze nepodepsané transakce a vystupovat podepsané transakce.

2.5.1.5 Hardwarové peněženky

Při využití hardwarové peněženky jsou privátní klíče uloženy ve speciálním zařízení, přímo k tomu určeném. Zařízení se připojují k internetu jen při vykonávání transakce, tudíž nevystavují obsah útokům ze sítě.

2.5.1.6 Fyzické formy Bitcoinů.

Další možností jak uložit Bitcoin je využití některé ze specializovaných firem, které implementují privátní klíče do fyzických vyražených mincí. Jak již bylo řečeno bitcoin neexistuje jako digitální soubor, jde pouze záznam o vlastnění určité částky, skrz provedené transakce. Přesto je možné od specializovaných výrobců objednat kovové mince, do kterých je tento záznam implementován a je možné je do jisté míry považovat za fyzické mince.

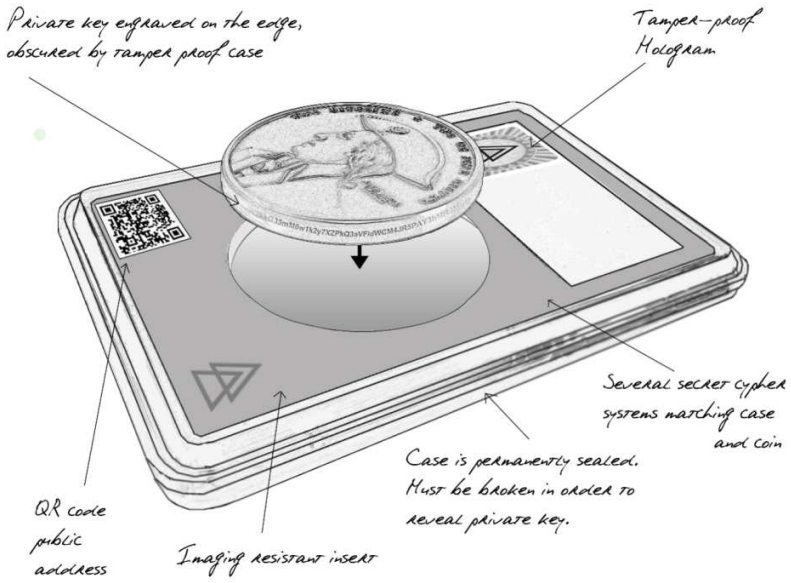
2.5.1.6.1 Titan BTC

Jednou ze společností vyrábějící takovéto mince je Titan Mint Inc. Společnost nabízí dvě verze mincí. První je jednodušší a také s nižším zabezpečením. Jedná se o kovovou minci opatřenou ochranou nálepkou pod mincí, kterou je skryt privátní klíč. Ke každému privátnímu klíči je matematicky přiřazena adresa, na které je v tomto případě uložen 1 BTC. Jak uvádí web TitanBTC [107] v případě, že chce uživatel takovýto bitcoin přenést do své peněženky sloupne bezpečnostní nálepku a importuje privátní klíč do své peněženky. Druhou možností je mince s dvoufázovým ověřením. Takovéto mince obsahují nálepku, pod kterou je kód k vyzvednutí mince, a navíc jsou registrovány na uživatelské jméno. Pokud chce uživatel prodat takovouto minci, musí podle webu TitanBTC [108] předat i údaje, na které je registrována. Fillmore, T. [102] uvádí, že vzhledem k vysokým nárokům na zabezpečení, společnost nabízí takzvanou sto deseti procentní ochranu, čímž se zavazuje, že v případě prolomení bezpečnostních prvků mince nahradí 110% jejich hodnoty.

2.5.1.6.2 Alitin Mint

Společnost vyrábějící fyzické mince s bitcoiny, zaměřená především na sběratele. Alitin Mint vyrábí limitované série mincí s odlišným přístupem k zabezpečení než výše zmíněný TitanBTC. Podle oficiálních stránek společnosti [7], si vyšší cena bitcoinů zasluhuje také lepší zabezpečení, než je ukrytí privátních klíčů pod nálepku na zadní straně mince. Při ověření mince, která je zaregistrovaná, vkládá uživatel maximální důvěru do společnosti, která toto zajišťuje. Mince vyráběné u Alitin mint tak místo těchto metod spoléhají na uložení mince do speciální krabičky, podobně jak tomu je i u klasických sběratelských mincí. Jak zobrazuje obrázek č. 5 níže, bezpečnostní opatření se skládá z mince, která má na okraji vyražené privátní klíče, tato mince je uchována v krabičce, což zabraňuje, aby kdokoli přečetl privátní klíče. Krabička je také opatřena dalšími bezpečnostními prvky, a pokud chce majitel převést minci do své peněženky, musí tuto krabičku otevřít. V případě, že chce majitel prodat

fyzickou minci, musí ji prodat v neporušené krabičce, jen tak má kupující jistotu, že bitcoiny nebyly převedeny do peněženky.



Obrázek 4 Alitin Mint bezpečnostní prvky. Zdroj Alitinmint [7]

2.5.2 Konkrétní peněženky

2.5.2.1 CoinBase

Jedná se o peněženku dostupnou buď jako webová, nebo jako mobilní aplikace pro zařízení s IOS či Android. Podle webových stránek této peněženky [39]ji využívá 2 miliony uživatelů a je plně podporována v devatenácti zemích světa.

Pro lepší zabezpečení nabízí CoinBase takzvaný trezor, pomocí kterého může uživatel přijímat platby stejně jako v normální peněžence, ale navíc také disponuje dodatečnou ochranou.Při vytváření trezoru si uživatel může vybrat, zda svěří správu přímo CoinBase, či se o klíče k trezoru bude starat sám. Uživatel si také může zvolit takzvaný Multisig trezor, kdy přizve další důvěryhodné uživatele, kteří musí schválit výběr finančních prostředků. Navíc je zde 48 hodinová lhůta, po kterou může být výběr zrušen.

2.5.2.2 Armory

Desktopová peněženka Armory je open-source projekt zaměřený především na bezpečnost. Jak popisuje McCormick, J. [86] pro fungování této peněženky je potřeba standardní Bitcoin klient, který Armory potřebuje pro fungování. Tato peněženka patří ke složitějším k nastavení,

McCormick, J. [86] dodává, že je složitější se v této peněžence zorientovat, na druhou stranu se však jedná o jednu z nejlepších a nejbezpečnějších desktopových peněženek.

2.5.2.3 Multibit

Multibit je jednoduchá desktopová peněženka. Podle Hajdarbegovic, N. [66] si ji od roku 2011 stáhlo přes 1,5 milionu uživatelů. Mezi hlavní funkce patří především jednoduchost a rychlost synchronizace.

2.5.2.4 Trezor

Trezor český produkt zaměřený především na náročnější uživatele, kteří mají v bitcoinech uloženy větší částky. Trezor se skládá z dvou částí první je samotné hardwarové zařízení a druhou online peněženka. Transakce jsou vytvářeny v online peněžence a poté potvrzeny pomocí tlačítek na tomto trezoru. Zařízení nemusí být neustále připojeno k počítači, čímž se snižuje riziko, že budou privátní klíče vyzrazeny.

2.5.3 Brawker

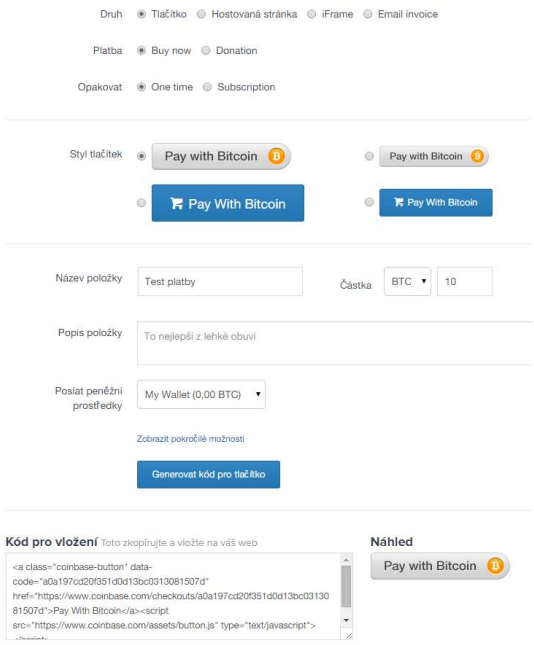
Webová služba, která funguje trochu odlišně než ostatní směnárny. Cílem je umožnit platit uživatelům pomocí bitcoinů i v internetových obchodech, které to samy o sobě neumožňují. Podle Palmer, D. [94], nabízí Brawker určité výhody. Umožňuje ušetřit při platbě za zboží pomocí bitcoinu. Umožňuje získat slevu z nákupu pro uživatele vlastnícího bitcoiny, tím že je spojí s uživateli, kteří by rádi získali bitcoiny. V případě, že chce uživatel koupit zboží v nějakém internetovém obchodě, zadá do systému webovou adresu odkazující na toto zboží, celkovou hodnotu a další parametry. Také si vybere požadovanou slevu, která může činit až 20% z celkové částky. Čím je však sleva vyšší, tím je pochopitelně nabídka méně atraktivní pro kupující, protože získají nižší hodnotu bitcoinů. Nabídka je následně uložena v systému, a pokud někdo bude ochoten na ni přistoupit, dojde k uskutečnění transakce. Ve snaze zajistit dostatečnou bezpečnost obou stran využívá Brawker transakce s ověření více stranami. V případě problému jedné ze zúčastněných stran je možné se tak obrátit na Brawker a požadovat řešení.

2.5.4 Platebníbrány

Systémy umožňující uživatelům, kteří chtějí přijímat platby v bitcoinech, integrovat platbu do webových stránek.

2.5.4.1 Coinbase

Webová peněženka nabízí nástroje nejen pro přijímání a odesílání bitcoinů, ale také různé nástroje pro obchodníky. Přes webové rozhraní je možné si nakonfigurovat, jak budou bitcoiny přijímány. Uživatel má na výběr z několika druhů implementace plateb. Může volit mezi tlačítkem, fakturou a dalšími možnostmi. Dále si může zvolit, jestli bude platba jednorázová či opakovaná. Uživatel vyplní svůj obchodní profil, údaje o zboží a poté si vygeneruje HTML kód, který může umístit na svou stránku.



Obrázek 5 Generovaní platebních tlačítek. Vlastní zpracování. Zdroj Coinbase [38]

2.5.5 Coinmarketcap

Jednotlivé hodnoty a parametry kryptoměn je možné prozkoumat například na webu Coinmarketcap [44]. Tato webová služba zobrazuje data u více jak 480 kryptoměn. Uživatelé mohou prozkoumávat parametry jako cena, celková tržní kapitalizace, a počet mincí v oběhu. Coinmarket také umožňuje zobrazit ceny kryptoměn na jednotlivých trzích, grafy vývoje hodnoty v čase a řadu dalších ukazatelů.

2.5.6 Proof of existence

Proof of existence je webová služba využívající principy Bitcoinu k potvrzení, že daný dokument existoval v určitém čase. Podle oficiální stránky [97] tohoto projektu jsoudata dokumentu převedena na hodnoty hash funkce SHA-256 a poté pomocí transakce zahrnuta do

Blockchainu. Bitcoin ve svém systému umožňuje využít několik skritpů, v tomto případě se využívá skriptu OP_RETURN. Apodaca, R. [10] uvádí, že tento skript označí výstupy transakce jako prokazatelně neutratitelné a také umožní přidání malého množství dat, v tomto případě se jedná o označení a hash dokumentu.

2.5.6.1 Princip funkce

Uživatel přes webové rozhraní nahraje určitý soubor. Následně vygenerován hash souboru a adresa, na kterou má zaslat částku 5 mBTC neboli 0,005 BTC. Po zaslání této částky je platba provázána a vytvořena transakce, ve které je zahrnut hash souboru. Pokud posléze uživatel nahraje stejný soubor pro kontrolu, je tento soubor rozpoznán a podle transakce lze ověřit, kdy byla zahrnuta do blockchainu a podle toho ověřit čas existence dokumentu.

2.5.6.2 Označení transakcí

0x444f4350524f4f46

Příklad transakce

3dda1885d5579b476e83cb1a1b130df253f45542580df9b1074ec0c6442d86c8

Hash dokumentu

6976a5e7fffe4e589a0be7e9cc192aee61885b5c8a771694f248f78bc871ad66

OP_return

444f4350524f4f466976a5e7fffe4e589a0be7e9cc192aee61885b5c8a771694f248f78bc871ad66

2.5.7 Vlastní Bitcoin adresa

Standardní Bitcoinové adresy jsou náhodně generovány, ovšem s použitím vhodných metod je možné si vytvořit adresu s částí přizpůsobenou podle vlastních požadavků. Takovéto vytvořené adresy se nazývají vanity adresy. Vanity adresa musí splňovat několik základních parametrů, které jsou kladeny i na obyčejné adresy. Všechny bitcionové adresy začínají podle Antonopoulose, A. [1] číslem 1. Také nesmí obsahovat snadno zaměnitelné znaky jako 0, O a L a I. K. Uživatel si vybere, jaké znaky chce mít v adrese a poté program k tomu určený začne generovat privátní klíče, dokud není nalezena shoda. Vytvoření takové adresy je možné využít buď internetové služby nebo program Vanitygen. Rozdíl mezi těmito dvěma metodami je především v bezpečnosti, rychlosti a ceně. Online služby jako je například Vanitygen.com [56] nabízejí vygenerování adresy s až 5 vlastními znaky na začátku zdarma, delší adresy jsou zpoplatněny. Uživatel také musí spoléhat na to, že takováto webová služba neukládá

vygenerované privátní klíče, které by mohli být zneužity. Druhou možností je program Vanitygen, program je dostupný pro Windows a spouští se z příkazového řádku. Uživatel si také může vybrat, jestli bude cílem najít adresu s konkrétními znaky na začátku či uvnitř adresy. Rychlost vygenerování klíče je závislá na výpočetním výkonu použitého hardware podle webu Bitcointalk [12] program při využití čtyřjádrového procesoru v 64 bitovém módu prohledá přibližně 300-700 tisíc klíčů za sekundu.

2.6 Bitcoin hardware a ostatní využití

Systém bitcoinu staví na těžení. Jak již bylo uvedeno v kapitole 2.3.3 těžení spočívá ve využívání výpočetního výkonu k provozu celé Bitcoinové sítě. Zajišťuje bezpečnost sítě a potvrzuje transakce a vytváří nové mince, které tak uvádí do oběhu.

2.6.1 Těžební hardware

Za těžební hardware je možno považovat jakýkoliv hardware, schopný spustit težební program, který zajišťuje samotné těžení Bitcoinu či jiných kryptoměn. Pro provádění těžení motivuje uživatele především odměna v podobě nově vytvořených mincí. Čím se zapojovalo více uživatelů, tím bylo nutné upravovat složitost těžení, tak aby síť zůstala dostatečně bezpečná. Zatímco na začátku projektu bylo možné těžit pouze za pomocí standardního domácího počítače, se vzrůstající složitostí se začali objevovat stále lepší a lepší metody těžení. Řada firem se následně začala zabývat přímo výrobou specializovaného hardwaru určeného pouze k těžení.

2.6.1.1 Etapy těžení

Vývoj těžení prošel několika etapami jak popisuje Liu, A [82], jednalo se především o těžbu pomocí procesoru, grafické karty a specializované ASIC obvody.

2.6.1.1.1 Těžba pomocí procesoru

V počátku bylo možné vytěžit bitcoiny i pomocí procesoru standardního stolního počítače dnes je to však pro mnohem vyšší náročnost vytěžení v podstatě nemožné.

2.6.1.1.2 Těžba pomocí grafické karty

Následující etapou ve vývoji těžení bylo využití grafických karet, které jsou pro těžení mnohem lépe vybaveny než procesory. Těžení je tak mnohem rychlejší.

2.6.1.1.3 ASIC

Zkratka označuje *aplication specific integrated circuit.* Jedná se o zařízení určené pro jednu specifickou funkci. Na výrobu speciálních zařízení určených pouze pro těžbu bitcoinu se zaměřuje řada výrobců. Takovéto zařízení jsou mnohonásobně efektivnější než předešlé metody, ale také jsou výrazně dražší.

