

VYSOKÁ ŠKOLA EKONOMICKÁ V PRAZE
FAKULTA MEZINÁRODNÍCH VZTAHŮ



Studijní obor: Manažer obchodu

**Využitelnost bitcoin/kryptoměn v
e-commerce a retailu
(Bakalářská práce)**

Autor: Semi Ennafaa

Vedoucí práce: Ing. Alena Filipová, Ph.D.

Čestné prohlášení

Prohlašuji, že jsem tuto bakalářskou práci s názvem „Využitelnost bitcoin/kryptoměn v e-commerce a retailu“ vypracoval samostatně pod vedením a uvedl jsem použitou literaturu a jiné zdroje a vyznačil všechny citace z pramenů.

V Praze dne 7. 12. 2018

...

Poděkování

Děkuji vedoucí mé bakalářské práce paní prof. Ing. Alena Filipová, Ph.D. za její podnětné připomínky, odborné vedení a čas, který mi při tvorbě této bakalářské práce věnovala.

Zejména jí pak děkuji za její velmi vstřícný přístup a trpělivost.

Obsah

Úvod	1
1. Vymezení kryptoměn	2
1.1. Obecná definice kryptoměn	2
1.2. Základní prvky principu fungování bitcoinu	3
1.3. Generování a emise bitcoinu	8
1.4. Vznik bitcoinu	11
1.5. Burzy a platební brány	17
1.6. Alternativní kryptoměny	21
1.7. Zákonná definice, účtování a vykazování kryptoměn	24
1.8. Zhodnocení dopadů a působení kryptoměn na světovou ekonomiku a odvětví retailu	26
2. Posouzení využitelnosti kryptoměn	27
2.1. Analýza dodavatelů	29
2.2. Analýza konkurence	31
2.3. Rizika	35
2.4. SWOT	38
2.5. Průzkum	Chyba! Záznam není definován.
Závěr:	41
Infografika	Chyba! Záznam není definován.
Seznam zdrojů	42

Úvod

Tématem této bakalářské práce je zhodnocení využitelnosti bitcoinu potažmo kryptoměn v oblasti e-commerce a retailu. Kryptoměny fungující na principu blockchainu, tedy sdílené elektronické účetní knihy, jsou fenoménem posledních let. Zvláště pak v roce 2017 zaznamenal tento jev ohromný nárůst popularity i obecného povědomí rovněž u laické veřejnosti. Za referenční kryptoměnu lze považovat bitcoin, tedy první kryptoměnu, která má nejdelší historii i poměrně jasný vývoj v čase. Z tohoto důvodu v rámci této práce budu pracovat především právě s daty spojenými s touto konkrétní kryptoměnou, kterou považuji za referenční. Cílem je tedy především zhodnocení možností i rizik, které pro případné zájemce představuje nasazení bitcoinu coby alternativní formy elektronického platebního styku v prostředí e-commerce a retailu. Kryptoměnám, potažmo bitcoinu, se již věnuji více jak sedm let, kdy jsem měl možnost sledovat jeho vývoj nejen z pohledu ekonomického, ale i technického. Ostatně právě prvotní nadšení pro kryptoměny bylo jedním z důvodů, proč jsem se rozhodl pro studium na Vysoké škole ekonomické. Mezi základní otázky, na které bych rád touto prací odpověděl jsou spojené se zhodnocením možností využití bitcoinu v e-commerce a retailu. Na úvod bych se rád zaměřil na základní informace o kryptoměnách a bitcoinu. To znamená na základní strukturu a principy na kterých je decentralizovaná síť bitcoin postavena. Zaměřím se rovněž na to, jakým způsobem bitcoiny vznikají, jaké procesy vedou k jejich vzniku a jakým způsobem jsou transakce uvnitř sítě realizovány. Nedílnou součástí pro pochopení fenoménu, kterým bitcoinu jsou je jejich historie, která je spojena s mnoha milníky, které ovlivnily budoucí vývoj kryptoměn obecně a jejich popularizaci. Z pohledu obchodníka je jistě zajímavé i nahlédnout na způsoby, jakým lze s kryptoměnami obchodovat a jaké služby případně využít pro využití v e-commerce a retailu. Nutno podotknout, že i přesto, že bitcoin je hlavním důvodem popularizace kryptoměn. Veřejnost jej prakticky vnímá jako synonymum pro kryptoměny, tak v dnešní době existují tisíce alternativ využívajících stejný nebo velmi podobně fungující princip blockchain. Okrajově se zaměříme na několik konkurenčních kryptoměn, které představují vývojové pokračovatele bitcoiny, byť například jejich mechanismy ověřování či cíle jsou odlišné. V druhé části se zaměřuji na to, jakým způsobem lze integrovat platbu bitcoinem v oblasti e-commerce a retailu. Zhodnotím rizika i potencionální přínosy z pohledu obchodníka a zároveň nabízím srovnání ostatními konvenčními způsoby plateb. Základní transakce v síti bitcoin využívá konceptu blockchain, který je popsán v kapitole „Základní prvky principů fungování bitcoinu“. Z pohledu uživatele vše začíná stažením a nainstalováním patřičného software. V

tomto případě je to elektronická peněženka – wallet. Tyto peněženky je možné využít prakticky ve všech současných počítačových operačních systémech, včetně mobilních zařízení. Následuje vytvoření unikátní adresy v rámci sítě bitcoin, která slouží k jasné identifikaci při zadání i přijetí platby. V tomto směru je bitcoinpseudo-anonymní, což znamená, že jednotlivé účastníky platby lze identifikovat pouze v rámci sítě (na základě unikátní adresy) ovšem nelze je přiřadit ke konkrétním uživatelům s reálnou identitou. Aby mohla být platba zanesena do účetní knihy, též označované jako blockchain, je nutné transakci ověřit. Až poté, co dojde k ověření je transakce v rámci bloku transakcí připojena na konec blockchainu (řetězce již ověřených bloků). Takto ověřená a uložená transakce zůstává v rámci celého blockchainu zapsána trvale a informace o ní je veřejně dostupná. V případě, že uživatel chce provést konverzi na standardní státní fiat měny, je nutné provést již standardní směnu mezi jednotlivými uživateli nebo využít služeb specializovaných směnárů či platebních bran.

1. Vymezení kryptoměn

1.1. Obecná definice kryptoměn

„Digitální měna, ve které jsou použity kryptografické techniky k regulaci generování jednotek měny a jejich ověřování při převodu. To vše zcela nezávisle na centrální bance.“¹

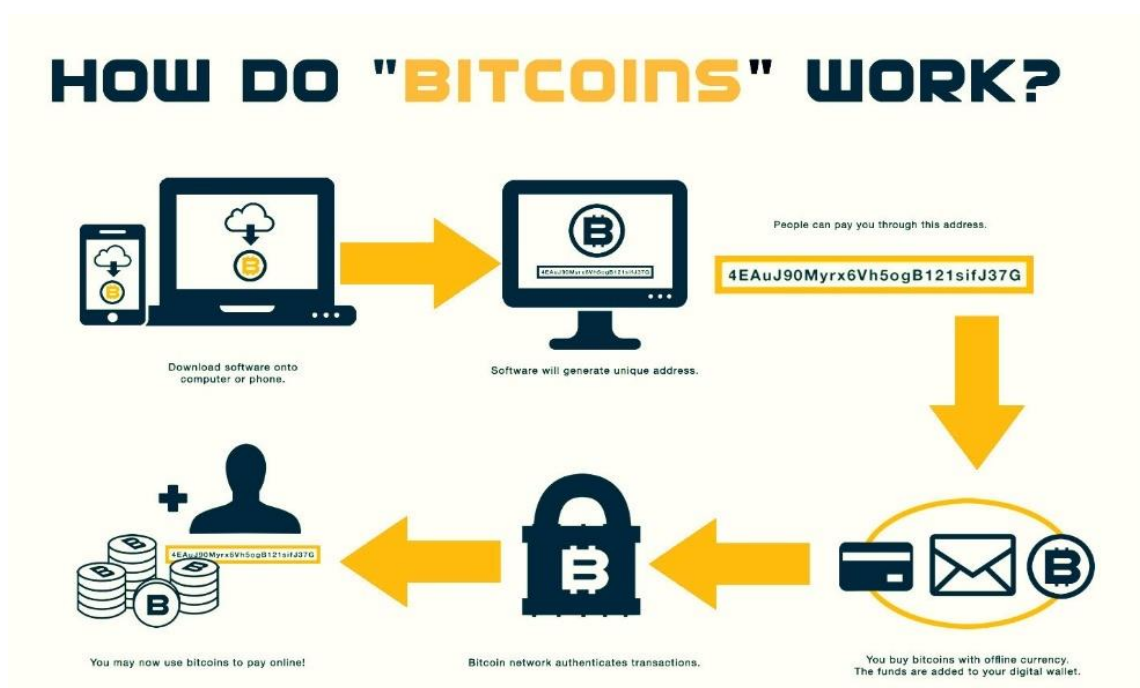
„Kryptoměna je digitální aktivum, které je designováno pro funkci výměnného média využívajícího pokročilé formy kryptografie pro zabezpečení finančních transakcí, správě vytváření dalších jednotek a vytváření přenosů aktiv. Kryptoměny jsou určitou alternativou k běžným měnám a ostatním digitálním měnám. Kryptoměny používají decentralizovanou kontrolu, což je protikladem k standardním bankovním systémům. Decentralizovaná kontrola jednotlivých kryptoměn využívá distribuovanou účetní knihu, obvykle blockchain, sloužící jako veřejná databáze finančních transakcí.“²

Obě výše zmíněné definice vystihují podstatu kryptoměn, ale ani v jednom případě je nelze označit za přesnou definici. To je do určité míry způsobeno samou podstatou kryptoměn, a to absolutní decentralizací všech prostředků, spolu s absencí jedinečné autority vydávající přesné

¹CryptocurrencyDefinition | Oxforddictionaries [online]. [vid. 1. listopad 2018]. Dostupné z: <https://en.oxforddictionaries.com/definition/cryptocurrency>

²What is cryptocurrency [online]. [vid. 14. srpen 2018]. Dostupné z: <https://www.thestreet.com/investing/bitcoin/what-is-cryptocurrency-14679467>

definice či jiné pokyny. Obsah je tak generován zcela automaticky. Základem kryptoměn, ostatně jak již plyne z názvu, je kryptografie, která umožňuje zabezpečit provoz celé decentralizované sítě, a to s pomocí výpočetního výkonu jednotlivých klientských stanic. Ty byly v poslední době do značné míry nahrazeny specializovanými hardwarovými prostředky. Spolu s kryptoměnami je spojována i anonymita uživatelů v rámci celého procesu přenosu. Nutno podotknout, že nejde o anonymitu absolutní, ale spíš lze hovořit o pseudoanonymitě, kdy není znám konkrétní majitel virtuální peněženky, ale pouze konkrétní adresa peněženky zanesená do veřejně dostupné účetní knihy – blockchainu³. Přestává však být anonymní ve chvíli, kdy se pokusí s někým kryptoměnu směnit v rámci obchodování s kryptoměnami. Stejným způsobem lze do určité míry dohledat identitu i ve chvíli, kdy se rozhodne BTC či jinou kryptoměnu směnit za libovolnou fiat měnu.⁴



Obrázek 1 Základní popis transakce⁵

1.2. Základní prvky principu fungování bitcoinu

Mezi základní prvky, které vytvářejí decentralizovanou síť bitcoinu (rovněž označovaného zkratkou BTC), se kterými se při případném zavedení kryptoměn musíte seznámit, patří níže uvedené termíny. Vzhledem k tomu, že cílem práce je zhodnotit možnosti kryptoměn a jejich

³ Arvind, Narayanan. Blockchains: Past, Present, and Future. Houston (USA), 2018: SIGCSE '18, 2018. ISBN: 978-1-4503-4706-8.

⁴ Stefan, Dziembowski. Introduction to Cryptocurrencies. Houston (USA), 2015: CCS '15 Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, 2015. 978-1-4503-3832-5.

⁵ How bitcoin works [online]. [vid. 11. únor 2018]. Dostupné z: <https://steemit.com/cryptocurrency/@jonvickers/how-bitcoin-works>

využití v e-commerce a retailu, jsem se rozhodl popis funkcí zjednodušit pro snazší pochopení. V případě implementace do vlastních softwarových řešení je nutné pochopit hlubší technické náležitosti celého řešení, což ovšem předmětem této práce není.

Blok

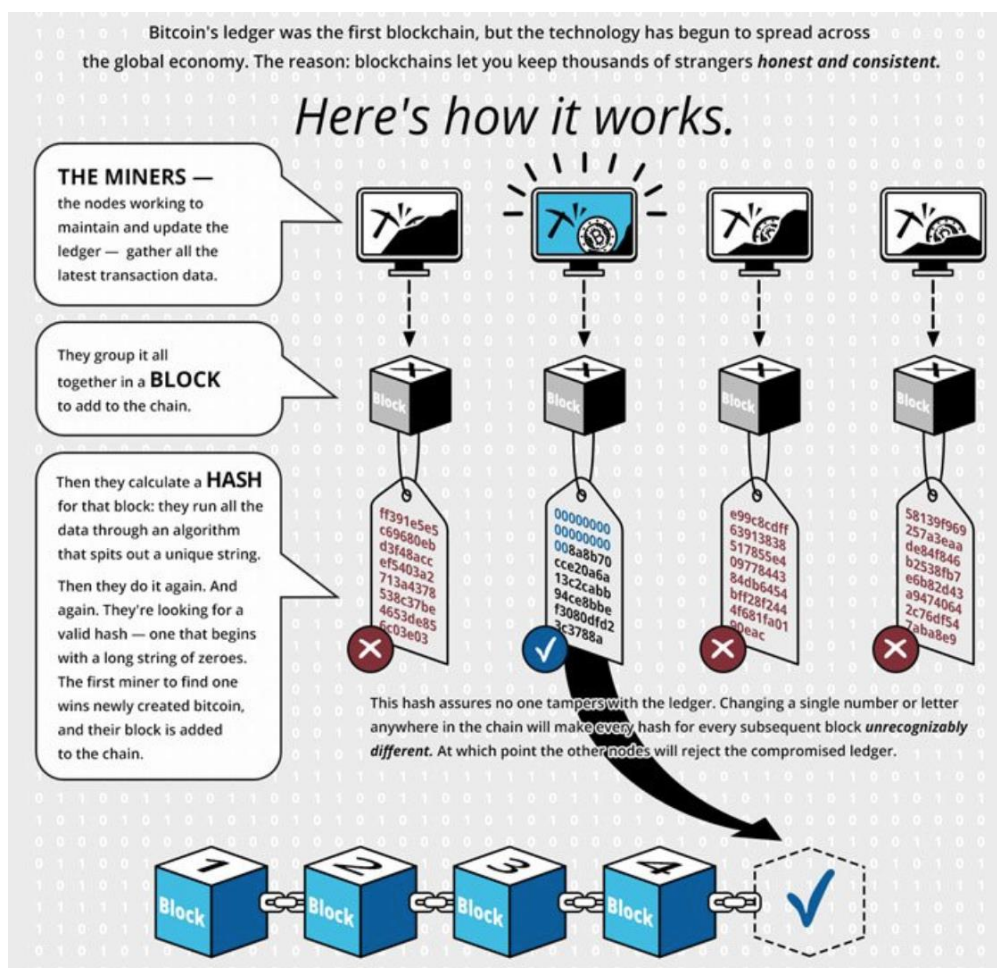
Základním stavebním prvkem celé decentralizované sítě je blok. To je soubor informací o aktuálně provedených transakcích v rámci sítě konkrétní kryptoměny. Tyto informace v bloku je nutné ověřit, k čemuž slouží složitý matematický výpočet využívající prvky kryptografie. K tomuto účelu, tedy vyřešení složitého kryptografického úkolu, slouží tisíce počítačů a specializovaných zařízení zapojených do decentralizované sítě. Ty využívají svůj výkon k vytěžení správné odpovědi na zadaný úkol. Za tento úkol jsou majitelé „těžících“ zařízení odměňováni v případě nalezení správné odpovědi, a to generováním nových mincí. Nové bloky následně musí získat unikátní identifikační znak tzv. hash a až poté je možné je zařadit do celkového řetězce tzv. blockchainu⁶.