Obrázek 6 Monarch – asic karta pro těžení kryptoměn. Zdroj: ButterflyLabs[34]

3 Ostatní kryptoměny

Jelikož Bitcoin nabízí otevřený kód je na jeho technologiích založena celá řada dalších kryptoměn. Na webu Coinmarketcap [44] je možné zobrazit 486 různých kryptoměn. Většina z těchto kryptoměn se liší v drobných parametrech, podle webu Cryptocoinsnews [110] se jedná v podstatě o klony bitcoinu. Řada těchto kryptoměn vykazuje pouze drobné změny v rychlosti, hash algoritmu, či dalších parametrech. Některé jsou však zajímavější a snaží se uživatelům nabídnout také něco navíc, jako například větší zabezpečení.

3.1 Namecoin

Podle Wilmoth, J. [110] se jedná o první alternativní měnu založenou v dubnu 2011. Stejně jako bitcoin je horní hranice omezena na 21 milionů kusů, odměna je 50 kusů a půlí se každých 210 tisíc bloků. Zdrojový kód je také volně dostupný a každý ho tak může využít podle svého. Kromě společných parametrů s Bitcoinem, však přidává některé další vlastnosti. V době psaní tohoto textu se namecoin obchodoval za 0,45 dolaru za jeden namecoin (NMC). Celková hodnota všech mincí na trhu byla 4,8 milionu dolarů. Hlavním rozdílem oproti

Bitcoinu je, že kromě funkce peněžní, je také pomocí namecoinu možné registrovat doménu .bit. Jak popisuje Gilson, D. [63] tato doména těží z vlastností decentralizovaného systému a aplikuje ho na DNS. Normální DNS servery jsou pod správou centrálních autorit. V Namecoin protokolu je toto držení decentralizované, podobně jako v Bitcionu ověřování transakcí.

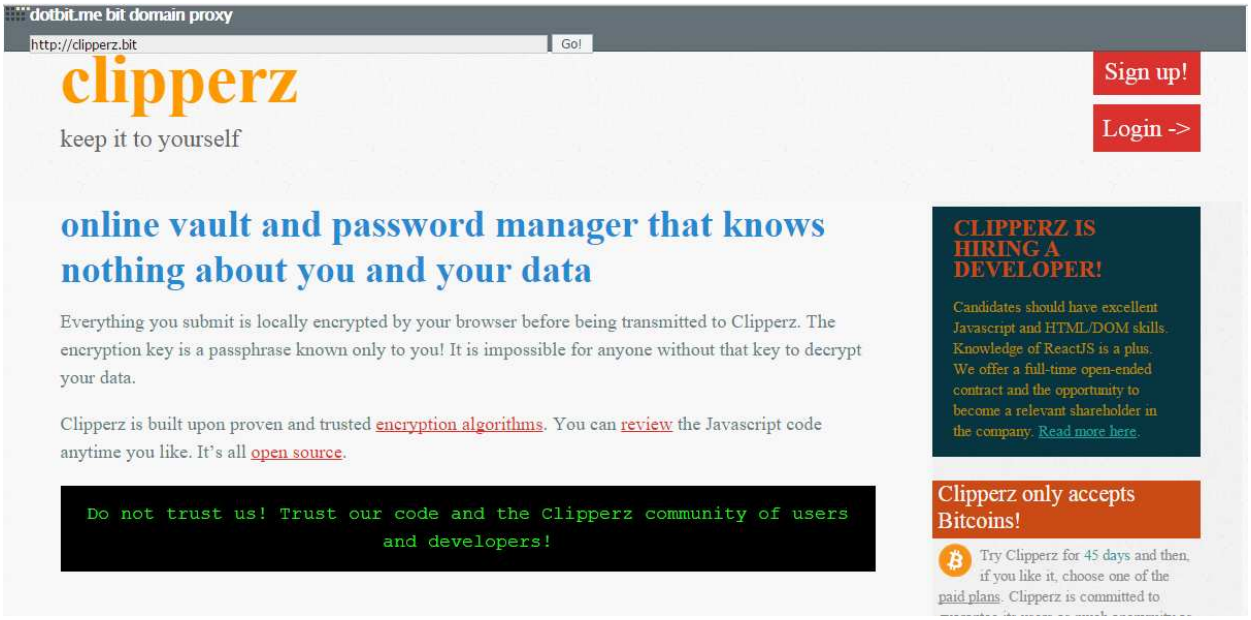
Podle oficiálního webu [90] jsou stránky s doménou .bit, díky decentralizaci odolné vůči cenzuře a různým útokům. Bitcoin technologie zajišťuje, že každý uživatel v celém světě má na svém počítači k dispozici stejný seznam dat. Zároveň však nikdo nemůže ilegálně tyto data změnit.

V Namecoin protokolu jsou tak zahrnuty 3 typy transakcí

- **name_new**
  - předobjednání nové doména. Za tuto transakci zaplatí uživatel 0.01 NMC.
- **name_firstupdate**
  - Registrace domény a umožnění veřejné dostupnosti této domény. Cena je proměnlivá a v době psaní tohoto textu činila 0 NMC.
- **name_update**
  - zdarma využité pro aktualizování, či převedení domény.

Aktuální ceny je možné zjistit například na webu Dotbit [51]. Všechny transakce jsou také zpoplatněny částkou 0,005 NMC.

Podle webu Dotbit [52] bylo v době psaní tohoto textu registrováno přes 140 tisíc domén .bit. Na téměř 5300 z nich byly webové stránky. Vzhledem k odlišnému fungování od normálního internetu je však prohlížení takovýchto stránek složitější. Web Dotbit [52] poskytuje proxy server, se kterým je možné se připojit na stránky s touto doménou.



Obrázek 7 Doména založená Namecoinu. Zdroj: Dotbit [51]

3.2 DarkCoin[1]

Kryptografická měna, založená nazačátku roku 2014. V době psaní tohoto textu byla hodnota jedné darkcoin mince (DRK) přibližně 1,3 dolaru trh s touto kryptoměnou měl celkem hodnotu přibližně 6,8 milionu dolarů. Tato kryptoměna je zaměřená na co nejlepší ochranu soukromí. DarkCoin se podle oficiální webové stránky [48] snaží pomocí anonymizačních technologií zabránit vystopovatelnosti transakcí. DarkCoin využívá protokol inovativní decentralizované sítě serverů nazývaných Masternodes. Podle Greenberga, A. [65] Darkcoin nabízí větší anonymitu než Bitcoin, protože takzvaně míchá platby jednotlivých uživatelů, takže je neuvěřitelně složité vysledovat transakci. Darkcoin pro anonymizaci transakcí využívá takzvaný Darsksend. Jak uvádí Higgins, S. [70] Darsksend je založen na konceptu CoinJoin od vývojáře Bitcoinu Gregory Maxwell [84]. Jedná se o automatické kombinování plateb uživatele s dalšíma dvěma. Pro kohokoli analyzujícího blockchain, je následně velmi složité zjistit, kde peníze skončily.

3.2.1 Darksend

V případě, že uživatel chce provést převod přes Darksend. Tyto mince jsou poslány do anonymizačního procesu. Během tohoto procesu se částka spojí s dalšími od ostatních uživatelů a poté putují přes jednotlivé servery nazývané Masternode. Uživatelé si mohou vybrat mezi 2 až 8 těchto serverů, kterými jejich mince následně projde. Po dokončení anonymizačního procesu jsou mince vráceny pod náhodnou adresou do uživatelovy peněženky. Poté mohou být poslány cílovému subjektu.

3.2.2 Masternode

Primární funkcí těchto serverů je zajistit anonymizační proces. Jak popisuje oficiální web [48], uživatelé Darkcoinu mohou být odměňováni nejen za těžení mincí, ale také za provoz tohoto serveru. Uživatelé, kteří chtějí provozovat vlastní Masternode server a získat tak odměnu musí nejprve mít 1000 darkcoinů jako jakousi formu zajištění. Pokud uživatel tyto mince utratí, jeho Masternode bude vyřazen z možnosti získat odměnu. Za poskytování služeb získá jeden náhodně vybraný Masternode server 20 % z odměny za vytěžený blok.

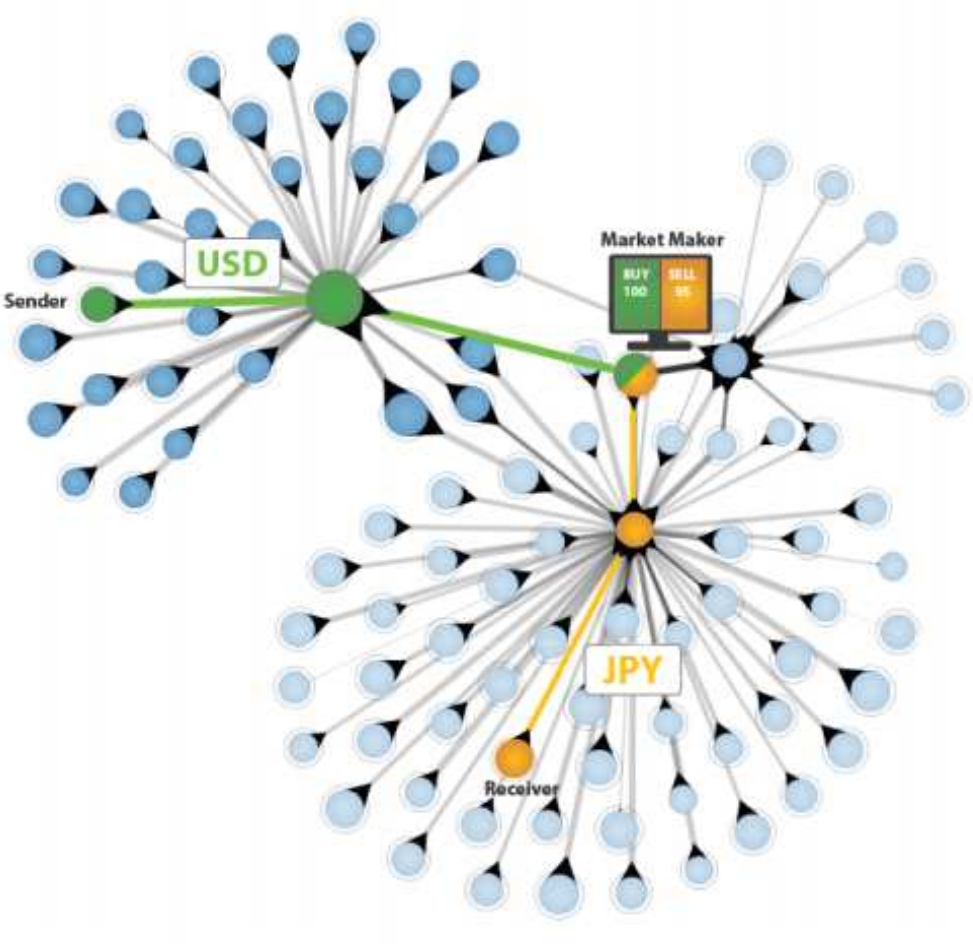
[1] Projekt DarkCoin se 16. Března 2015 přejmenoval na Dash, Viz. na dashpay.io

3.3 Litecoin

Litecoin je jednou ze známějších kryptoměn. S Bitcoinem sdílí základní charakteristiku. Ovšem celkový počet mincí bude až 84 milionů, také používá Scrypt jako hash algoritmus na rozdíl od Bitcoinu, který využívá SHA-256. Podle oficiálního webu [83], Litecoin nabízí rychlejší potvrzení a lepší efektivitu oproti Bitcoinu. Cenový vývoj je velice podobný Bitcionu, po téměř dvouročním drobném růstu následoval výrazný růst a poté postupné snížení ceny. Například na burze BTC-e [45] zažil Litecoin od roku 2012 postupný nárůst z téměř nulové hodnoty až téměř na 40 dolaru za kus, kterého dosáhl nakonci roku 2013 od této doby má jeho hodnota klesající tendenci. Na počátku roku 2015 se hodnota pohybovala okolo 1,35 dolaru za kus.

3.4 Ripple

Ripple je projekt, který staví na stejných principech jako Bitcoin, ale zaměřuje se na globální transakce prováděné v libovolné měně. Ripple je vytvářený společností Ripple labs, tato společnost také spravuje uvolňování peněz. Jak uvádí McIntyre, D. [87] Ripple nevyužívá pro uvolňování mincí těžení. Digitální měny ripple(XRP) bylo na začátku vydáno 100 bilionů kusů. Společnost plánuje uvolnit přes 80% toto množství do oběhu a 20% si plánuje ponechat jako kompenzace na finanční náklady. V době psaní tohoto textu držela společnost přes 70 bilionů kusů. Podle Ripple [100], podporuje Ripple řadu měn a uživatelům tak umožňuje mít účet v jedné měně a odesílat platby v jiné. Ripple síť tak v podstatě slouží k převádění měn, pomocí takzvaných tvůrců trhu. Na obrázku níže je pro lepší představu uvedena vizualizace sítě. Uživatel s účtem v amerických dolarech (USD) zaplatí v japonských jenech (JPY) pomocí tvůrce trhu, který od něj nakoupí americké dolary a dodá jeny. Jednotlivé transakce, vývoj ceny a další statistiky je možné prozkoumat pomocí webu Ripple charts[101].



Obrázek 8 Vizualizace systému fungování služby Ripple. Zdroj: Ripple [100]

4 Kryptoměny a legislativa v evropské unii

Bitcoin a další podobné projekty naplňují některé základní znaky klasických měn. Mohou například sloužit k nákupu a prodeji různých druhů zboží. Řadou dalších parametrů se však klasickým měnám nepodobají. Jelikož se kryptoměny liší v mnoha parametrech, není možné jednoduše zařadit do určité kategorie, jako jsou měny, komodity, akcie a další podobná aktiva. Následující text se zaměřuje na státní regulace kryptografických měn v Evropské unii a České republice.

4.1 Evropská unie a Bitcoin

Kromě kryptoměn také existují další formy virtuálních peněz. Evropská centrální banka ve své analýze [56]dělí virtuální měny do tří kategorií.

1) Uzavřené virtuální měny

   Nejedná se o měny, které by měli nějaký vztah ke skutečné ekonomice. Takovéto měny mohou být představovány například penězi v počítačových hrách.

2) Virtuální měny s jednosměrným tokem

   Měny, které mohou být zakoupeny za reálné peníze, ale tyto nakoupené virtuální peníze již není možné směnit zpět za skutečné.

3) Virtuální měny s obousměrnými toky

   Mohou být nakupovány a prodávány za určité kurzy. Pod tuto kategorii spadá Bitcoin a další kryptografické měny.

Přestože všechny tyto kategorie zahrnují název měna a také v souvislosti s Bitcoinem se často využívá slovo měna, podle Evropské centrální banky [56] nejedná o skutečné měny. Kromě toho je problémem stále velmi nízký počet obchodníků, kteří platby pomocí kryptoměn přijímají. Stejně tak je problémem samotná forma kryptoměn, které nemají žádnou fyzickou formu. Evropská centrální banka [56] pod pojmem měna chápe médium, které má také formu bankovek a mincí, z tohoto důvodu nemohou být v podstatě žádné virtuální měny považovány za skutečné měny. V zemích, které vstoupily do eurozóny a jako své zákonné platidlo přijali měnu Euro, je jak uvádí Leach, R. [80], přímo zákonem určeno, že tato měna musí být přijímána pro platbu za dluh v těchto zemích. Pokud by se stejný zákon aplikoval na

kryptoměny, znamenalo by to, že by dlužník mohl zaplatit svůj dluh například pomocí Bitcoinu, což je vzhledem k stále nízkému počtu uživatelů těžko představitelné. Původní zpráva Evropské centrální banky [57] uváděla několik rizik souvisejících s kryptoměnami, stejně tak ve zprávě z března 2015 [56] upozorňuje, že většina těchto rizik stále trvá. Jedná se především o problémy s praním špinavých peněz a financováním terorismu. Tabulka č. 3 uvádí vyjádření některých zemí Evropské unie k problematice virtuálních měn.