Blockchain Po dokončení ověření bloku se blok zařazuje do řetězce již ověřených bloků, tzv. blockchainu. Informace v blockchainu představují sdílenou účetní knihu, která umožňuje chronologicky řazená data transakcí v jednotlivých blocích případně dohledat a ověřit. Blockchain v sobě obsahuje záznamy o všech provedených transakcích od samého prvopočátku, tedy vzniku prvního bloku. Ten bývá označován jako Genesis blok⁷ a v případě bitcoinu byl vytvořen 3.1. 2009. Blockchain je díky decentralizaci celé sítě šířen jednotlivými uzly, které představují jednotlivé počítače zpracovávající úlohy pro ověření transakcí. Díky tomu je prakticky nemožné změnit již uložené informace, protože za správnou verzi účetní knihy, tedy blockchain je považována ta verze, která je ověřena většinou. Většina není určena počtem uživatelů, ale většinovým výkonem, který provádějí ověřovací výpočty. V současné době celý blockchain kryptoměny bitcoinu je uložen v jednotné databázi o velikosti okolo 168 GB⁸.

⁶Debasis, Bhattacharya. Bitcoins, Blockchains and Cybersecurity. Baltimore, Maryland, (USA), 2018: SIGCSE '18, 2018. ISBN: 978-1-4503-5103-4.

⁷Genesis Block[online]. [vid. 16. duben 2015]. Dostupné z: <https://www.investopedia.com/terms/g/genesis-block.asp>

⁸Blockchain size [online]. [vid. 18. červen 2018]. Dostupné z: <https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/>



Obrázek 2 Názorný příklad fungování blockchain⁹Základem jsou těžaři spravující celou databázi, kteří seřazují transakce do bloků, ověřují je a následně řadí do řetězce

Peněženka

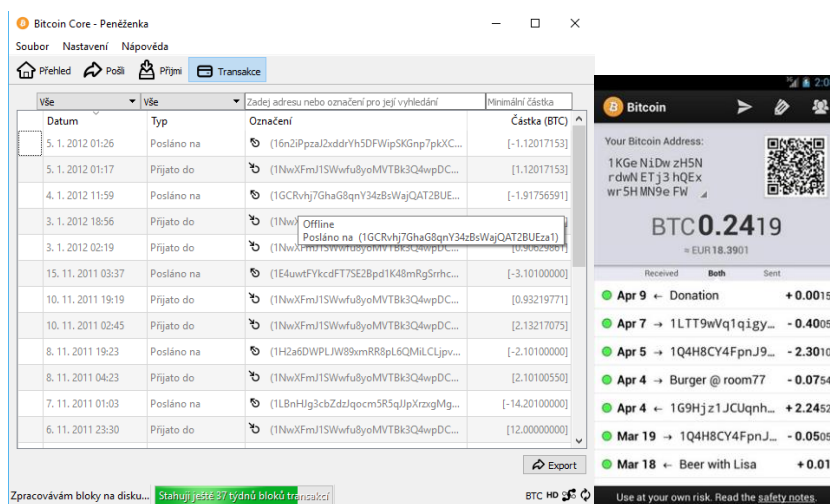
Z pohledu běžného uživatele je vstupní branou do využívání kryptoměn včetně bitcoinu. Program je označován příznačně jako peněženka neboli anglickým výrazem wallet¹⁰. S pomocí tohoto programu získáte přístup do decentralizované sítě, a to včetně své unikátní adresy. Z pohledu běžného uživatele a potencionálního zákazníka využívajícího bitcoin pro platby v retailu a e-commerce představuje rychlý vývoj těchto aplikací zjednodušení využití peněženek, resp. plateb bitcoinem, což znamená velký krok kupředu pro masivní rozšíření.

⁹ Blockchain[online]. [vid. 18. červen 2018]. Dostupné z:

https://i.investopedia.com/image/png/1542048203442/screen_shot_20181112_at_1.43.06_pm.png

¹⁰ Choose your Bitcoin wallet [online]. [vid. 7. prosince 2018]. Dostupné z: <https://bitcoin.org/en/choose-your-wallet>

Peněženka ovšem nemusí mít pouze formu aplikace například v mobilním telefonu, ale může být rovněž dostupná přes webové rozhraní nebo s využitím specializovaného hardware. V případě požadavku na maximální bezpečnost je možné využít tzv. cold wallet¹¹, tedy peněženky, které bez přístupu k síti pracují offline. Tyto peněženky mohou být uloženy na bezpečném místě, ať už na digitálním nosiči či fyzicky, například vytištěné na papíře.



Obrázek 3 bitcoinwallet pro operační systém MS Windows.¹²

Obrázek 4 Peněženka pro mobilní zařízení.¹³

Adresa

Adresa je jednoduše generovaný identifikátor, složený z 26 – 35 alfanumerických znaků s řadou začínající číslem 1 nebo 3. Lze jej pro jednodušší pochopení přirovnat k číslu účtu v bance. Adresy jsou generovány zdarma a může je tak vytvořit jakýkoliv uživatel, ať už online nebo offline. Samotná adresa se stane aktivní až po jejím prvním použití, kdy je následně zařazena do blockchain. Adres je možné generovat neomezené množství, kdy měly fungovat jako jednorázové tokeny. Identifikátor adresy je natolik nezaměnitelný, že při jejím zadávání je téměř nemožné provést záměnu za jinou adresu a provést tak platbu na špatný „účet“. Pravděpodobnost záměny je tak zhruba 1 : 4.29 miliardám. Spolu s adresou se rovněž generuje i osobní klíč.¹⁴

¹¹ Alexandra, Dmitrenko. Secure Wallet-Assisted Offline Bitcoin Payments with Double-Spender Revocation. bu Dhabi, (Spojené Arabské Emiráty), 2017: ASIA CCS '17 Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security, 2017, ISBN: 978-1-4503-4944-4

¹² bitcoin Core[vlastní zdroj]. [vid. 16. březen 2018].

¹³ bitcoinWallet[online]. [vid. 16. březen 2018]. Dostupné z: <https://bitcoinwallet.com/>

¹⁴ bitcoinAdress[online]. [vid. 29. leden 2018]. Dostupné z: <https://www.coindesk.com/information/how-do-bitcoin-transactions-work>

Osobní klíč

Osobní klíč (privatekey) je heslem, které je nutné pro zaslání BTC na cílovou adresu. Opět i v tomto případě je možné osobní klíč přirovnat k běžně používanému pinu pro přihlášení do internetového bankovníctví. Tento osobní klíč představuje 256bitové číslo, které je uloženo v peněžence. V peněžence je možné mít uloženo více privátních klíčů současně. Existuje několik různých formátů privátních klíčů, ale z pohledu běžného uživatele rozdíl mezi nimi nehraje zásadní roli. Je rovněž nutné si uvědomit, že pokud kdokoliv neoprávněně získá přístup k privátním klíčům, získá přístup i k provádění libovolných transakcí. Také v tomto případě je důležité uvědomit si fakt, že veškeré transakce jsou nevratné, v případě neoprávněného platebního příkazu neexistuje autorita, která by mohla průběh transakce zvrátit. Privátní klíče mohou být zálohovány nejen v digitální podobě, ale i ve fyzické podobě například vytisknutím na běžné tiskárně.¹⁵

Hašovací funkce - hash

„Hašovací funkce je matematická funkce (resp. algoritmus) pro převod vstupních dat do (relativně) malého čísla. Výstup hašovací funkce se označuje výtah, miniatura, otisk, fingerprint či hash (česky uváděno též někdy jako haš). Hašovací funkce se používají k rychlejšímu prohledávání tabulky, porovnávání dat (například pro hledání položek v databázi, odhalování duplicitních záznamů, hledání malware antivirovým programem), při hledání podobných úseků DNA sekvencí v bioinformatice i jinde. V podobě kryptografické hašovací funkce je používána pro vytváření a ověřování elektronického podpisu, zajištění integrity dat atd.“¹⁶

V případě bitcoinu jde o hash kryptografický, kdy je tato funkce používána pro zajištění integrity dat v databázi potažmo blockchainu. Konkrétně se jedná o 256bitové SHA-256 šifrování.¹⁷ Metody šifrování nejsou u všech kryptoměn stejné, proto se může lišit, jak způsob průběhu těžení, tak i možnosti jaké hardwarové prvky pro ně využít.

¹⁵ Bitcoin Private Keys: Everything You Need To Know [online]. [vid. 15. září 2018]. Dostupné z: <https://coinsutra.com/bitcoin-private-key/>

¹⁶ Hašovací funkce [online]. [vid. 29. listopad 2017]. Dostupné z: http://crypto-world.info/klima/2005/cryptofest_2005.htm

¹⁷ Jak těžké je uhodnout hodnotu hashe SHA-256? [online]. [vid. 28. července 2017]. Dostupné z: <https://www.root.cz/zpravicky/jak-tezke-je-uhodnout-hodnotu-hashe-sha-256/>



Obrázek 5- Příklad zpracování vstupu s pomocí SHA256 šifrování

1.3. Generování a emitace bitcoinu¹⁹

bitcoin je často, i když ne zcela oprávněně, přirovnáván ke zlatu. Přestože toto přirovnání není zcela přesné, způsob získávání zlata i bitcoinu je obrazně řečeno podobný, přestože se odehrává ve zcela jiné dimenzi. V obou případech je proces získávání zlata, resp. bitcoinů označován jako těžení (mining). Při těžení je hlavní cílem dosáhnout ověření transakce prací (proof of work), tedy výpočetním výkonem nutným pro správný výpočet. Druhotný následek provádění této práce je emitace nových bitcoinů do oběhu. Těmi jsou odměňováni právě uživatelé, kteří se podílejí na těžení. Těžení ovšem není jedinou možností, jak mohou nové mince v rámci sítě vzniknout. Další možností vygenerování mincí takzvaným „předtěžením“, kdy jsou mince na počátku vygenerovány. Tento způsob ovšem u bitcoinu nebyl použit, ale je využit se například u kryptoměny Ripple.

Dostupnost bitcoinů

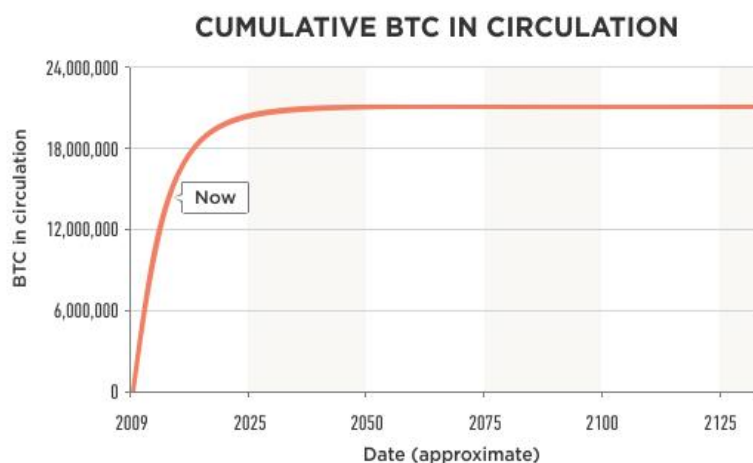
Podobně, jako drahé kovy, i bitcoin není, co se týká kvantity, neomezený. Celkový počet BTC je fixně limitován částkou 21 000 000 BTC. Z této částky již bylo vytěženo zhruba 17 000 000 BTC, takže zbývá vytěžít 4 000 000 BTC. Z uvedené vytěžené částky, která je již v oběhu, lze odečíst zhruba 30 % BTC²⁰, které byly v průběhu existence sítě ztraceny. Mezi hlavní důvody ztráty patří již zmíněný fakt, že všechny transakce jsou definitivní, proto jakákoliv chyba může znamenat ztrátu BTC. V případě ztráty přístupu do peněženky je také nutné počítat s tím, že není prakticky možné znovu tento přístup obnovit, a veškeré bitcoiny umístěné v peněžence

¹⁸bitcoinMining: A CloserLookUnderthe Hood[online]. [vid. 12. duben 2017]. Dostupné z: <https://news.bitcoin.com/bitcoin-mining-closer-look-hood/>

¹⁹ Bitcoin Emission: How Many Coins We Have, How Many Are to Come And Why Is It So [online]. [vid. 31. květen 2018]. Dostupné z: <https://thecoinshark.net/bitcoin-emission-how-many-coins-we-have-how-many-are-to-come-and-why-is-it-so/>

²⁰ Nearly 4 Million Bitcoins Lost Forever [online]. [vid. 25. listopad 2017]. Dostupné z: <http://fortune.com/2017/11/25/lost-bitcoins/>

jsou tak navždy ztraceny. S přihlédnutím k faktu, že už je v současné době vytěženo více jako 80 % z celkového množství bitcoinů, lze s jistotou v budoucím průběhu vývoje očekávat deflaci. V důsledku těžby se sice měnový základ zvyšuje, ale tento stav je pouze dočasný. Pevný měnový základ je jev, který je obecně v oblasti ekonomie vnímán spíše negativně. Deflační spirála může vést ke spekulativnímu chování, kdy si subjekty budou hromadit kryptoměnu s vidinou vyšší budoucí hodnoty. Názory na to, jak se s podobnou situací vypořádá kryptoměna typu BTC se různí, ale většinový názor je takový, že bitcoin není běžnou měnou a v celkovém konceptu se s touto situací počítá. Rovněž je důležité upozornit na to, že jeden BTC je možné dělit až 10^8 a v současné době vzhledem k hodnotě bitcoinu se obvykle používá jednotky mBTC, tedy jedna tisícina BTC.