Země	Vyjádření	Varování	Kontrola
Belgie	Není zákonným platidlem ani elektronickými penězi	Ano	Ne
Česká republika	Bitcoiny 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 například se zlatem.	Ano	Ne. Bitcoiny by měly být regulovány na Evropské či globální úrovni
Estonsko	Není zákonné platidlo, ale alternativní platební prostředek	Ano	
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.
Chorvatsko	Není zákonné platidlo, elektronické peníze ani zahraniční měna		Ne
Irsko		Ano	Ne
Itálie	Není zákonným platidlem	Ano	
Kypr		Ano	Ne
Litva		Ano	
Lotyšsko		Ano	Ne
Lucembursko	Není zákonné platidlo	Ano	Společnosti působící ve finančním sektoru, poskytující služby související s virtuálními měnami musí mít povolení od ministerstva financí a být zaregistrování u CSSF kontrolor finančního sektoru
Maďarsko		Ano	Ne
Malta	Není zákonné platidlo	Ano	Ne

Německo	Není zákonné platidlo, ale finanční instrument, zúčtovací jednotka	Ano	Standardní úkony zahrnující bitcoiny nejsou kontrolovány. Některá využití mohou vyžadovat licenci.
Nizozemí		Ano	
Polsko	Není zákonné platidlo		
Portugalsko		Ano	Ne
Rakousko		Ano	Ne, od některých společností nabízejících služby související s virtuálními měnami je vyžadovaná licence
Řecko		Ano	
Slovensko		Ano	Ne
Slovinsko	Není měnou ani platebním instrumentem. Bitcoin by mohl spadat pod zákon o prevenci praní peněz a financování terorismu	Ano	
Španělsko	Virtuální měny nejsou považovány za legální měny, jelikož nejsou vydávány vládním měnovým orgánem	Ne	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	

Tabulka 3 Kryptoměny a legislativa v zemích evropské unie. Zdroj: Evropská centrální banka [56]

Z dat uvedených v tabulce je vidět, že žádná z členských zemí Evropské unie nepovažuje virtuální měny, a tudíž ani Bitcoin a další kryptoměny, za zákonné platidlo. Jak již bylo zmíněno, tyto měny je složité zařadit, tudíž se vyjádření jednotlivých států omezuje na definování, co virtuální měny nejsou. Případně považují tyto měny za aktivum (Švédsko), či alternativní platební prostředek(Estonsko). Z celkového počtu 28 členských států se jich vyjádřilo 26 a většina varovala před možnými problémy pramenícími z využívání virtuálních měn. Ovšem u kontroly se názory jednotlivých členských států rozcházejí. Nejčastější jsou případy, kdy tyto měny nejsou vůbec regulovány, nebo je licence vyžadována pouze k určitým úkonům.

4.2 Daň z přidané hodnoty v evropské unii

Od prvního ledna roku 2015 začal v Evropské unii platit nový zákon o dani z přidané hodnoty(DPH). Tento zákon také obsahuje část, která se dotýká elektronicky poskytovaných

služeb. Do elektronicky poskytovaných služeb spadá, podle webu Europa [55], každá služba, která je poskytována pomocí elektronické sítě a pro zajištění funkčnosti vyžaduje minimální zásahy. Zákon tak kromě prodeje elektronických knih, filmů, online aukcí a dalších podobných služeb ovlivňuje také kryptografické měny. Toto opatření má podle webu Europa [58] za úkol zajistit, aby daň z přidané hodnoty, v případě elektronicky poskytovaných služeb, byla zaplacena ve stejném státě, ve kterém je služba využívána. Jak uvádějí vysvětlivky k směrnici o DPH [59], pro zajištění tohoto požadavku, je od provozovatelů elektronicky poskytovaných služeb požadováno zaznamenání dvou důkazů o místě pobytu jejich zákazníků. Jako možnost prokázání místa pobytu může sloužit fakturační adresa, ip adresa, a další podobné dokumenty. V případě, že si zákazník například zakoupí nějaký produkt či službu pomocí kryptoměn, mohou být od obchodníka vyžadovány důkazy o místě pobytu. Podle Vanesy Mock [112] však není cílem těchto opatření zamezit anonymním platbám. Nařízení tak sice přímo neohrožují platby, ale zvyšující se požadavky kladené na obchodníky, mohou však odradit od přijímání těchto plateb.

4.3 Česká republika

V České republice stejně jako v dalších zemích evropské unie není možné považovat Bitcoin za měnu. Podle Vrbíkové, L. [61] Bitcoin a další podobné měny podle současných zákonů, platných v české republice nejsou penězi, formou měny ani cenným papírem nebo komoditou. Jak dodává Vrbíková, L. [61]: *„Vzhledem ke své nehmotné povaze jsou tak kryptoměny nejblíže definici cenina sui generis (svého druhu), podobně jako např. stravenky, poukázky, vouchery a podobně“*. V ČR je tak jako v dalších zemích potřeba příslušné legislativy, pod kterou budou tyto kryptoměny spadat.

4.3.1 Transakce mezi uživateli

Jedním ze základních prvků, na kterých stojí Bitcoin, jsou přímé transakce mezi uživateli. Transakce, jak již bylo řečeno, nezahrnují osobní data a v případě nevyzrazení těchto osobních dat je velmi složité dopátrat jednotlivé účastníky transakce. Tato pseudoanonymita se může z pohledu legislativy jevit nežádoucí. Z pohledu současné legislativy je možné čerpat z vyjádření České národní banky [47], podle které tyto vzájemné transakce mezi uživateli nejsou žádnou platební službou. Tudíž nespadají pod zákon o platebním styku (ZPS), stejně jako nákup či prodej bitcoinů.

4.3.2 Směnárny a burzy

V předchozí části byly uvedeny rozdíly v požadavcích na ověření uživatelského účtu. Tyto rozdílné požadavky na osobní údaje jsou způsobeny různými regulačními opatřeními, podle kterých je s kryptoměnami nakládáno ve státech, ve kterých jsou tyto služby provozovány. Vzhledem k tomu, že česká legislativa nepovažuje Bitcoin za peníze, nejsou na směnárny s Bitcoinem kladeny stejné požadavky jako na klasické směnárny. Podle české národní banky [47] totiž směna bitcoinů za české koruny nevykazuje znaky směnárenské činnosti, která je definovaná jako: *„směna bankovek, mincí nebo šeků znějících na určitou měnu za bankovky, mince nebo šeky znějící na jinou měnu.“*. Klasické směnárny tak podléhají regulaci podle zákona o směnárenské činnosti. Podle tohoto zákona, mohou směnárenskou činnost vykonávat banky, spořitelní družstva, česká národní banka, směnárníci a další podobné subjekty. Pro získání povolení směnárenského povolení je také potřeba splnit řadu požadavků. V případě, že by kryptoměny spadali pod stejnou definici, jako standardní měny musely by tak i směnárny s kryptoměnami v České republice splňovat tyto nároky.

4.3.3 Výjimky

Podle České národní banky [47] bitcoiny nejsou investičními nástroji, jelikož nesplňují charakteristiku cenných papírů. Ovšem v případě obchodování derivátů na bitcoiny mohou naplňovat znaky investičních nástrojů. V takovém případě může být nutné povolení. Stejně tak by bylo nutné povolení v případě fondu investujícího do kryptoměn. Poslední výjimkou je pokud by byly naplněny znaky platební služby například u Bitcoinové burzy.

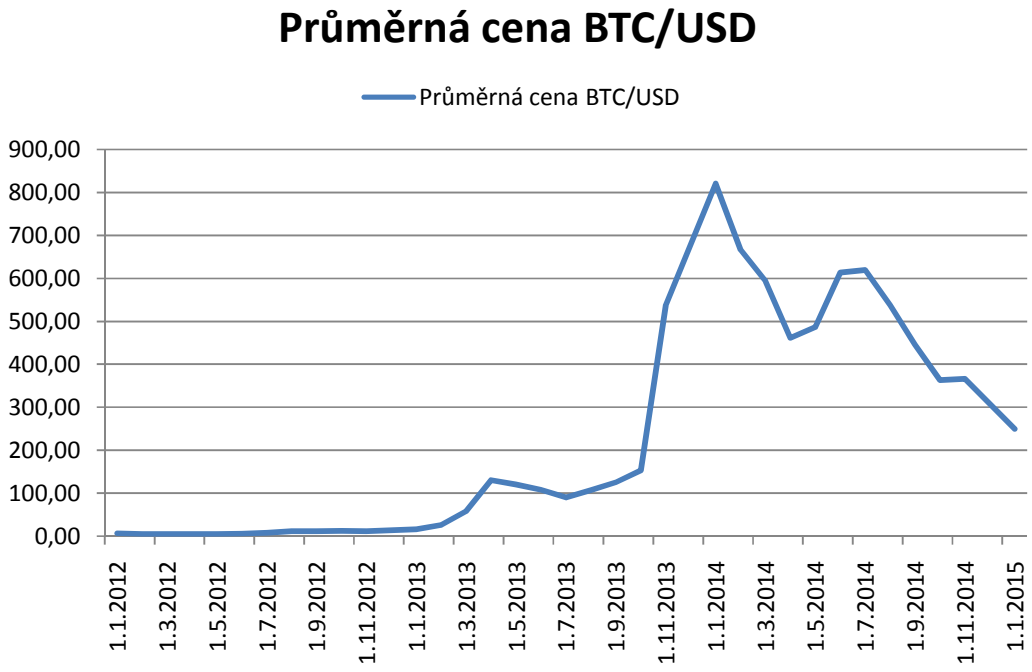
Zařazení a tudíž i případné regulování kryptoměn není jednoduché. Ovšem Evropská centrální banka [56] v době psaní tohoto textu nepovažovala za nutné rozšíření současných právních rámců evropské unie. Podobných názorů je také Česká národní banka [47], která nepovažuje Bitcoin za měnu a tudíž její standardní využití nepodléhá regulaci. V České republice stejně jako v dalších zemích Evropské unie podléhá určité formě regulace pouze nabízení určitých služeb, ve kterých dochází k využívání Bitcoinu a dalších podobných měn. Jedná se tak o směnárny a další podobné služby, u kterých je vyžadováno, aby jejich provozovatel měl příslušnou licenci. Zdá se tedy, že využívání kryptografických měn není stále tak rozšířené, aby bylo cílem nějaké výraznější regulace ze strany evropské unie. Je tedy otázkou při jak vysoké rozšířenosti kryptoměn by se Evropská unie začala více angažovat v regulaci těchto projektů. Kryptoměny jsou stále jen okrajovou záležitostí v porovnání s kreditními kartami a

dalšími platbami. V případě, že bude tento podíl narůstat, je možné očekávat zvyšující se zájem centrálních autorit zavést určité formy regulačních mechanismů. Dalším možným problémem může být široká regulace určitých problému, do kterých budou spadat také kryptoměny. Příkladem může být výše zmíněná směrnice o DPH. Cílem nařízení je sice umožnit lepší vybírání daní, ale vzhledem k tomu, že kryptoměny jsou podle stávající definice elektronickou službou, budou tímto zákonem také ovlivňovány. Kryptoměnám by tak nejvíce prospělo stanovení samostatné kategorie, do které by zhlediska legislativy spadaly.

5 Praktická část

5.1 Cena

V předchozí části textu, která se věnovala charakteristickým znakům, byl Bitcoin popsán jako decentralizovaná měna, která nespoléhá na regulaci státních a jiných institucí. Volné prostředí má značný efekt na cenu. Jak je vidět na grafu č. 1, za období posledních tří let, se měsíční průměrná cena, během několika měsíců měnila řádově ve stovkách dolarů za jeden bitcoin. Výkyvy kolísání ceny je možné blíže porovnat pomocí volatility.



Graf 1 Vývoj ceny od roku 2012 do začátku roku 2015. Zdroj Blockchain [26]

5.2 Volatilita

Volatilita je veličina, která popisuje kolísání hodnoty určitého aktiva v daném časovém období. Čím je volatilita nižší, tím stabilnější je cena aktiva v čase. Naopak při vysoké volatilitě je cena nestabilní a v průběhu času se značně mění, lze tak hovořit o rizikovějším aktivu, s více nepředvídatelnou cenou. Jak popisuje Houstecky, P. [74]Volatilita se značí řeckým písmenem sigma a lze jí rozlišit do několika druhů. Základními jsou historická a implikovaná volatilita. V následujícím textu je vždy počítáno s historickou volatilitou.

Historická volatilita popisuje kolísání hodnot v minulosti, zatímco implikovaná se snaží odhadnout budoucí volatilitu. Historická volatilita se tedy počítá z dat o cenách za dané období. Ve výpočtu se využívají logaritmické denní výnosy a jejich směrodatná odchylka (postup je podrobněji popsán níže). Výhodou historické volatility je relativně snadná dostupnost a zdrojových dat nutných k výpočtu.

Výpočet:
pro výpočet je podle Houstecky, P. [73] potřeba znát základní 3 parametry:

1) Základní časová perioda, na které je volatilita počítána
2) Počet těchto časových period ve výpočtu
3) Počet period v roce pro převedení volatility na roční

Postup výpočtu:

1) Výpočet logaritmických výnosů

   $$R_n = ln\left(\frac{C_n}{C_{n-1}}\right)$$

   Ln přirozený logaritmus

   Cn = uzavírací cena

   Cn-1 = uzavírací cena předchozího dne

2) Výpočet směrodatné odchylky logaritmických výnosů

   Výpočet směrodatné odchylky pro logaritmické výnosy se skládá ze tří mezikroků:

   Výpočet aritmetického průměru:

   $$R_{avg} = \frac{\sum_{i=1}^{n} R_i}{n}$$

   Výpočet čtvercové odchylka

   $$\left(R_i - R_{avg}\right)^2$$

   Výpočet rozptylu

   $$\sigma^2 = \frac{\sum_{i=1}^{n}\left(R_i - R_{avg}\right)^2}{n-1}$$

Výpočet směrodatné odchylky

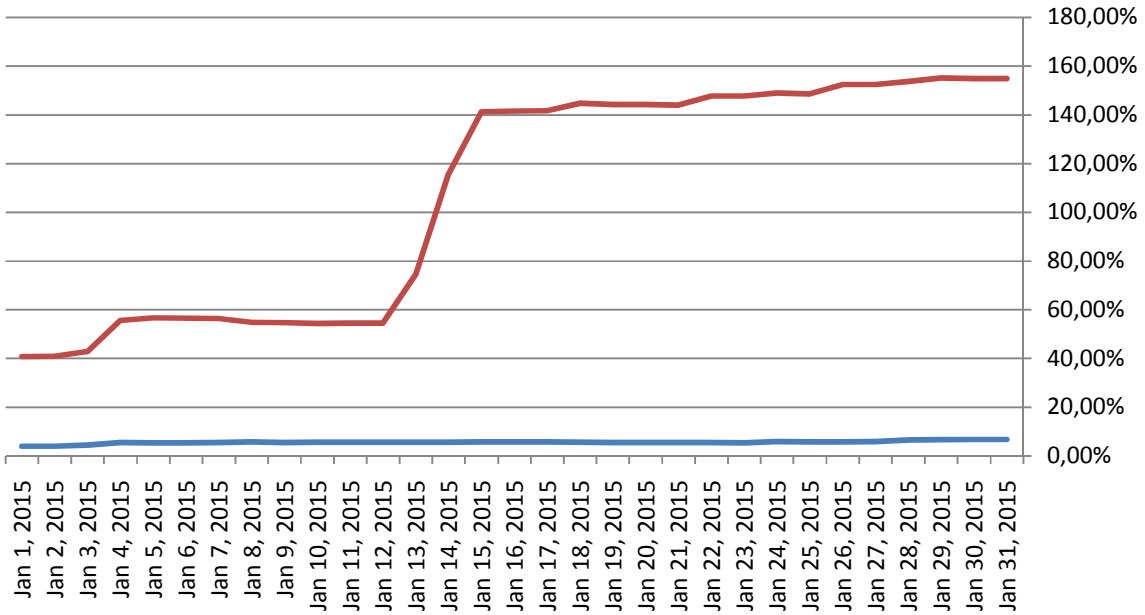
$$\sigma = \sqrt{\frac{\sum_{i=1}^{n}(R_i - R_{avg})^2}{n-1}}$$

3) Převedení volatility na roční

   Podle Carola, A. [36] se volatilita většinou uvádí jako anualizovaná. Jedná se o vynásobení volatility odmocninou z počtu sledovaných období v roce. Například při porovnávání denních údajů se násobí číslem 365.

   $\sigma_{roční} = \sigma\sqrt{T}$

Konkrétní výpočet třiceti denní anualizované volatility za je uveden v grafu č. 2. Jak je vidět, historická volatilita Bitcoinu byla na velmi vysoké úrovni. Anualizovaná volatilita často překročila i hodnotu 100 %. Při porovnání s volatilitou britské libry je vidět jak veliký rozdíl je mezi oběma měnami. Zatímco u libry se volatilita dlouhodobě pohybuje okolo 7 % u Bitcoinu se mění a její hodnoty jsou často i deset krát větší.



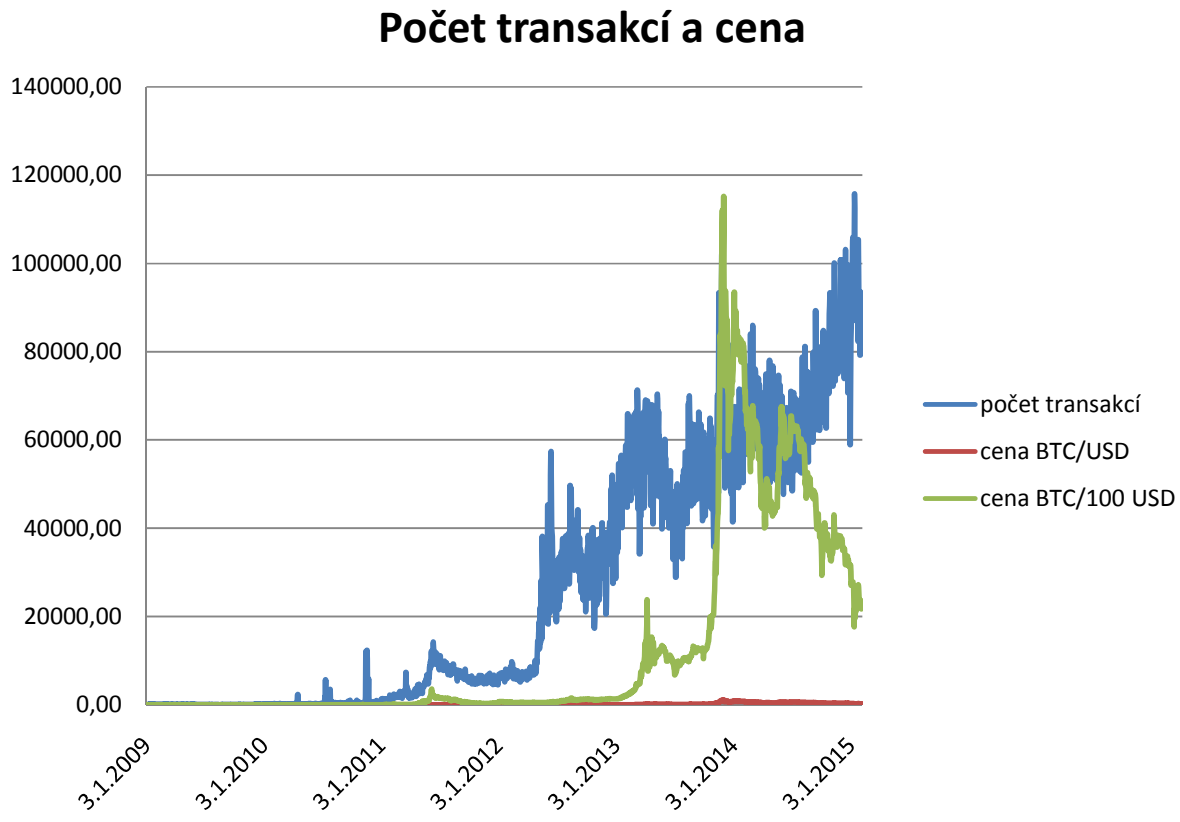
Graf 2 Volatilita Bitcoinu a amerického dolaru. Vlastní zpracování. Zdroj dat: Blockchain [26], Oanda [91]

Jelikož hlavní představa o využití Bitcoinu je umožnit jeho pohodlné využívání jako platebního prostředku, vysoká volatilita způsobuje několik problémů. Podle následovníků

keynesiánské ekonomické teorie [5] definuje peníze několik základních funkcí. Měly by dobře sloužit jako účetní jednotka, prostředek směny a také jako uchovatel hodnoty. Vysoká volatilita značící výrazné výkyvy v cenách tak naznačuje, že jako prostředek k uchování hodnoty se bitcoiny jeví rizikové, toto může být jeden z důvodů, proč více jak 95% uživatelů má podle Bitcoinrichlist [16] ve svých Bitcoinových peněženkách uloženo méně jak 0,001 BTC. Tedy o něco méně než jeden americký dolar, podle hodnoty z února 2015. Dalším problémem vysoké volatility je přijímání bitcoinů obchodníky. V případě, že obchodník přijímá bitcoiny, které následně nechává v peněžence, vystavuje se riziku propadu ceny, která může způsobit vyvolat menší či záporný zisk z této platby. Pokud tak chce obchodník umožnit uživatelům platby bitcoinem a zároveň se vyhnout tomuto riziku, může platby bitcoinem okamžitě převádět do stabilnějších měn. Podle Siedla, R. [105] tak činí většina firem akceptujících bitcoiny. Díky tomuto principu jsou chráněni před vysokou volatilitou, ovšem také se snižuje potenciál měny. Cílem je aby byla využívána k placení a nikoliv, aby sloužila pouze jako prostředek, který bude okamžitě směněn za bezpečnější variantu. Vysoká volatilita se tedy jeví jako problém jak pro obchodníky, tak pro normální uživatele. Výhodou však může být pro spekulanty, kteří vyhledávají rizikové obchody. Vysoká volatilita už principu vytváří příležitosti velmi rychlých výdělků stejně jako ztrát.

5.3 Porovnání počtu transakcí a ceny

Přes vysoké cenové výkyvy by se dalo předpokládat, že cena bude alespoň částečně následovat trend oblíbenosti systému Bitcoinu, a že se rostoucí počet transakcí provedených za určité období alespoň minimálně projeví v podobném celkovém trendu i u ceny. Porovnání těchto dvou parametrů zobrazuje graf č. 3. S využitím počtu denních transakcí a ceny je možné porovnat, zda cenu bitcoinů může ovlivňovat jejich oblíbenost jako platidla.



Graf 3 Vývoj transakcí a ceny. Vlastní zpracování. Zdroj dat: Blockchain [27]

Vzhledem k vysokému počtu transakcí, je pro lepší možnost porovnání v grafu č..3, cena bitcoinů uváděna také jako počet nutný k nákupu 100 bitcoinů. Ze začátku sledovaného období lze pozorovat podobné trendy, jak u počtu transakcí, tak i u ceny. Na začátku června roku 2011 byl cenový vývoj velmi podobný vývoji transakcí. Postupem času však cena stoupala stále strměji, na rozdíl od počtu transakcí, které pozvolně rostly. Cena posléze vystoupala až ke své maximální hodnotě 1151 dolarů za jeden Bitcoin. Tento růst ceny byl následován krachem americké burzy Mt.Gox, která podle Cuthbertson, A. [46] měla tento růst

na svědomí. Takovýto růst způsobilo zdejší algoritmické obchodování, které vyhnalo cenu do těchto neopodstatněných hodnot. K této hodnotě se už od té doby cena zdaleka nepřiblížila, ale naopak začala výrazně klesat. Cena od tohoto maxima klesla na hodnotu 400 dolarů a její pokles doprovázel i občasný pokles počtu transakcí. Ovšem zatímco v dlouhodobém horizontu cena pokračovala v poklesu až na hranici okolo 200 dolarů, počet transakcí naopak stoupal. Z rostoucího počtu transakcí a současně klesající ceny vyplívá, že nestabilní cena nebrání v rozšiřování využívání.

5.4 Porovnání ceny a událostí

Kromě oblíbenosti mohou být pro cenový vývoj také důležité informace a zprávy související s regulacemi, přijímáním kryptoměn obchodníky a další důležité související informace. Jak již bylo popsáno v kapitole věnované charakteristice, Bitcoin značí pouze záznam o přijetých mincích a hodnota je tvořena především důvěrou uživatelů. Z těchto vlastností vyplívá složitost určení jejich hodnoty. U klasických měn ručí za jejich hodnotu vláda a u akcií je možné do jisté míry určit skutečnou hodnotu společnosti alespoň podle vlastněného majetku. Značným problémem Bitcoinu nemožnost snadného určení této hodnoty. Díky tomuto problému se tak uživatelé musí mnohem více spoléhat na zdroje informací, které mají větší vliv na cenu. Tabulka č. 4 zobrazuje cenu Bitcoinu v poměru k americkému dolaru a k významné události, pro porovnání jejich možného dopadu na cenu. Po negativních událostech, jako například v Únoru po uzavření směnárny Mt.gox, stejně jako po zprávách oznamujících, že čínská vláda se chystá zakázat Bitcoin, následoval předpokládaný negativní pohyb ceny. Naproti tomu, u některých událostí, které je možné označit jako pozitivní, se očekávaný vliv vůbec neprojevil. Jedná se o oznámení o přijímání bitcoinů jako platidla velkými společnostmi jako je Microsoft a další. U takových to zpráv by se dalo předpokládat, že když takto velká společnost důvěřuje Bitcoinu, bude to mít příznivý vliv na cenu. Růst by se také dal očekávat v případě významných investic do nových firem nabízejících různé služby orientované na Bitcoin a další kryptoměny. Ovšem, jak je vidět z následující tabulky v těchto případech, naopak často následoval pokles ceny. Vliv těchto událostí na cenu je tedy sporný. Některé události jsou následovány odpovídajícím, negativním či pozitivním, pohybem ceny. Na druhou stranu řada dalších událostí, u kterých by se dal očekávat určitý efekt, ale cenový vývoj je následován přesně opačnou reakcí. Pro opravdu spolehlivé závěry by bylo nutné analyzovat mnohonásobně vyšší počty událostí, než je prezentováno v tabulce. Cílem této

prezentace dat uvedených v tabulce č. 4 je tedy spíše zobrazit, jak nepředpokládaný vývoj ceny může následovat po určitých událostech.

Datum	Událost	Cena	Cena za 10 dní	Změna (%)
8. 2. 2014	Směnárna Mt.Gox v problémech[2]	707	626,77	-11,35%
28. 3. 2014	Zprávy o zákazu bitcoinu v Číně [3]	503	447,74	-10,99%
13. 5. 2014	Bitpay získává investici 30 milionů dolarů[4]	438,95	527,47	20,17
29. 5. 2014	Dish akceptuje bitcoin[5]	568	652	14,789
3. 6. 2014	Apple po dlouhé době povoluje bitcoin aplikaci v obchodě applestore[6]	673,9	582	-13,64
18. 6. 2014	Dell začíná přijímat platby[7]	604,6	597,08	-1,24
26. 9. 2014	Paypal přijímá bitcoin[8]	405,14	331,2	-18,25
14. 11. 2014	Coinbase získává investici 50 milionů dolarů[9]	396,56	384	-3,17%
17. 11. 2014	Aukce 50 tisíc zabavených bitcoinů[10]	378,48	372,62	-1,55g
14. 12. 2014	Microsoft začíná přijímat platby bitcoinem[11]	350,31	336,96	-3,81

Tabulka 4 Události a následný vývoj ceny. Zdroj dat o cenách Blockchain [26]

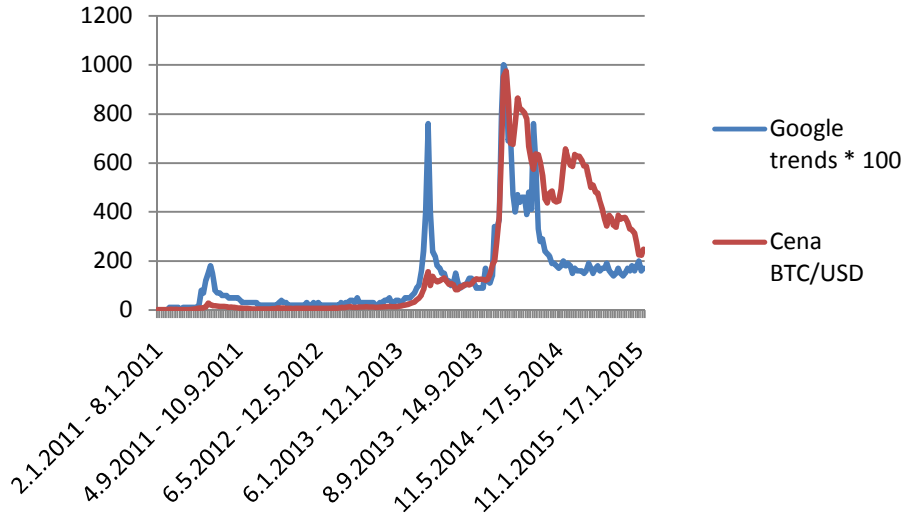
5.5 Porovnání ceny a Google trends

S oblíbeností, stejně jako se zprávami souvisí také frekvence vyhledávání v internetových vyhledávačích. Různé události tak mohou vyvolávat různý zájem o vyhledávání a tento zájem, se posléze může také projevovat také na ceně. Trendy ve vyhledávání je možné prozkoumat pomocí analytických nástrojů společnosti Google. Google trends je webový nástroj

[2] http://www.coindesk.com/mt-gox-first-bitcoin-exchange-dead/
[3] http://moneymorning.com/2014/03/28/bitcoin-prices-tank-rumors-china-ban/
[4] http://fortune.com/2014/05/13/bitpay-payment-company-snags-30-million-investment/
[5] http://www.coindesk.com/dish-becomes-worlds-largest-company-accept-bitcoin/
[6] https://www.cryptocoinsnews.com/apple-reverses-anti-bitcoin-app-policy-allows-mobile-wallets-back-apple-store/
[7] http://techcrunch.com/2014/07/18/dell-now-accepts-bitcoin-for-all-online-u-s-purchases/
[8] http://money.cnn.com/2014/09/26/technology/paypal-bitcoin/
[9] http://techcrunch.com/2014/11/14/coinbase-desparately-seeking-series-c/
[10] http://pando.com/2014/11/17/us-marshals-auction-50000-more-bitcoins-seized-from-silk-road/
[11] http://www.gizmag.com/microsoft-accepts-bitcoin/35209/

umožňující prozkoumávat trendy ve vyhledávání. Pomocí této služby je možno prozkoumat zadaná klíčová slova a zobrazit relativní počet vyhledávání k celkovému počtu vyhledávání na tomto vyhledávači. V grafu se data zobrazují jako hodnoty od 0 do 100, přičemž 0 značí nedostatek dat a 100 vrcholný zájem. Data tedy nezobrazují konkrétní počty kolikrát bylo toto slovo hledáno, ale lze na nich pozorovat vzrůstající či klesající relativní zájem uživatelů o tato vyhledávání.

Následující graf zobrazuje 7 denní průměrnou cenu v porovnání s hodnotou Google trends. Tato hodnota je pro lepší přehlednost a porovnání ještě vynásobena koeficientem 100. Na začátku období se jednalo o neznámý projekt, kterému hlavní zpravodajská média nevěnovala příliš zájmu. Z grafu č. 5 je vidět, jak po první přibližně jeden a půl roku je cena i zájem o vyhledávání velmi nízký. V březnu 2013 se však začal projekt Bitcoinu dostávat do zpravodajství a potřeba dodatečných informací tak vyvolávala nárůst ve vyhledávání. Tento výrazně větší zájem o vyhledávání také koresponduje s růstem ceny. Další období kdy lze pozorovat podobný trend u vyhledávání i u ceny je okolo října 2013, kdy byla cena vyhnána až na dosavadní maximum. Od tohoto okamžiku se však obě křivky rozcházejí a vývoj ceny se již dále nepodobá zájmu o vyhledávání. Jako nejpravděpodobněji vysvětlení se jeví, že se zprávy a informace o Bitcoinu dostaly k dostatečnému počtu lidí a tudíž zájem o vyhledávání od této doby nezaznamenává další výrazné nárůsty.