Graf 1 Znáznorňuje uvolňování bitcoinů do oběhu v čase²¹

Základní podmínky pro těžení

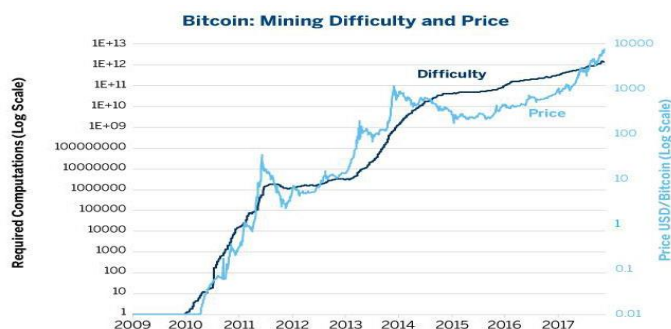
Proces těžení (mining)²², který je základní činností pohánějící decentralizovanou síť bitcoinu, je činností poměrně sofistikovanou, vyžadující splnění specifických softwarových i hardwarových požadavků. Většina softwaru, který je nutný pro účast na těžení, je nabízena zdarma. V minulosti a v počátcích vývoje bitcoinu byly k těžení využívány především výkonné počítačové grafické karty. Ty se ukázaly být velmi efektivní pro provádění příslušných matematických výpočtů. S postupnou popularizací a růstem hodnoty bitcoinu začala vznikat i první dedikovaná hardwarová řešení typu ASIC²³ (Application-Specific Integrated Circuits),

²¹How many bitcoins are in circulation[online]. [vid. 31. březen 2018]. Dostupné z: https://en.bitcoinwiki.org/wiki/File:How_many_bitcoins_are_in_circulation_.jpg

²² Everything you need know about mining[online]. [vid. 20. listopad 2018]. Dostupné z: <https://www.bitcoinmining.com/>

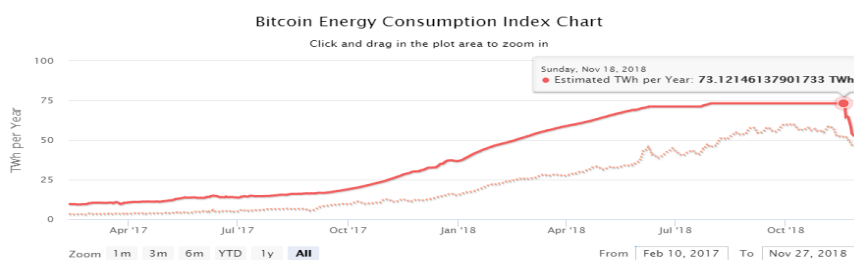
²³Application-Specific Integrated Circuit [online]. [vid. 31. březen 2018]. Dostupné z: <https://www.techopedia.com/definition/2357/application-specific-integrated-circuit-asic>

kteřá již byla určena striktně pro těžení. Nárůst celkového výkonu v síti ale neznamená zrychlení celkové těžby BTC. Řešení sítě bitcoinu počítá se změnami výpočetního výkonu v rámci sítě a automaticky koriguje obtížnost zadávaných kryptografických úkolů. K této korekci dochází zhruba každých čtrnáct dnů.



Graf 2 Růst obtížnosti výpočtu matematických úloh pro ověření transakcí v závislosti na růstu kurzu BTC/USD²⁴

Nicméně s vyšším výkonem speciálních hardwarových řešení nedošlo k zásadnímu snížení vstupních nákladů spojených s extrémní spotřebou elektrické energie. Těžení bitcoinu v současné době je tak rentabilní pouze pro velké těžební farmy, které nabízejí extrémní výpočetní výkon a mají tak šanci správně vyřešit požadované matematické úlohy. V současné době dochází k ověření a zařazení nových bloků průměrně každých deset minut. Nutno podotknout, že řešení ve formě dnes již komerčního těžení se stalo značným ekologickým problémem. Celkový objem využité energie představuje 0,5%²⁵ celosvětové spotřeby elektřiny, tedy o něco málo méně, než je celková spotřeba celé ČR za rok. Ta činí 73,8 TWh za rok²⁶.



Graf 3 - Graf zobrazuje nárůst spotřeby el. energie v rámci sítě bitcoin. Celkový produkovaný výkon²⁷

²⁴ bitcoinDifficulty Chart and Graph.[online]. [vid. 31. březen 2018]. Dostupné z: <https://www.coinwarz.com/difficulty-charts/bitcoin-difficulty-chart>

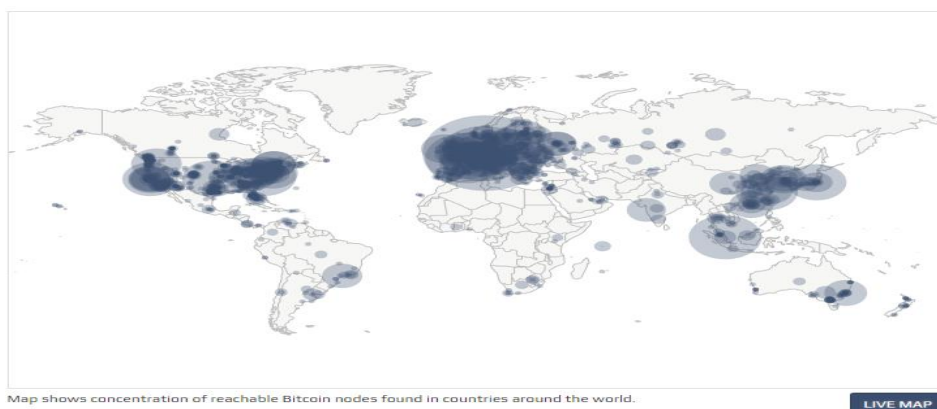
²⁵ Bitcoin's energy usage is huge – we can't afford to ignore it. [online]. [vid. 17. leden 2018]. Dostupné z: <https://www.theguardian.com/technology/2018/jan/17/bitcoin-electricity-usage-huge-climate-cryptocurrency>

²⁶ Spotřeba elektřiny v Česku stoupla na nový rekord. [online]. [vid. 24. květen 2018]. Dostupné z: <https://zpravy.aktualne.cz/ekonomika/spotreba-elektřiny-v-cr-loni-vzrostla-na-rekordnich-73-8-twh/r~688d7a705f3011e8bbdd0cc47ab5f122/>

²⁷ bitcoinEnergyConsumption Index. [online]. [vid. 31. březen 2018]. Dostupné z: <https://digiconomist.net/bitcoin-energy-consumption>

Odměna

V případě správného vyřešení matematické úlohy je řešitel, tedy těžař, odměněn. Tato odměna se v průběhu vývoje bitcoinu snižuje. Po vytěžení každých 250 000 bloků²⁸, tedy zhruba každé čtyři roky je krácena o polovinu. Na počátku tak byli řešitelé odměňováni za vytěžený blok částkou 50 BTC. V současné době za správné řešení se získává 12,5 BTC. Právě tato odměna za práci těžařům představuje rovněž i proces emitace nových mincí do oběhu. S růstem popularity, a především s vlnami růstu kurzu BTC, dochází k nárůstu členů decentralizované sítě.