Graf 4 Porovnání ceny a Google trends. Vlastní zpracování. Zdroj: Blockchain [26], Google trends [64]

5.6 Burzy

Cena je jako u většiny ostatních aktiv nejpříměji ovlivňována poptávkou a nabídkou. Na trhu již funguje celá řada burz či směnáren, kde je možné obchodovat s kryprografickými měnami. Kromě Bitcoinu se nejčastěji obchoduje také Litecoin a Dark coin. Bitcoinových burz existuje značné množství, ovšem značný podíl na trhu si rozděluje pouze několik největších společností. V době psaní tohoto textu evidoval Coinmarketcap [44] aktivních 36 burz nabízejících obchodování různých měnových párů. Z tohoto počtu 28 obchodovalo více jak 10 000 dolarů a pouze 12 více jak 100 000 dolarů denně. Největších 5 společností v čele s BTC-china si tak drží více jak 90% podíl na trhu. Nejvíce se bitcoiny obchoduje na čínském a americkém trhu, respektive za čínský juan a americký dolar. Největšími americkými burzami tak byli Bitfinex a Bitstamp. Ve značném kontrastu tak působí porovnání amerického trhu s čínským. Na čínské burze působící Btc-china, která je absolutně největší burzou s kryptografickými měnami, se tak za den zobchoduje třikrát více bitcoinů než na předchozích zmíněných amerických burzách.

1	BTCChina	BTC/CNY	32 797 300 USD	233.67	47,56%
2	BtcTrade	BTC/CNY	15 786 400 USD	234.31	22,89%
3	Bitfinex	BTC/USD	7 879 880 USD	233.63	11,43%
4	OkCoin Intl.	BTC/USD	3 730 220 USD	233.89	5,41%
5	Bitstamp	BTC/USD	2 115 520 USD	233.43	3,07%
6	Coinbase Exchange	BTC/USD	2 099 840 USD	233.98	3,05%
7	BTC-E	BTC/USD	2 081 530 USD	225.12	3,02%
8	LakeBTC	BTC/USD	881 851 USD	235.39	1,28%
9	Yunbi	BTC/CNY	253 304 USD	234.35	0,37%
10	Coinsetter	BTC/USD	244 709 USD	233.56	0,35%
11	itBit	BTC/USD	241 415 USD	233.81	0,35%
12	Bitonic	BTC/EUR	101 653 USD	230.03	0,15%
13	BitBay	BTC/PLN	98 747 USD	237.10	0,14%
14	HitBTC	BTC/USD	78 662 USD	249.01	0,11%
15	Exmo	BTC/RUB	75 764 USD	239.06	0,11%

Tabulka 5 Tržní podíly jednotlivých burz. Zdroj: Coinmarketcap [43]

5.7 Konkrétní burzy

5.7.1 Otevření účtu a poplatky

5.7.1.1 Bitstamp

Pro samotné otevření účtu u této společnosti je potřeba pouze vyplnit základní údaje o uživateli. Založení je jednoduché a rychlé, ovšem ověření účtu, které umožní vkládat a vybírat finanční prostředky a obchodovat s nimi, je složitější. Společnost vyžaduje osobní doklad, kterým může být cestovní pas, občanský průkaz nebo řidičský průkaz. Dále je potřeba doklad o pobytu, jako který může posloužit například výpis z bankovního účtu.

5.7.1.2 Bitfinex

Bitfinex podobně jako Bitstamp, požaduje zadání základních údajů a navíc také umožňuje výběr mezi odlišnými druhy účtu, podle požadovaného využití. Pro vkládání amerických dolarů je také potřeba ověření účtu. Ověření účtu opět spočívá v zadání bankovních a osobních informací a navíc ještě ve vyplnění dodatečného formuláře. V případě převádění financí bankovním převodem si Bitfinex účtuje minimální poplatek 20 dolarů. Naproti tomu také umožňuje vybírat a vkládat finanční prostředky pomocí normálních Bitcoinových transakcí. A to celé bez ověření účtu.

5.7.1.3 Btc-e

Je ruská společnost provozující burzu, na které je možno obchodovat, kromě Bitcoinu také Namecoin, Litecoin nebo Ppcoin. Kryptoměny je možné obchodovat v páru s eury, dolary, čínskými juany a ruskými rubly. Založení účtu je jednoduché a společnost umožňuje výběry i vkládání libovolné měny bez nutnosti ověření účtu.

5.7.1.4 Okcoin

OK coin umožňuje obchodovat Bitcoin a Litecoin. Ověření účtu u této společnosti spočívá systému založenému na úrovních, které určují, jaké částky může uživatel vložit a jakým způsobem. První úroveň, která umožňuje neomezené vkládání a vybírání kryptoměn a to až do výše 2000 dolarů za den. Pro získání první úrovně ověření je vyžadováno ověření emailu a vyplnění základních osobních dat. Přičemž data stačí vyplnit a účet je ověřen bez hlubší kontroly jejich pravosti.

5.7.1.5 LakeBtc

Další čínská burza obchodující bitcoin za americké dolary nebo čínské juany. Pro vložení financí bankovním převodem je opět potřeba ověření. Ověření zahrnuje naskenování identifikačních dokumentů a zadání dalších osobních údajů. Kromě bankovního převodu je možné vložit prostředky přes bitcoinové transakce nebo přes Ripple, které byl věnován prostor již dříve.

	Poplatky za vložení		Další poplatky			Poplatky za výběr	
Burza	BTC	Bankovní převod	Transakce (%)	Maker (%)	Taker (%)	BTC	Bankovní převod
LakeBTC[12]	Zdarma	Zdarma	x	0,15	0,2	Zdarma	5 + %
Okcoin[13]	Zdarma	Zdarma	x	0,1	0,2	Zdarma	15 + %
Bitstamp[14]	Zdarma	0,05 % (Min. $7,5)	0,25-0,10	x	x	Zdarma	0,09 % (Min. $15)
Btc-e[15]	Zdarma	$20	0,2	x	x	Zdarma	x
Bitfinex[16]	Zdarma	$20	x	0,1	0,2		20

Tabulka 6 Poplatky na jednotlivých burzách. Vlastní zpracování. Zdroj: oficiální webové stranky společností

	Ověření		Bezpečnost			
Burza	Sken dokladů	potvrzení pobytu	osobni data	historie přihlášení	sms ověření	google authentificator
LakeBTC[17]	1	0	1	1	0	1
Okcoin[18]	0	0	1	1	1	1
Bitstamp[19]	1	1	1	1	0	1
Btc-e[20]	0	0	0	1	0	1
Bitfinex[21]	1	1	1	1	1	1

Tabulka 7 požadavky na otevření účtu a bezpečnost. Vlastní zpracování. Zdroj: oficiální webové stránky společností

5.7.1.5.1.1 Maker-taker systém

Činnost jednotlivých společností je financována formou poplatků od zákazníků. Nejčastější jsou dva typy poplatků prvním je zpoplatnění jednotlivých transakcí určitou procentuální sazbou, která se také často mění podle obchodovaného objemu za určitý čas. Druhou možností

[12] https://www.lakebtc.com/s/fees?locale=en
[13] https://www.okcoin.cn/about/fees.do
[14] https://www.bitstamp.net/fee_schedule/
[15] https://btc-e.com/page/2
[16] https://www.bitfinex.com/pages/fees
[17] https://www.lakebtc.com/s/about?locale=en
[18] https://www.okcoin.cn/about/security.do
[19] https://www.bitstamp.net/account/security/two-factor-authentication/
[20] https://btc-e.com/reg
[21] https://www.bitfinex.com/pages/security

je takzvaný Maker-taker model. V tomto modelu jsou dva poplatky jeden "maker" obvykle nižší a druhý "taker". Podle společnosti Coinfloor [42] jsou maker poplatky placeny když uživatel prodává za vyšší, nebo nakupuje za nižší cenu, než je aktuální burzovní cena. Taker poplatek je placen v ostatních případech. Společnosti tak vpodstatě odměnují makery za vkládání likvidity nižšími poplatky.

5.7.2 Možnosti obchodování

5.7.2.1 Nákup/prodej

Standardní nákup nebo prodej určitého měnového páru podle určitého kurzu. Jedná se o základní prvek, který nabízejí všechny burzy. Některé burzy jako například OK coin nabízejí pokročilejší funkce, kdy je možné nastavit cenu, která když bude dosažena, tak se provede nákup nebo prodej a další pokročilé příkazy možnosti.

5.7.2.2 Maržové obchodování (margin trading)

Tato možnost spočívá ve využití úvěru k obchodování. Uživatel si tak vypůjčí určitou částku, se kterou obchoduje. Po uzavření svého obchodu vrátí tuto částku a úroky. Maržové obchodování nabízejí společnosti jako Bitfinex, Ok coin, Campbx a další.

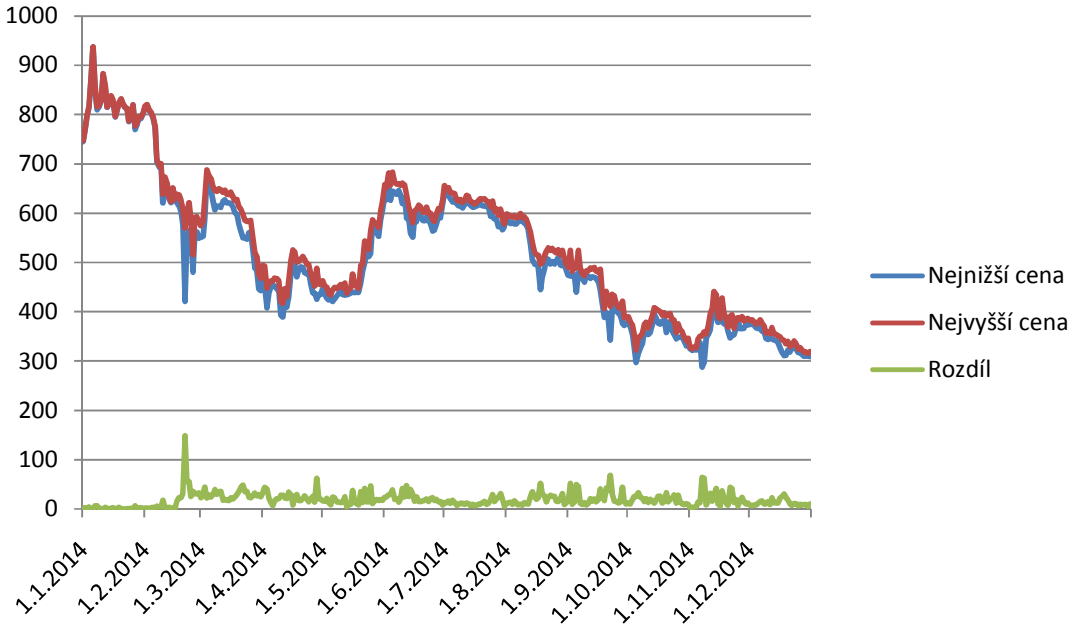
5.7.2.3 Futures

Kromě obchodování měnových párů, ať se jedná o páry kryptografických měn nebo jde o spojení s klasickou měnou jako je dolar či euro, umožňují některé burzy obchodovat také takzvané futures kontrakty. Jak již název napovídá futures kontrakty spočívají ve stanovení budoucího data a ceny, za které bude realizován prodej či nákup. Podle Tylečky, J. [109], lze futures kontrakty charakterizovat jako určitou dohodu dvou stran o nákupu, nebo prodeji určitého množství za předem danou cenu k budoucímu datu. Futures kontrakty lze obchodovat komodity jako je zlato, ropa a další, akcie měnové páry nebo právě kryptoměny. Jak dodává Tylečka, J. [109] u futures kontraktu se obchodník zavazuje při nákupu zaplatit a při prodeji fyzicky dodat požadované množství. Cílem obchodníka však často není fyzicky vlastnit dané aktivum, ale spíše realizovat zisk na zvýšení či poklesu kurzu. Proto se u futures kontraktu realizuje zisk vytvořením protipozice. Nejjednodušeji lze vysvětlit fungování futures kontraktů na konkrétním příkladu. V určitý den je cena bitcoinu 350 USD za jeden kus. Obchodník předpokládá, že kurz bude růst, tak uskuteční futures kontrakt, kde se zaváže, že za 30 dní nakoupí 10 bitcoinů za cenu 350 dolarů. Za 30 dní kurz vzroste na 370 dolarů za btc, ale obchodník nakoupí za 350 a zároveň je prodá za 370, tím realizuje zisk 200 dolarů, aniž by

fyzicky musel nějaké bitcoiny obdržet. Futures kontrakty je možné obchodovat na burzách jako je Okcoin nebo Orderbook.

5.7.3 Cena a směnárny

Kromě rozdílů v obchodovaných párech, poskytovaných službách a poplatcích se burzy liší také cenou. Graf č. 6 zobrazuje porovnání rozdílu cen zahrnujících data ze směnáren Bitstamp, Bitfinex, BTC-e, Bitkonan, LakeBTC, 1coin a Kraken. V grafu jsou vždy uvedeny nejnižší a nejvyšší cena z výše uvedených směnáren pro konkrétní den. Průměrná nejnižší cena za sledované období byla 515,53 a nejvyšší 534,24. Rozdíl mezi nejlevnějšími a nejdražšími nabídkami tak průměrně činil 18,71 dolaru.



Graf 5 Rozdílné ceny na burzách. Vlastní zpracování. Zdroj: Quandl [98]

Každá ze směnáren tedy nabízí rozdílné ceny, tabulka č. 8 porovnává podíl jednotlivých směnáren na nejnižších a nejvyšších cenách. Za sledované období měla nejčastěji nejnižší cenu směnárna BTC-E, která ji držela téměř v padesáti procentech roku 2014. Naopak nejvyšší ceny držela směnárna Bitkonan. Naprosto nejvyšší rozdíl mezi jednotlivými cenami byl také u této směnárny a jednalo se o více jak 100 dolarový rozdíl.

Směnárna	Minimální cena (%)	Maximální cena (%)
Bitstamp	8,77%	7,95%
Bitfinex	7,12%	11,23%
BTC-e	46,58%	0,00%
Bitkonan	11,78%	32,60%
LakeBTC	10,68%	9,86%
1coin	8,77%	15,07%
Kraken	6,30%	23,29%
Celkem	**100,00%**	**100,00%**

Tabulka 8 Podíly jednotlivých burz na minimálních a maximálních cenách. Vlastní zpracování. Zdroj dat: Quandl [98]

5.7.4 Porovnání poplatků za transakce

V předchozí části bylo popsáno, že jednou z výhod Bitcoinu mohou být velmi levné zahraniční platby, jelikož Bitcoin se vyznačuje velice nízkými poplatky za transakce. Jednotlivé transakce i s poplatky zobrazuje web Blockexplorer [96]. Například blok 343197 zahrnoval 1647 transakcí a celkem zahrnoval přibližně 0,265 BTC na poplatcích. Průměrný poplatek tak byl 0,000161 BTC a zdaleka nejčastější poplatek byl 0,0001 BTC. Tento poplatek tak odpovídá přibližně 50 haléřům za transakci. Při porovnání s mezinárodními platbami v rámci klasických bank je tak vidět značný rozdíl. Zatímco mezinárodní transakce prováděné pomocí bitcoinů jsou velmi levné a relativně rychlé. Problém nastává, pokud by uživatel chtěl provést transakci v rámci klasických měn a platbu bitcoiny využít, pouze k provedení transakce. V takovém případě je nutné využít směnáren, které si často účtují poplatky a také celou transakci prodlužují. Pro částečné vyřešení těchto problému je možné, využití například služby Ripple, která tyto umožňuje vložit různé druhy peněz a poté je odeslat v rámci vlastního protokolu. Ovšem i tento postup není ideální a vyžaduje, aby i druhá strana měla u této služby účet.