Obrázek 6 Koncentrace aktivních nodů sítě bitcoin k 27.11 2018²⁹

1.4. Vznik bitcoinu³⁰

Zdroje, ze kterých technologické principy bitcoinu čerpají

bitcoin, tedy první skutečně prorazivší kryptoměna, vznikla na základě dlouholetých úvah a pokusů, které přinesly základní principy, ze kterých bitcoin následně vycházel. Díky nerealizovanému Bit Gold³¹ nebo prvnímu funkčnímu schématu proof-of-work, byl umožněn vznik kryptoměn tak, jak je známe dnes.

Vznik bitcoin

Historie bitcoinu sahá do roku 2008, kdy byla poprvé registrována doména bitcoin.org a záhy uveřejněny i podklady k funkčním schématům bitcoinu. Tyto podklady s názvem („bitcoin“) „A Peer-to-Peer Electronic Cash System“ byly rozeslány seznamu uživatelů z komunity

²⁸Bitcoin Block Reward Halving Countdown. [vid. 7. prosinec 2018]. <https://www.bitcoinblockhalf.com/>

²⁹BitNodes[online]. [vid. 27. listopad 2018]. Dostupné z: <https://bitnodes.earn.com/>

³⁰Bitcoin History: Timeline, Origins and Founder.[online]. [vid. 17. srpen 2018]. Dostupné z: <https://www.thestreet.com/investing/bitcoin/bitcoin-history-14686578>

³¹What Is Bit Gold? The Brainchild of Blockchain Pioneer Nick Szabo.[online]. [vid. 22. květen 2018]. Dostupné z: <https://coincentral.com/what-is-bit-gold-the-brainchild-of-blockchain-pioneer-nick-szabo/>

zabývající se kryptografií a její implementací do nového funkčního systému plateb. Autorem tohoto emailu s popisem funkčních principů decentralizované sítě byl odesílatel, který byl podepsán jako Satoshi Nakamoto. Krátce poté na začátku roku 2009 již byla spuštěna samotná síť bitcoin a byl vytěžen první blok, byť jediným uživatelem v tu chvíli byl právě a pouze zmíněný Satoshi Nakamoto. Součástí tohoto bloku byla i informace z titulku The Times vydaná 3. ledna 2009³², což má o prokazovat právě datum prvního úspěšného vyřešení a zařazení bloku do blockchainu. První transakce mezi dvěma uživateli pak proběhla až o rok později. Z dnešního pohledu působí poněkud úsměvně fakt, že první finanční operace posloužila k nákupu dvou kusů pizzy. A to za cenu domluvenou cenu 10 000 BTC, což při dnešním kurzu odpovídá 1 386 000 000 Kč..

Satoshi Nakamoto

Samotná postava autora konceptu bitcoinu vzbuzuje značné emoce a pro mnoho seriózních investorů právě jeho nejasný původ představoval značný problém. Skutečná identita Satoshi Nakamota není doposud odkryta a není tak jasné, zdali šlo o jediného člověka či dokonce skupinu lidí. V každém případě v období po spuštění celého projektu dokázal vygenerovat částku okolo jednoho miliónu BTC, které se ovšem nikdy nedostaly do oběhu. Podle dostupných dat z blockchainu je patrné, že tato částka byla vytěžena na jednom počítači, o čemž svědčí i pravidelné výpadky v záznamech o vytěžených blocích. Poslední komunikace s entitou Satoshi Nakamoto proběhla na začátku roku 2011 a od té doby se subjekt Satoshi Nakamoto zcela vytratil. To i nadále vzbuzuje spekulace o tom, jaký byl původní záměr tvůrce bitcoinu.

bitcoin Foundation³³

The bitcoin Foundation je americká nezisková společnost, která vznikla v roce 2012. Byla založena především za účelem jednotného vývoje a zvýšení reputace bitcoinu, který v letech před jejím vznikem byl spojován s několika skandály. Zároveň měla posloužit jako instituce, která bude pro laickou i odbornou veřejnost představovat instituci s relevantními informací o bitcoinu a jeho směřování. Celý model bitcoin Foundation je inspirován neziskovou společností Linux Foundation dozorující nad vývojem operačních systémů na bázi Linuxu. Zakladateli a původními členy bitcoin Foundation jsou průkopníci v oblasti kryptoměn Gavin Andresen, Charlie Shrem, Mark Karpeles, Peter Vessenes, Roger Ver, Patrick Murck a Mehul Puri. V další

³²Bitcoin's Quirky Genesis Block Turns Eight Years Old [online]. [vid. 3. leden 2018]. Dostupné z: <https://news.bitcoin.com/bitcoins-quirky-genesis-block-turns-eight-years-old-today/>

³³bitcoin foundation[online]. [vid. 10. listopad 2018]. Dostupné z: <https://bitcoinfoundation.org/>

fázi byla členská základna bitcoin Foundation rozdělena na více částí: na zakládající členy, hlavní členskou základnu a zástupce průmyslu. Členem se může stát kdokoliv, kdo má zájem o vývoj a vše spojené s bitcoinem. Nutno podotknout, že bitcoin Foundation nemá exekutivní funkci a už z principu nemůže sama o sobě žádným způsobem přímo ovlivnit vývoj bitcoinu.³⁴³⁵

Vývojové milníky bitcoin v čase

1998–2009- Formování základních technologických postupů

V tomto čase se formovaly základy a myšlenky, z nichž kryptoměny vycházely. Vzniklo mnoho projektů jako B-Money nebo Bit Gold, které využívaly mnoho postupů následně využitých v koncepci bitcoinu, ale projekty nikdy nedospěly do finální fáze.

2008–Satoshi

První zmínky o projektu bitcoinu spojeném s postavou Satoshi Nakamota. Zároveň rozeslání konceptu bitcoinu úzkému okruhu uživatelů zabývajících se kryptografií a jejím využitím.

2009 -Zrození bitcoinu

Jsou vytěženy první bloky a vytvořeny první aplikace umožňující těžení bitcoinu. Dochází k připojení více uživatelů, ale bitcoin stále zůstává doménou pár desítek nadšenců.

2010 – První reálné transakce

Rok 2010 je rokem kdy byly provedeny první platební transakce, byť jen mezi jednotlivými uživateli. Rovněž je to první rok, kdy lze říci, že bitcoin byl poprvé ohodnocen vůči americkému dolaru právě na základě provedených transakcí.