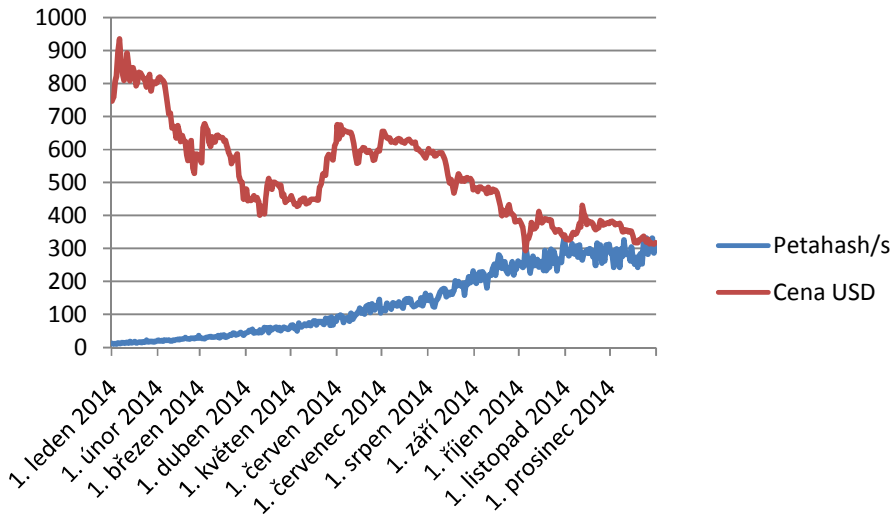
Banka	Poplatek za mezinárnodní plabu
Airbank[22]	100,00 Kč
Zuno[23]	280,00 Kč
Fio[24]	100,00 Kč
Gemoney [25]	220,00 Kč
Raiffeisen[26]	300,00 Kč

Tabulka 9 Poplatky za mezinárodní platby u českých bank. Vlastní zpracování. Zdroj dat: sazebníky bank

5.7.5 Význam poplatků

Veškeré poplatky z transakcí v bloku připadají těžaři, který tento blok vytvoří. Kromě těchto poplatků náleží těžaři ještě odměna, která v době psaní tohoto textu činila 25 BTC za blok. V případě výrazného poklesu ceny však tak budou mít vytěžené mince nižší hodnotu. Cena od Ledna do Prosince 2014 klesla téměř 700 dolarů za kus. Růst či pokles ceny je také často následován stejnou rekcí u výkonu výpočetní sítě. Ovšem nelze říci, že by na sobě tyto dva parametry přímo závisely. Přes dlouhodobě klesající cenu a tudíž nižší hodnotu odměn pro těžaře, celkový výkon Bitcoinové sítě neustále stoupá. Výkon také ovlivňuje mnoho dalších parametrů jako, je vývoj těžebního hardwaru a ceny elektrické energie a dalších nákladů nutných pro těžení. Firmy nabízející tento hardware se snaží zvyšovat výkon a zároveň omezovat nároky na elektrickou energii. Vzhledem k snižující se ceně a zvyšujícímu se výpočetnímu výkonu, byla například společnost Cex [37] nucena dočasně pozastavit takzvaný cloud mining, který spočívá v pronájmu těžebního výkonu uživatelům. Pro těžaře je tedy cena značně důležitým faktorem. Je značný rozdíl, jestli odměna 25 BTC za vytěžení bloku bude mít hodnotu 15,5 tisíce dolarů jako v Červenci roku 2014 nebo přibližně polovinu jako na konci stejného roku. Motivace těžařů k poskytování svého výpočetního výkonu tak může často záviset na celkové ceně.

[22] https://www.airbank.cz/cs/bezny-ucet/cenik-a-poplatky/cenik/
[23] http://www.zuno.cz/pomoc/uzitecne-informace/cenik/
[24] www.fio.cz/o-nas/dokumenty-ceniky/ceniky-sazebniky
[25] https://www.gemoney.cz/dokumenty-ke-stazeni/sazebniky?docid=1316
[26] https://www.rb.cz/attachments/ceniky/cenik-pi-1-011214.pdf



Graf 6 Výkon Bitcoinové sítě(hash rate) a cena. Zdroj Blockchain [24]

Kromě odměny za vytvoření bloku náleží těžaři i všechny poplatky za transakce zahrnuté v tomto bloku. Za posledních 1000 bloků vytvořených mezi 31. 12. 2014 a 25. 12. 2014 byla průměrná výše poplatků přibližně 0,09 BTC což je při průměrné ceně 317,6 USD/BTC zhruba 28 dolarů. Odměna za vytvoření bloku činila 25 BTC, což bylo přibližně 7944 dolarů. Je tak zřejmé, že poplatky v tomto období mají jen mizivý podíl na celkovém zisku z bloku a jejich velikost je v porovnání s výši odměnou téměř zanedbatelná. Do budoucna se ovšem význam poplatků může značně měnit, jak již bylo uvedeno v kapitole věnované parametrům Bitcoinu, Bitcoin je navržen tak, aby se velikost těchto odměn půlila každých 210000 bloků. Po každém dalším půlení této odměny se tedy význam poplatků bude zvyšovat.

V době psaní tohoto textu bylo vytěženo 344 819 bloků do dalšího půlení a tedy snížení odměny z 25 na 12,5 BTC zbývá vytěžit 75181 bloků. Síť automaticky upravuje složitost a vytěžení bloku tak, aby trvala 10 minut, díky tomuto je možné odhadnout, že k dalšímu půlení dojde v druhé polovině roku 2016. Jelikož nic nenaznačuje, že v budoucnu by mohlo dojít k velmi výraznému snížení spotřeby elektrické energie a těžebního hardwaru, lze tak do budoucna očekávat určité zvýšení poplatků, nebo zavedení jiné formy financování těžby.

5.8 Analýza ilegálního využití kryptoměn

V kapitole o bezpečnosti bylo upozorněno na několik vlastností, které mohou být lehce zneužity k ilegálnímu využití. Jednalo se především o pseudoanonymní systém a složitost

regulace. Níže jsou rozebrány některé případy, kdy byly kryptoměny přímo či nepřímo využity k páchání ilegálních činností.

5.8.1 Ilegální tržiště

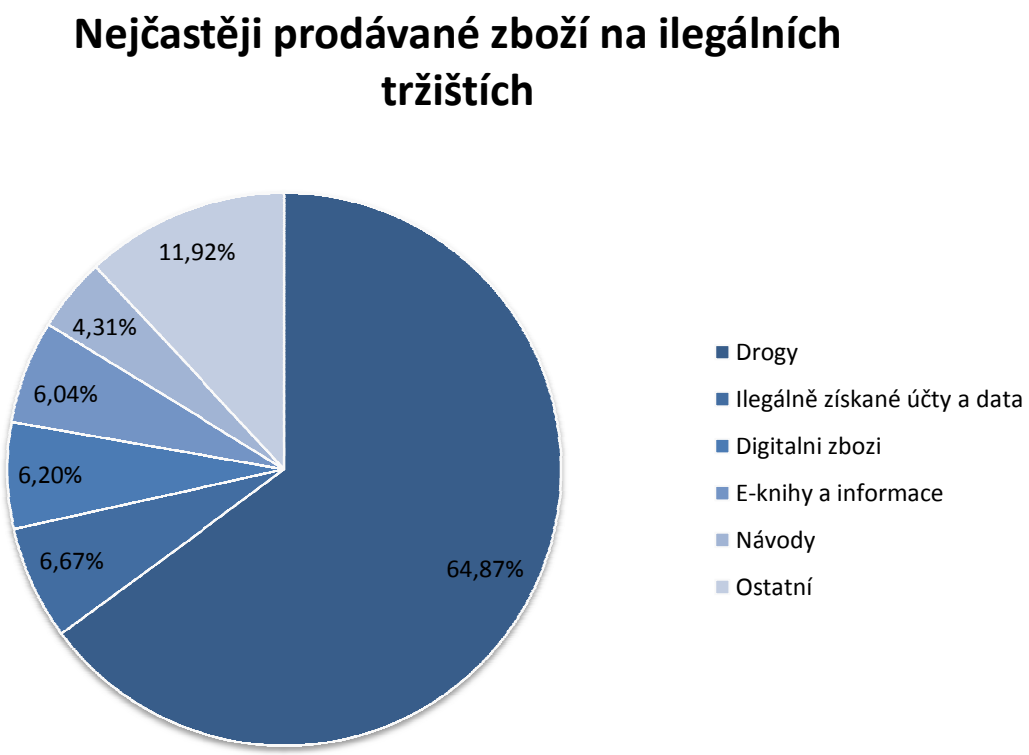
Obtížně vystopovatelné transakce a další parametry kryptoměn, ve spojení s anonymizačními programy usnadňují fungování ilegálních tržišť. Tato tržiště s v mnohém podobají webům jako je například americký Ebay, či české Aukro, ovšem zde však obchoduje s drogami, zbraněmi a podobným ilegálním zbožím. První z podobných služeb byl web Silk road, který fungoval do roku 2013. Na tomto webu se jednalo o ilegální zboží zahrnující zbraně, drogy a další legálně neprodejné zboží. Podle Paglieryho, J. [4] bylo za pouhé dva roky existence, pomocí této služby provedeno přes 1,2 milionu ilegálních obchodů, v celkové hodnotě přesahující 9,5 milionu kusů bitcoinů. Z této částky si web také ukrojil přes 600 tisíc bitcoinů jako provizi. Vysoké zisky z ilegálního obchodu, který mohl přes webové rozhraní navštívit každý zkušenější uživatel, nemohly zůstat bez povšimnutí úředních orgánů. Jak popisuje Flitter, E. [62], v roce 2013, tak byl uzavřen Federálním úřadem pro vyšetřování (FBI). Při razii FBI zatkla hlavní provozovatele webu a také zabavila bitciony v celkové hodnotě přesahující hodnotu 3,6 milionu dolarů. Podobných ilegálních tržišť jsou k nalezení desítky. Takovéto weby jsou zpravidla provozovány na doméně .onion, na kterou se přistupuje přes anonymizační službu Tor. K anonymizaci využívá Tor takzvané cibulové směřování, kdy je komunikace směrována přes řadu uzlů provozovaných dobrovolníky.

Po chvíli prohledávání internetu lze narazit na řadu podobných služeb, či na kompletní a uvádějí pravidelně aktualizované seznamy ilegálních tržišť, jako například na webu Deepdotweb [49]. Pro samotné využívání vyžadují tyto služby velmi jednoduchou registraci. Pro registraci je vyžadováno pouze uživatelské jméno a heslo, zpravidla nejsou vyžadovány ani email či další údaje. Pokročilejší služby vyžadují i bezpečnostní PIN kód, který slouží pro lepší zabezpečení výběrů. Ze zkoumaných tržišť řada opakovaně nefungovala, či se později ukázalo, že se jedná o podvod. Ovšem některé služby vypadají velmi profesionálně a na první pohled není vůbec zřetelné, že nabízejí ilegální zboží. Na prozkoumaných tržištích se celkem nabízelo více jak 48 000 položek. I bez tržiště Agora market, který tvoří téměř polovinu trhu, se jedná o značné množství.

Tržiště	Počet položek	Podíl
Dream Market	783	1,61%
Agora	21000	43,12%
Mr. NiceGuy	1064	2,18%
Abraxas	3527	7,24%
BlackBank	5451	11,19%
AlphaBay	3912	8,03%
nucleus	9407	19,32%
Middleearth	3553	7,30%
celkem	48697	

Tabulka 10 Ilegální tržiště. Vlastní zpracování. Zdroj adres: Deepdotweb [50]

Jednotlivé nabízené druhy zboží zobrazuje graf č. 8. Z nabízeného zboží jednoznačně převažují drogy. Další kategorie si drží velmi velký odstup. Jedná se o různé návody popisující jak prolomit webové stránky, či jak pašovat drogy. Do těchto kategorií digitální zboží, jakojsou pirátské verze softwaru, počítačové viry a další podobné zboží. Dále se jedná se o nelgálně získané účty od společností jako je například Netflix, Uber a podobně. Vzhledem k tomto množství je jisté, že pokud nebude nenalezena efektivní cesta jak, těmto službám zabránit v činnosti bude Bitcoin pro ilegální aktivity ještě dlouho využíván.



Graf 7 Zboží prodávané na ilegálních tržištích. Vlastní zpracování. Zdroj adres: Deepdotweb [50]

5.8.2 Počítačové viry a krádeže zahrnující kryptoměny

Především Bitcoin, ale také ostatní kryptoměny čelí vzhledem k rosoucí ceně a širšímu využívání stále většímu zájmu hackerů. Kryptoměny jsou tak často vystaveny pokusům o krádež či jsou využívány v různých počítačových virech.

5.8.2.1 Ransomware

Jedná se o druh malware, který zabrání v přístupu k infikovanému počítači, za jehož opětovné zpřístupnění vyžaduje zaplacení výkupného. Na infikovaném počítači se zobrazí zpráva oznamující uživateli, že jeho počítač byl zablokován. Tato zpráva je často doplněna o státní znaky, či znaky kontrolních orgánů, aby zvýšila svoji důvěryhodnost. Pro opětovné odblokování obsahu je vyžadováno zaplacení výkupného k čemuž jsou často využívány kryptoměny.

5.8.2.1.1 Cryptolocker

Jedním z příkladů ransomware, který pro zaplacení vyžadoval platbu v bitcoinech byl virus cryptolocker. V případě infikování tímto virem jsou soubory na počítači zašifrovány a na

zaplacení výkupného měl uživatel 72 hodin. Podle Jarvise, K. [78] se do konce roku 2013 se počet infikovaných počítačů pohyboval od 200 do 250 tisíc a na výkupném získali útočníci bitcoiny v celkové hodnotě blížící se milionu amerických dolarů.

5.8.2.1.2 BitCrypt

Dalším příkladem podobných programů je BitCrypt. BitCrypt zašifruje soubory na disku a následně vyžaduje platbu v hodnotě 0,4 BTC k jejich zpřístupnění. Kromě toho také obsahuje virus, který se snaží získat informace z Bitcoinových peněženek. Jak uvádí Perigaud, F. [95] systém BitCryptu byl již prolomen. V souboru s instrukcemi pro uživatele je uvedeno, že soubory jsou zašifrovány šifrou RSA-1024, podle Perigaud, F. [95] využil autor tohoto viru pouze RSA-426, která může být na běžném počítači prolomena v řádu desítek hodin.

5.8.2.1.3 Zneužití počítačů k těžení

Dalším způsobem, kdy dochází k využití kryptoměn je zneužití počítačů k těžení. V takovémto případě je množství počítačů infikováno virem, který je následně využije pro těžení bitcoinů. Podle bezpečnostní analýzy společnosti Mcafee [85] však jediní, kterým tyto viry přinášejí zisk, jsou jejich prodejci.

5.8.2.2 Krádeže

Častým cílem krádeží se stávají především větší směnárny a další služby sdružující uživatele kryptoměn. Jelikož jsou transakce veřejné je však pro pachatele velmi složité převést peníze do jiné měny a nebýt vyzrazen. K jedné z největších krádeží došlo v prosinci roku 2013, kdy bylo z ilegálního internetového tržiště Sheep market ukradeno 96 000 bitcoinů v celkové hodnotě přesahující 60 milionu dolarů. Někteří z uživatelů tohoto tržiště se však snažili uniklé bitcoiny stopovat a dopátrali se až k programátorovi České republiky. Podle Blažka, V. [21] se tento pachatel snažil na začátku roku 2015 převést peníze z bitcionů do českých bank a následně byl odhalen a obviněn z praní špinavých peněz. Následující tabulka zobrazuje přehled některých dalších krádeží bitcoinů.

Datum	Burza	Počet Bitcoinů	Průměrná Cena za 7 dní od krádeže	Přibližná hodnota v době krádeže (USD)
18 Únor 2015	KipCoin[27]	3000	239,8386	719 000
14. Únor 2015	BTER[28]	7170	241,3114	1 730 000
4. Leden 2015	Bitstamp[29]	19000	276,13	5 247 000
2. Březen 2014	Flexcoin[30]	896	636,5943	570 000
17. Listopad 2013	BIPS[31]	1295	642,16	831 592
26. Říjen 2013	Inputs.io[32]	4100	196,4786	806 000
1. Říjen 2013	Canadian Bitcoins[33]	150	119,61	18 000

Tabulka 11 Krádeže zahrnující Bitcoin. Vlastní zpracování. Zdroj dat o ceně: Blockchain [26]

5.8.3 Ponziho schéma

Ponziho schéma je druh investičního podvodu. Jedná se systém, kdy podvodník nabízí investorovi vysoké zhodnocení, která však platí ze vkladů ostatních investorů. Když fond přestane získávat nové investory, přestane být schopný platit výnosy a zhroutí se. První takovýto podvod využívající Bitcion byl hedgeový fond Bitcoin Savings & Trust. Tento "fond" sliboval neskutečně vysoký úrok 7% procent týdně z vložených bitcoinů. Postupem času přestal být fond schopný splácet zisky investorům a tím krýt svoji ilegální činnost a celý podvod byl odhalen. Podle zprávy Komise Spojených států amerických pro cenné papíry a burzu [103], byl pachatel odsouzen k zaplacení 40 milionů dolarů na odškodném a pokutách.

5.8.4 Online kasina

Jak klasická kasína, tak také ty na internetu vyžadují ve většině států různá povolení, jsou regulována a kontrolována. Naproti tomu Bitcoinová kasina, jako je například Satoshidice a další těží z principu kryptoměn, kdy je pro hru potřeba pouze Bitcoinová adresa. Tyto služby často sídlí v zemích, kde jejich činnost není ilegální, ovšem vzhledem k tomu, že jsou dostupné i ve státech kde jsou onilne kasina regulována, je možné jejich činnost, či využívání považovat při nejmenším na hraně zákona. Například již výše zmíněný web Satoshidice se

[27] http://www.newsbtc.com/2015/02/19/chinese-bitcoin-exchange-kipcoin-shuts-claims-losing-3000-btc-hackers/
[28] http://insidebitcoins.com/news/chinese-bitcoin-exchange-bter-claims-theft-of-1-75-million-btc/29913
[29] http://www.zdnet.com/article/bitstamp-bitcoin-exchange-suspended-amid-hack-concerns-heres-what-we-know/
[30] http://www.coindesk.com/bitcoin-bank-flexcoin-close-600000-bitcoin-theft/Flexcoin
[31] http://www.coindesk.com/bitcoin-payment-processor-bips-attacked-1m-stolen/
[32] http://www.wired.com/2013/11/inputs/
[33] http://www.ottawacitizen.com/business/Ottawa+bitcoin+exchange+defrauded+cyber+currency/9628321/story.html

proti možným problémům chrání, tím že vyžaduje od uživatele potvrzení, že se nachází v lokalitě, kde je tato služba legální. Toto potvrzení však spočívá pouze v souhlasu s podmínkami a není nijak kontrolováno. Ovšem vzhledem k pseudoanonymitě kryptoměn, by bylo pro kontrolní orgán velice složité vystopovat jednotlivého hráče, který hraje přesto, že v místě, kde se právě nachází, je tato služba ilegální. Online kasina využívající kryptoměn jsou velice oblíbená. Podle webu Blockchain[28] patří adresy online kasina Satoshidice k jedněm z nejvyužívanějších.

6 Závěr

V této práci byl představen základní pohled na kryptoměny a možnosti jejich využití. Jedním z podcílů bylo porovnání kryptoměn s normálními měnami. Tato část porovnávala především volatilitu neboli výkyvy v kurzu měn. Ukázalo se, že Bitcoin má mnohem vyšší volatilitu než normální měny. Také bylo upozorněno na několik problémů, vyplívajících vysoké kolísavaosti kurzu. Jednalo se především o problémy s uchováním hodnoty a také problémy, které mohou dopadnout na obchodníky. Bitcoin také některými parametry působí spíše jako aktivum než měna.

V následující části byly rozebrány některé cenové vlivy, které by mohly ovlivňovat bitcoin. Řada předpokládaných vlivů se vůbec neprojevila, nebo měla jiný než očekávaný vliv. Především se jednalo o oblíbenost této kryptoměny. I přes narůstající počet transakcí cena stále klesá. Stejně tak tomu bylo i u různých událostí. Zkoumány byly také významné události jako problémy velkých Bitcoinových burz, či přijímání Bitcoinu významnými společnostmi. Po většině událostí nastal naprosto neočekáváný vliv na cenu. Přesto, že některé vyloženě pozitivní události, jako je rozšiřování přijímání Bitcoinu, nebo investice do firem, byly následovány snížením ceny.

V analýze ilegálního využití kryptoměn bylo prozkoumáno několik tržišť s ilegálním zbožím. Počet nabízeného zboží ukazuje oblíbenost Bitcionu pro tento účel. Mezi nejčastěji nabízené zboží patřily především drogy, digitální zboží a různé návody a informace. Stejně tak množství krádeží a využití kryptoměn u počítačových virů, značí velkou oblibu Bitcoinu pro kriminální aktivitu.

Kriminální aktivita, pseudoanonymní transakce a řada dalších vlastností je často trnem v oku pro regulační orgány v jednotlivých zemích. V řadě zemí se spekulovalo zákazu či značném omezení Bitcoinu a dalších kryptoměn. V Evropské unii a České republice zatím nejsou samotné kryptoměny nijak regulovány. Pouze obchodování s nimi často vyžaduje různé licence. V žádné ze zkoumaných zemí nejsou kryptoměny považovány za skutečnou měnu. Problémem je především nízká schopnost státních orgánu adaptovat se na nové technologie a tak kryptoměny zařadit pod určitou legislativní definici. Je také velmi nepravděpodobné, že v nejbližší době bude Bitcoin či jiná kryptoměna uznána skutečnou měnou. V nejbližší budoucnosti je také velmi nepravděpodobné, že dojde ke skutečně masivnímu rozšíření

kryptoměn. Roku 2016 však čeká Bitcoin půlení odměn za těžení, které může vést ke snížení zájmu o těžení či zvýšení poplatků za transakce.

Bitcoin přišel s některými velmi originálními mechanismy a bude tak jistě zajímavé sledovat jakým směrem se vývoj kryptoměn bude ubírat. Bitcoinu by velmi prospěla určitá stabilizace ceny a také snížení volatility, v takovém případě by mohl daleko lépe splňovat požadavky kladené na měny. Již nyní je však znatelný přínos Bitcoinu v technologiích, na kterých staví. Systém, kdy rozhoduje většina výpočetního výkonu, nebo systém veřejné knihy záznamů také přejala celá řada služeb. Celkové vypuštění centrální autority tak nabízí zajímavé možnosti využití nejen u platidel.

7 Literatura

[1] ANTONOPOULOS, Andreas M.Mastering Bitcoin: Unlocking Digital Cryptocurrencies. 1. vyd. O'Reilly Media, 2014. 298 s. ISBN: 978-1449374044

[2] COX, James. Bitcoin and Digital Currencies. Laissez Faire Books, 2013. 112 s. ISBN: 978-1-62129-095-7

[3] JAKCMAN, J.T. Bitcoin for beginners Dita. CreateSpace Independent Publishing Platform, 2014. 110 s. ISBN: 978-1499260861

[4] PAGLIERY, Jose. Bitcoin and the future of money. Chicago: Triumph Books LLC, 2014. 256 s. ISBN: 978-1629370361

[5] ROCHON, Louis-Philipe. ROSSI, Sergio. Modern Theories of Money: The Nature and Role of Money in Capitalist Economies. Edward Elgar Publishing

[6] SINGH, Simon. Kniha kódů a šifer. přel. Koubský Petr, Eckhardtová Dita. 2. vyd. Praha: Dokořán, 2009. 384 s. ISBN 978-80-7363-268-7

8 Ostatní zdroje:

[7] ALITIN MINT. About Alitin Mint [online]. Alitinmint.com,[cit. 2015-1-15] Dostupný z: http://www.alitinmint.com/Home/About

[8] ANDRESEN, Gavin. Neutralizing a 51% attack [online]. GavinTech, 1.Květen 2012[cit. 2015-1-18]. Dostupný z: http://gavintech.blogspot.cz/2012/05/neutralizing-51-attack.html

[9] APODACA, Richard L. A Gentle Introduction to Bitcoin Cold Storage [online]. Bitzuma, 29. Březen 2014, poslední aktualizace 31. Říjen 2014, [cit. 2015-30-1]. Dostupný z: http://bitzuma.com/posts/a-gentle-introduction

[10] APODACA, Richard L. OP_RETURN and the Future of Bitcoin[online], Bitzuma, 29. Březen 2014 [cit. 2015-2-3] Dostupný z: http://bitzuma.com/posts/op-return-and-the-future-of-bitcoin/

[11] BIEGEL, Ofir. What is a 51% attack- simplified bitcion tutorial, 99bitcoins [online], 99 Bitcoins, 1. Duben 2014 [cit. 2015-1-18]. Dostupný z: http://99bitcoins.com/51-attack-simplified-bitcoin-tutorial/

[12] BITCIONTALK. Vanitygen: Vanity bitcoin address generator/miner [v0.22][online], Bitcointalk 4. Červenec 2011 [cit. 2015-2-3]. Dostupný z: https://bitcointalk.org/index.php?topic=25804.0

[13] BITCOIN.ORG. Some Bitcoin words you might hear[online]. Bitcoin.org, [cit. 2015-1-13]. Dostupný z: https://bitcoin.org/en/vocabulary

[14] Bitcoin.org. Some things you need to know [online]. Bitcoin.org, [cit. 2014-12-1]. Dostupný z: https://bitcoin.org/en/you-need-to-know

[15] BITCOINMINING, Bitcoin mining pools[online]. Bitcoin mining, [cit. 2015-3-14], Dostupný z: http://www.bitcoinmining.com/bitcoin-mining-pools/

[16] BITCOINRICHLIST. Bitcoin Distribution by Address at Block 290,000 [online]. Bitcoinrichtlist [cit. 2015-2-25]. Dostupný z: http://bitcoinrichlist.com/charts/bitcoin-distribution-by-address?atblock=280000

[17] BITCOINWISDOM. Bitcoin Difficulty [online], Bitcoinwisdom, [cit. 2015-3-1]. Dostupný z: https://bitcoinwisdom.com/bitcoin/difficulty

[18] Bitrated.com, FAQ [online]. Bitrated, [cit. 2014-12-1]. Dostupný z: https://www.bitrated.com/faq.html

[19] BITREF. [online]. [cit. 2015-3-30]. Dostupný z: http://bitref.com/1BYNK9AfpA2epfMBnBHTke8oc3CDLTuSEy

[20] BITSTAMP. FAQ[online].Bitstamp, [cit. 2015-4-14]. Dostupný z: https://cz.bitstamp.net/faq/

[21] BLAŽEK, Vojtěch. Jak se praly bitcoiny: Miliony z ciziny, vila napsaná na dědečka [online]. Ihned, 27. Březen 2015 [cit. 2015-4-1]. Dostupný z: http://archiv.ihned.cz/c1-63752430-jak-se-praly-bitcoiny-miliony-z-ciziny-vila-napsana-na-dedecka

[22] BLOCKEXPLORER. Blockexplorer, [cit. 2015-10-21]. Dostupný z: https://blockexplorer.com/q/hextarget

[23] BLOCKCHAIN. Blockchain size [online], Blockchain.info, [cit. 2015-1-17], dostupný z: https://blockchain.info/charts/blocks-size

[24] BLOCKCHAIN. Hash rate[online]. Blockchain, [cit. 2015-4-15]. Dostupný z: https://blockchain.info/pools

[25] BLOCKCHAIN. Hashrate Distribution: An estimation of hashrate distribution amongst the largest mining pools [online]Blockchain.info, [cit.2015-1-2]. Dostupný z: https://blockchain.info/pools

[26] BLOCKCHAIN. Market Price (USD)[online]. Blockchain, [cit. 2015-4-14]. Dostupný z: https://blockchain.info/charts/market-

price?showDataPoints=false&timespan=&show_header=true&daysAverageString=1&scale=0&format=csv&address=

[27] BLOCKCHAIN. Number of Transactions per day [online]. Blockchain, [cit. 2015-4-14]. Dostupný z: https://blockchain.info/charts/n-transactions?showDataPoints=false&timespan=all&show_header=true&daysAverageString=1&scale=0&format=csv&address=

[28] BLOCKCHAIN. Popular addresses [online]. Blockchain, [cit. 2015-3-24]. Dostupný z: https://blockchain.info/popular-addresses

[29] BOGOMOLNY, Alexander. Modular Arithmetic[online]. Cut The Knot, © 1996-2015 [cit. 2014-10-15]. Dostupný z: http://www.cut-the-knot.org/blue/Modulo.shtml

[30] BONADONNA, Erik. Bitcoin and the Double-Spending Problem [online]. Cornell University, 29. Březen 2013 [cit. 2015-3-1]. Dostupný z: http://blogs.cornell.edu/info4220/2013/03/29/bitcoin-and-the-double-spending-proble

[31] BOŘÁNEK, Roman. Bitcoin v nesnázích: hrozí mu 51% útok? [online], Root, 10. Leden 2014 [cit. 2015-1-18]. Dostupný z: http://www.root.cz/clanky/bitcoin-v-nesnazich-hrozi-mu-51-utok/

[32] BRADBURY, Danny, How anonymous is Bitcoin [online], Coindesk, 7. Červen 2013 [cit. 2014-12-1]. Dostupný z: http://www.coindesk.com/how-anonymous-is-bitcoin/

[33] BUTERIN, Vitalik. Block reward halving a guide[online]. Bitcoinmagazine, 27. Listopad 2012 [cit. 2015-10-21]. Dostupný z: http://bitcoinmagazine.com/2842/block-reward-halving-a-guide/

[34] BUTTERFLY LABS. The Monarch[online]. Butterfly Labs, [cit. 2015-4-14]. Dostupný z: http://www.butterflylabs.com/monarch/

[35] CAPKUN, Verdan, CAPKUN, Srdaj, GERVAIS, Arthut, KARAME, Ghasan, O.. Is Bitcoin a Decentralized Currency?[online], Cryptology ePring archive, [cit. 2015-1-26], dostupný zhttp://eprint.iacr.org/2013/829.pdf

[36] CAROL, Alexander. Volatility and correlation: measurement, models and applications [online]. ICMA center, [cit. 2015-2-18]. Dostupný z: http://www.icmacentre.ac.uk/pdf/financialriskchapter.pdf

[37] CEX.IO , CEX.IO Temporarily Suspends Cloud Mining Services[online], CEX.IO Blog, 12. Leden 2015 [cit. 2015-3-10] , Dostupný z: http://blog.cex.io/news/cex-io-temporarily-suspends-cloud-mining-services/

[38] COINBASE. [online]. [cit. 2015-1-18]. Dostupný z: https://www.coinbase.com/

[39] COINBASE. About[online], Coinbase, [cit. 2015-2-1]. Dostupný z: https://www.coinbase.com/about

[40] COINBASE. Bitcoin glossary[online]. Coinbase, [cit. 2015-4-14]. Dostupný z: https://support.coinbase.com/customer/portal/articles/1833695-bitcoin-glossary

[41] COINDESK, How to Store Your Bitcoins[online], Coindesk, poslední aktualizace 22. Prosinec 2014 [cit. 2015-1-13]. Dostupný z: http://www.coindesk.com/information/how-to-store-your-bitcoins/

[42] COINFLOOR, Our fees[online]. Coinfloor, [cit. 2015-3-10], Dostupný z: https://coinfloor.co.uk/fees

[43] COINMARKETCAP. Bitcoin markets[online], Coinmarketcap, [cit. 2015-4-14]. Dostupný z: http://coinmarketcap.com/ http://coinmarketcap.com/currencies/bitcoin/#markets