2011 – Vznik první konkurence a první akceptace plateb bitcoinem

Popularita bitcoinu je na vzestupu, k čemuž přispěla především akceptace některých neziskových společností včetně WikiLeaks³⁶. Vznikají první virální videa³⁷ a bitcoin se tak dostává do povědomí širší veřejnosti. Zároveň se začínají objevovat další kryptoměny, které

³⁴ bitcoin foundation[online]. [vid. 10. listopad 2018]. Dostupné z: <https://bitcoinfoundation.org/>

³⁵WhatisthebitcoinFoundation, and WhatDoesit Do? [online]. [vid. 18. duben 2018]. Dostupné z: <https://www.investopedia.com/tech/what-bitcoin-foundation-and-what-does-it-do/>

³⁶ WikiLeaks Asks For Anonymous Bitcoin Donations [online]. [vid. 14. červen 2011]. Dostupné z: <https://www.forbes.com/sites/andygreenberg/2011/06/14/wikileaks-asks-for-anonymous-bitcoin-donations/#c38dc144f73b>

³⁷Whatis bitcoin[online]. [vid. 10. listopad 2012]. Dostupné z: <https://www.weusecoins.com/>

využívají koncepty bitcoinu s nejrůznějšími modifikacemi. Mezi nejznámější patří Litecoin, jehož vývoj je s bitcoinem velmi úzce spjat.

2012– Růst popularity

Rok 2012 je ve znamení růstu popularity a pronikání bitcoinu do mainstreamu. bitcoin se začíná objevovat v populárních seriálech i talk show, především v USA. Zároveň nejpoblárnější platební brána BitPay oznamuje první milník s více jak tisícem obchodníků³⁸ využívajících jejich služby.

2013– První bitcoinová bublina

Rok 2013 byl především ve znamení první bitcoinové bubliny, která jasně ukázala nezralost bitcoinu coby reálné alternativy pro elektronické platby. Hodnota se během velmi krátkého času vyšplhala až k \$1000, čímž se bitcoin stal rychle zajímavou spekulací pro mnoho už nejen drobných investorů. Souběžně s rostoucím kurzem se začínají objevovat i první problémy technického rázu, kdy došlo prvnímu rozštěpení blockchainu a nestandardnímu dočasnému pozastavení obchodování. Zároveň výše obchodovaného objemu peněz vzrostla natolik, že neunikla zájmu mnoha státních regulátorů finančních trhů. V Thajsku dochází prvnímu celostátnímu zákazu používání Bitconu³⁹ a ve Spojených státech jsou bitcoiny zatím spojovány především s nelegální činností, a to hlavně s kauzou Silk Road⁴⁰. Na tomto nelegálním tržišti uloženém v deep webu, tedy v běžně nedostupné části internetu, se právě bitcoiny využívaly jako měna pro nákup prakticky všeho zakázaného. Po zásahu FBI a konfiskaci nelegálního tržiště Silk Road včetně hlavní peněženky přichází další špatná zpráva. Největší směnárna není schopná vyplácet bitcoiny svým klientům a obecná nestabilita způsobuje prudký poklesu kurzu BTC, který tak rychle ztrácí šedesát procent své hodnoty.

2014 – Krach Mt.Gox

Popularita bitcoinu dál roste, stejně je tomu u ostatních kryptoměn. bitcoin začíná být akceptován i mnoha hlavními hráči na poli IT technologií jako je Dell nebo Microsoft. To vše

³⁸ BitPay Exceeds 1,000 Merchants Accepting Bitcoin [online]. [vid. 11. září 2012]. Dostupné z: <https://www.businesswire.com/news/home/20120911005855/en/BitPay-Exceeds-1000-Merchants-Accepting-Bitcoin>

³⁹ Thailand bans Bitcoin [online]. [vid. 30. července 2013]. Dostupné z: <https://www.ft.com/content/c08a26df-537c-3bd1-a10b-734050003839>

⁴⁰ The History of Silk Road: A Tale of Drugs, Extortion & Bitcoin [online]. [vid. 20. listopadu 2018]. Dostupné z: <https://blockonomi.com/history-of-silk-road/>

ovšem zůstává ve stínu krachu největší bitcoinové burzy MtGox⁴¹. Uživatelé tak přicházejí celkem o více než 850 000 BTC. Dochází opět ke značné ztrátě hodnoty bitcoinu, který se propadá na pouhých 200 USD za BTC.

2015 – Problémy směnárů pokračují

Další rok je opět spojen s problémy bitcoinových směnárů. Ty pokračují, ovšem samotný provoz decentralizované sítě funguje bez větších problémů. Jasně se ukazuje, že nejrizikovější na celém řetězci je právě prostředník mezi uživatelem a sítí bitcoin. Obvykle tento problém nastává na úrovni zajištění konverze na státní fiat měny. I přesto celosvětově akceptuje bitcoin více než sto tisíc obchodníků⁴².

2016– bitcoin na vzestupu

I v tomto roce dochází k problémům a krachům několika velkých směnárů v čele s Bitfinexem. Úroveň výpočetního výkonu s popularitou těžení a rostoucím kurzem dosahuje výkonu 1 exahash/sec⁴³. bitcoin je nově akceptován největšími prodejci počítačových her, stejně jako třeba švýcarskými dráhami či přepravní společností Uber.

2017 – Prudký vzestup kurzu a prudký propad

Rok 2017 lze nazvat rokem bitcoinu, kdy popularita této kryptoměny dosáhla vrcholu. Díky kurzu, který se ve svém maximu hodnoty 19 000 USD za jeden BTC stává mainstreamovým hitem. Investovat do kryptoměn se zdálo být zárukou ke zbohatnutí. Vysoký kurz přináší i vysoké poplatky za transakce a znatelné snížení rychlosti prováděných transakcí. I to byl jeden z důvodů proč historicky poprvé dochází k takzvanému splitu, a to zcela záměrnému rozdělení blockchainu na dvě části. Nově tak vzniká kryptoměna bitcoin Cash, která může díky větší kapacitě jednotlivých bloků nabídnout vyšší rychlost vhodnou pro menší platby. Historická data před rozdělením blockchainu zůstávají u obou kryptoměn identická⁴⁴.

⁴¹ THE INSIDE STORY OF MT. GOX, BITCOIN'S \$460 MILLION DISASTER [online]. [vid. 3. březen 2014]. Dostupné z: <https://www.wired.com/2014/03/bitcoin-exchange/>

⁴² All Bitfinex clients to share 36% loss of assets following exchange hack [online]. [vid. 7. květen 2016]. Dostupné z: <https://www.theguardian.com/technology/2016/aug/07/bitfinex-exchange-customers-receive-36-percent-loss-tokens/>

⁴³ Bitcoin's Hashrate Crosses exahash.[online]. [vid. 7. květen 2016]. <https://news.bitcoin.com/bitcoin-hashrate-four-exahash-per-second/>

⁴⁴ Bitcoin's Roller-coaster Ride May Get Wilder. [online]. [vid. 23. prosinec 2017]. <https://www.voanews.com/a/bitcoin-wild-ride/4176331.html>

2018 – Křehká stabilita

V roce 2018 následuje rychlé vystřízlivění, kdy bitcoin během pár dnů ztrácí opět téměř padesát procent své hodnoty. Propad se zastavuje až na částce 6 000 USD za 1BTC, kde se kurz stabilně drží téměř po celý zbytek roku. Konec roku 2018 znamená opět další propad o 30 %, což znamená z pohledu investorů další ránu. Pro rozvíjení obchodu za využití plateb kryptoměnami to je spíše přínosné. Pozitivní přístup ke kryptoměnám je regionálně poměrně jasně definován. Hlavním hnacím motorem vývoje kryptoměn je západní svět. Mezi zeměmi otevřeně podporujícími kryptoměny a nabízejícími určitý právní rámec tak patří USA, Kanada, Austrálie a většina zemí EU. bitcoin zůstává ilegální v Číně, Rusku, Vietnamu a Jižní Koreji stejně jako části zemí Jižní Ameriky (Bolívie, Kolumbie a Ekvádor)⁴⁵.