[44] COINMARKETCAP. Crypto-Currency Market Capitalizations [online], Coinmarketcap, [cit. 2015-2-3]. dostupný z: http://coinmarketcap.com/

[45] CRYPTOCOINSCHARTS, LTC/USD - Litecoin / US Dollar alltime charts and orderbook from BTC-e[online]. Cryptocoincharts, [cit. 2015-1-25], Dostupný z: http://www.cryptocoincharts.info/pair/ltc/usd/btc-e/alltime

[46] CUTHBERTSON, Anthony. $1000 Bitcoin Bubble Blamed on Fraudulent MtGox Bots[online], International Business Time, 29. Květen 2014 [cit. 2015-3-1]. Dostupný z: http://www.ibtimes.co.uk/1000-bitcoin-bubble-blamed-fraud

[47] ČESKÁ NÁRODNÍ BANKA, Obchodování s bitcoiny[online]. CNB[cit.2015-3-14] Dostupný z: http://www.cnb.cz/miranda2/export/sites/www.cnb.cz/cs/faq/obchodovani_s_bitcoiny.pdf

[48] DARKCOIN, What is Darkcoin?[online], Darkcoin, [vid. 2015-1-21]. Dostupný z: https://www.darkcoin.io/about/what-is-darkcoin/

[49] DEEPDOTWEB. Silkroad 3 [online]. Deepdotweb, [cit. 2015-3-28], dostupný z: http://www.deepdotweb.com/marketplace-directory/listing/silk-road-3

[50] DEEPDOTWEB. Updated list of hidden markets [online], Deepdotweb, 28. Říjen 2913, poslední aktualizace 8. Duben 2015 [cit. 2015-3-28]. Dostupný z: http://www.deepdotweb.com/2013/10/28/updated-llist-of-hidden-marketpl

[51] DOTBIT. Domain cost[online]. Dotbit, [cit. 2015-2-6]. Dostupný z: http://dot-bit.org/tools/domainCost.php?block=210000

[52] DOTBIT. dotbit.me bit domain proxy[online]. Dotbit, [cit. 2015-2-6] Dostupný z: http://dotbit.me/

[53] DOTBIT. [online]. Dotbit[cit. 2015-1-18]. Dostupný z: http://proxy.dotbit.me/browse.php?u=http://clipperz.bit

[54] DRISCOLL, Scott. How Bitcoin works under the hood [online]. Scott Driscoll's Blog, 14. Červenec 2013 [cit. 2015-4-1]. Dostupný z: http://www.imponderablethings.com/2013/07/how-bitcoin-works-under-hood.html

[55] EUR-LEX, Proposal for a Council Regulation laying down implementing measures for Directive 77/388/EEC on the common system of value added tax /* COM/2004/0641 final */ [online]. Europa, [cit. 2015-3-11]. Dostupný z:

[56] EUROPIAN CENTRAL BANK, Virtual currency schemes – a further analysis[online]. Europa, Březen 2015 [cit. 2015-3-11], Dostupný z: http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf

[57] EUROPIAN CENTRAL BANK, Virtual currency schemes [online]. Europa, Říjen 2012 [cit. 2015-3-11]. Dostupný z: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

[58] EUROPIAN COMMISION, Telecommunications, broadcasting & electronic services[online], Europa [cit. 2015-3-12]. Dostupný z: http://ec.europa.eu/taxation_customs/taxation/vat/how_vat_works/telecom/index_en.htm#new_rules

[59] EUROPIAN COMMISION. Explanatory notes on the EU VAT changes to the place of supply of telecommunications, roadcasting and electronic services that enter into force in 2015[online], Europa, [cit. 2015-3-12]. Dostupný

[60] FAGAN, F.J, Bitcoin and international crime[online]. Baltimoresun, 25. Listopad 2013 [cit. 2015-1-18]. Dostupný z: http://www.baltimoresun.com/news/opinion/oped/bs-ed-bitcoin-20131125-story.html

[61] FILLNER, Karel. Na VŠMIEP v Praze proběhla zajímavá konference o BTC[online]. Btctip, 30. Března 2014 [cit. 2015-3-14] Dostupný z: http://btctip.cz/na-vsmiep-v-praze-probehla-zajimava-konference-o-btc

[62] FLITTER, Emily. FBI shuts alleged online drug marketplace[online], Reuters, 2.Říjen 2013 [cit. 2015-3-28], dostupný z: http://www.reuters.com/article/2013/10/02/us-crime-silkroad-raid-idUSBRE9910TR20131002

[63] GILSON, David. What are Namecoins and .bit domains?[online], Coindesk, 18. Červen [cit. 2015-2-6] Dostupný z: http://www.coindesk.com/what-are-namecoins-and-bit-domains/

[64] GOOGLE TRENDS. [online]. [cit. 2015-2-10]. Dostupný z: http://www.google.cz/trends/explore#q=bitcoin

[65] GREENBERG, Andy. Darkcoin, the Shadowy Cousin of Bitcoin[online], Is Booming, Wired, [20. Květen 2014], [cit. 2015-1-21] Dostupný z: http://www.wired.com/2014/05/darkcoin-is-booming/

[66] HAJDARBEGOVIC, Nermin. MultiBit Bitcoin Wallet Leapfrogs Coinbase to Reach 1.5 Million Downloads [online]. CoinDesk, 11. Květen 2014 [cit. 2015-2-1]. Dostupný z: http://www.coindesk.com/multibit-bitcoin-wallet-leap

[67] HÁLA, Vojtěch. Kvantová kryptografie [online). Aldebaran Bullentin. Praha: Aldebaran Group for Astrophysics, 2005 [cit. 2014-11-10]. ISSN: 1214-1674. Dostupný z: http://aldebaran.cz/bulletin/2005_14_kry.php

[68] HARDY, ZAMAN, Peter, Mehreen. The Mechanics of Virtual Currency: A Reportable Foreign Account? [online]. Bloomberg BNA, © 2014 [cit. 2015-1-29] , Dostupný z: http://www.postschell.com/site/files/bnainsights_hardyzam

[69] HASHCASH. Hashcash, [cit. 2014-10-22]. Dostupný z: http://www.hashcash.org/

[70] HIGGINS, Stan. How True Anonymity Made Darkcoin King of the Altcoins[online], Coindesk, 23. Květen 2015 [cit. 2015-1-21] Dostupný z: http://www.coindesk.com/true-anonymity-darkcoin-king-altcoins/

[71] HIGGINS, Stan. Study: Bitcoin Wallet Attacks Rose Sharply in 2013 [online].Coindesk, 10. Duben 2014 [cit. 2014-12-10]. Dostupný z: http://www.coindesk.com/study-nearly-6-million-bitcoin-wallets-attacked-2013/

[72] HISTORY OF BITCOIN, History of Bitcoin The world's first decentralized currency [online]. History of Bitcoin, [cit. 2014-11-13]. Dostupný z: http://historyofbitcoin.org/

[73] HOUSTECKY, Petr. Historical volatility calculation[online]. Mactoption, [cit. 2015-2-17]. Dostupný z: http://www.macroption.com/historical-volatility-calculation/

[74] HOUSTECKY, Petr. Volatility[online]. Macroption, © 2015 [cit. 2015-2-17]. Dostupný z: http://www.macroption.com/volatility/

[75] HRACH, Jan. Decentralizovaná kryptoměna Bitcoin [online]. Abc Linuxu, 27.Července 2011 [cit. 2014-10-21]. Dostupný z: http://www.abclinuxu.cz/clanky/decentralizovana-kryptomena-bitcoin#!/-1/

[76] JAMES, Mike. Inside Bitcoin - virtual currency. I programmer, [cit. 2014-10-21]. Dostupný z: http://www.i-programmer.info/babbages-bag/2486-inside-bitcoin-virtual-currency.html?start=1

[77] JANSEN, Cory. Hash Function[online]. Techopedia.[cit. 2014-11-1]. Dostupný z: http://www.techopedia.com/definition/19744/hash-function

[78] JARVIS, Keith. CryptoLocker Ransomware[online]. Dell SecureWorks, 18. Prosinec 2013 [cit. 2015-3-31]. Dostupný z: http://www.secureworks.com/cyber-threat-intelligence/threats/cryptolocker-ransomware/

[79] KLÍMA, Vlastimil. Hašovací funkce, principy, příklady a kolize[online]. Crypto-world, 19. Března 2005 [cit. 2014-11-10]. Dostupný z: http://crypto-world.info/klima/2005/cryptofest_2005.htm

[80] LEACH Robert, Robertleach, Quick guide to legal tender[online]. Robertleach.co.uk, © 2011 [cit. 2015-3-11] Dostupný z: http://robertleach.co.uk/wp-content/uploads/2011/05/Quick-guide-to-legal-tender3.pdf

[81] LIGHT, John. Securing your Bitcoins [online]. Let's talk Bitcoin, 6. Březen 2014 [cit. 2014-12-20]. Dostupný z: http://letstalkbitcoin.com/securing-your-bitcoins/

[82] LIU, Alec. A Guide to Bitcoin Mining: Why Someone Bought a $1,500 Bitcoin Miner on eBay f or $20,600. Motherboard, 22. Březen 2013 [cit. 2015-2-6]. Dostupný z: http://motherboard.vice.com/blog/a-guide-to-bitcoin-mini

[83] LITECOIN. [online]. [cit. 2014-11-27]. Dostupný z: http://motherboard.vice.com/blog/a-guide-to-bitcoin-mini

[84] MAXWELL, Gregory. CoinJoin: Bitcoin privacy for the real world[online]. Bitcointalk, 22. Srpen 2013 [cit. 2014-12-10]. Dostupný z: https://bitcointalk.org/index.php?topic=279249.0

[85] McAFEE, McAfee Labs Threats Report [online]. McAFEE, Leden 2014 [cit. 2015-1-25]. Dostupný z: http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2014.pdf

[86] MCCORMICK, Jamie. Bitcoin Armory Wallet Review[online], Bitcoinsinireland, 1. Prosinec 015-2-1]. Dostupný z: http://bitcoinsinireland.com/bitcoin-armory-wallet-review/

[87] MCINTYRE, Donald. The Ripple Network Review – What Is Ripple? [online]. Naation, 1. Srpen 2014 [cit. 2015-1-27]. Dostupný z: http://www.naation.com/2013/08/01/the-ripple-network-review-what-is-ripple/4103/

[88] MIČKA, Pavel. Algoritmus RSA[online]. Algoritmy, © 2008-2015 [cit. 2014-10-15]. Dostupný z: http://www.algoritmy.net/article/4033/RSA

[89] MORENO, Miguel. Bitcoin address collision [online], Miguelmoreno.net, [cit. 2015-3-1]. Dostupný z: http://www.miguelmoreno.net/bitcoin-address-collision/

[90] NAMECOIN. What's DNS? And why does Dot-Bit matter? [online]. Namecoin.info, [cit. 2015-2-6] Dostupný z: http://bit.namecoin.info/

[91] OANDA. Historical Exchange Rates [online]. Oanda, [cit. 2015-2-10]. Dostupný z: http://www.oanda.com/currency/historical-rates/

[92] OŠŤÁDAL, Radim. Teoretický základ a přehled kryptografických hashovacích funkcí[online]. Březen 2012 [cit. 2014-11-12]. Dostupný z: http://is.muni.cz/www/255508/hash_overview.pdf

[93] PAGLIERY, Jose. 8 things you can buy with bitcoins right now [online]. CNN Money, poslední aktualizace 26. Listopad 2013 [cit. 2015-1-29]. Dostupný z: http://money.cnn.com/gallery/technology/2013/11/25/buy-with-bitc

[94] PALMER, Daniel. Review: Brawker Let's You Buy 'Almost Anything' with Bitcoin[online]. Coindesk, 24. Prosinec 2014 [cit. 2015-2-4]. Dostupný z: http://www.coindesk.com/review-brawker-lets-buy-almost-anything-bitcoin/

[95] PERIGAUD, Fabien, PERNET, Cedric. Bitcrypt broken [online]. Cassidian Cyber Security, 20. Únor 2014 [cit. 2015-3-24]. Dostupný z: http://blog.cassidiancybersecurity.com/post/2014/02/Bitcrypt-broken

[96] PERRY, Daivd. Paper Wallets aren't Cold Storage[online]. Coding In My Sleep, 7. Listopad 2014 [cit. 2015-30-1]. Dostupný z: http://codinginmysleep.com/paper-wallets-arent-cold-storage/

[97] PROOFOFEXISTENCE. What is proof of existence? [online], Proofofexistence, [cit. 2015-2-3]. Dostupný z: http://www.proofofexistence.com/about

[98] QUANDL. Bitcoin Exchange Rates[online]. Quandl, [cit. 2015-4-14]. Dostupný z: https://www.quandl.com/c/markets/bitcoin-data

[99] RIPLE. How Ripple works, Ripple[online]. 16.Říjen 2014 [cit. 2015-1-27]. Dostupný z: https://ripple.com/knowledge_center/how-ripple-works/

[100] RIPPLE, Executive Summary for Financial Institutions [online]. Ripple, Leden 2015 [cit. 2015], Dostupný z: https://ripple.com/integrate/executive-summary-for-financial-institutions/

[101] RIPPLECHARTS, [cit. 2015-1-27] Dostupný z: http://www.ripplecharts.com/#/graph/

[102] RUBEN, Alexander. Review of TitanBTC's Cold Storage [online], Bitcoinmagazine, 20. Srpen 2014 [cit.2015], Dostupný z: https://bitcoinmagazine.com/15787/reviewtitanbtc/

[103] SATOSHI, Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System [online]. Bitcoin.org, [cit. 2014-11-13]. Dostupný z: https://bitcoin.org/bitcoin.pdf

[104] SAXOBANK. Slovnik pojmů – likvidita[online]. [cit. 2015-4-14]. Dostupný z: http://cz.saxobank.com/support/slovnik-pojmu/likvidita

[105] SIEDEL, Robin. Even Bitcoin's Fans Prefer to Keep Cash[online], The Wall Street Journal, 25. Prosinec 2014 [cit. 2015-3-1]. Dostupný z: http://www.wsj.com/articles/even-bitcoins-fans-prefer-to-keep-cash-1419539916

[106] SULLIVAN, Nick. ECDSA: The digital signature algorithm of a better internet[online]. Cloudflare blog, 10. Květen 2014 [cit. 2014-11-1]. Dostupný z: http://blog.cloudflare.com/ecdsa-the-digital-signature-algorithm-of-a-better-internet/

[107] TITAN BITCION. How to Redeem Private Key Titan Bitcoins[online], Titanbtc, [cit. 2015-] Dostupný z: https://www.titanbtc.com/how-to-redeem-private-key-titan-

[108] TITAN BITCION. Redeem your Coin, Titanbtc.com, [cit. 2015-1-15] Dostupný z: bitcoins/https://www.titanbtc.com/redeem/

[109] TYLEČEK, Jiří. Futures kontrakty: základní principy a informace[online], Hospodářské Noviny, 23. Říjen 2009 [cit. 2015-3-13]. Dostupný z: http://byznys.ihned.cz/c1-38767880-futures-kontrakty-zakladni-principy-a-info

[110] WILMOTH, Josiah. What is an altcoin? [online], Cryptocoinsnews, 9. Prosinec 2014 [cit. 2015-2-6]. Dostupný z: https://www.cryptocoinsnews.com/altcoin/

[111] WINTERS, Tristan. The Psychology of Decimals [online]. Bitcoin Magazine, 20. Listopad 2013 [cit. 2014-11-17]. Dostupný z: http://bitcoinmagazine.com/8274/the-psychology-of-decimals/

[112] WIRDUM , Aaron Van. New EU Legislation on VAT Could Be Bad News for Bitcoin[online]. Coindesk, 4. Únor 2015 [cit. 2015-3-14], Dostupný z: http://www.coindesk.com/new-eu-legislation-vat-bad-news-bitcoin/

[113] XORBIN. SHA-256 hash calculator, [cit. 2014-1-11]. Dostupný z: http://www.xorbin.com/tools/sha256-hash-calculator