Vývoj kurzu a korelace s popularitou

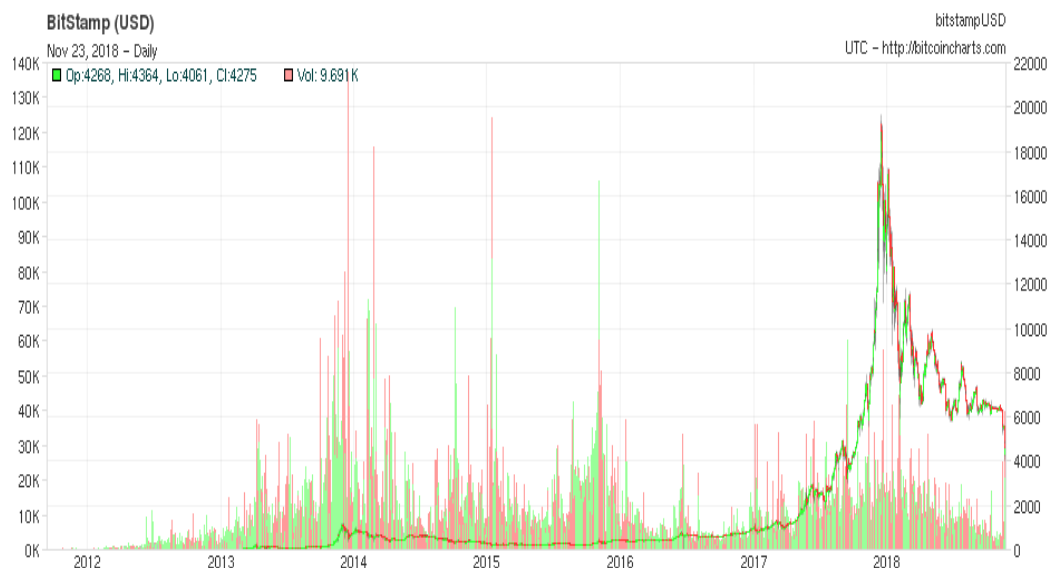
Jedním z největších problémů, se kterým se potýká bitcoin, je volatilita kurzu. Přestože původní záměr byl vytvořit platební alternativu k centralizovanému systému, který představují centrální banky, jsou v současnosti kryptoměny vnímány především jako investiční příležitost. V důsledku toho v průběhu historie došlo k mnoha finančním bublinám spojeným právě se zběsilými nákupy bitcoinu. Na druhou stranu právě finanční bubliny a příležitosti extrémních, byť nejistých zisků, byly tou nejlepší reklamou a šancí, jak dát světu o kryptoměnách vědět. Většina konkurenčních kryptoměn je úzce navázána na směnný kurz bitcoinu, a proto do značné míry jsou vystaveny stejným problémům. Většina krizí v historii vývoje BTC je spojena s finančními krizemi ve světě (např. Kyperská krize – 2012⁴⁶), zásahy státních institucí (zákaz používání kryptoměn v Číně – 2018⁴⁷) nebo hackerskými či jinými útoky na burzy (Mt.Gox – 2014⁴⁸). Tato nestabilita do značné míry komplikuje uvedení kryptoměn do přímého zapojení, například do využití v e-commerce a retailu. Z tohoto důvodu je v současné době optimální využívat platebních brán, která je řešena v následujících kapitolách.

⁴⁵ Legality of bitcoin by country or territory [online]. [vid. 7. prosinec 2018]. Dostupné z: https://en.wikipedia.org/wiki/Legality_of_bitcoin_by_country_or_territory

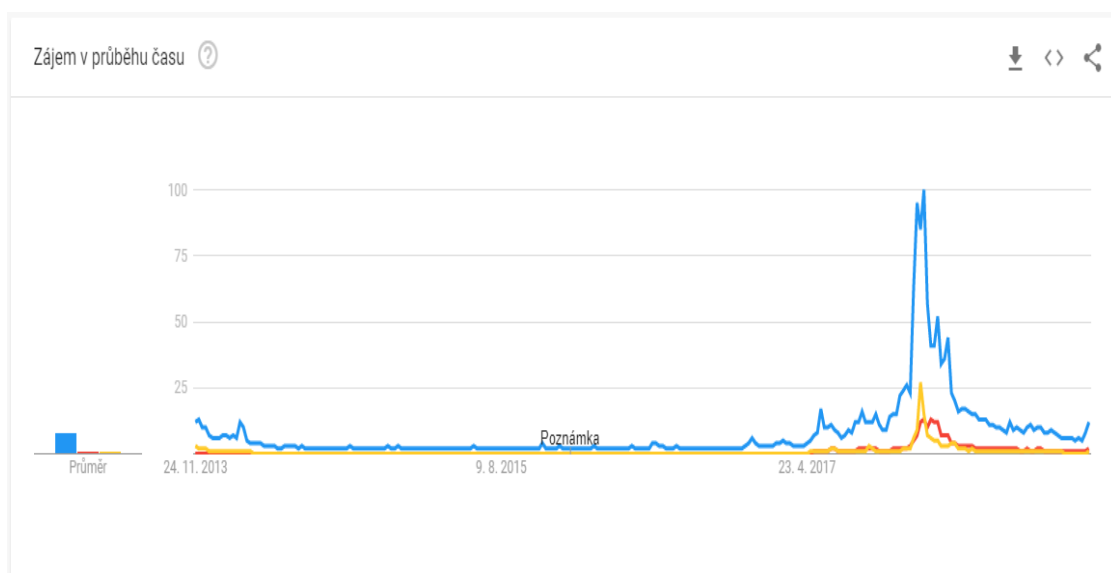
⁴⁶ Kypr je pátou zemí eurozóny, která kvůli krizi žádá o finanční pomoc. [online]. [vid. 25. červen 2012]. Dostupné z: <https://domaci.ihned.cz/c1-56296040-kypr-je-patou-zemi-eurozony-ktera-kvuli-krizi-zada-o-financi-pomoc>

⁴⁷ CHINA OFFICIALLY BANS ALL CRYPTO-RELATED COMMERCIAL ACTIVITIES [online]. [vid. 22. květen 2018] Dostupné z: <https://bitcoinist.com/china-officially-bans-crypto-activities/>

⁴⁸ THE INSIDE STORY OF MT. GOX, BITCOIN'S \$460 MILLION DISASTER [online]. [vid. 3. březen 2014]. Dostupné z: <https://www.wired.com/2014/03/bitcoin-exchange/>



Graf 4 Extrémní volatilita kurzu BTC od roku 2012 do roku 2018⁴⁹



Graf 5 Zájem o výraz bitcoin (modrý), Litecoin (žlutý) a Cryptocurrency (červený) v Google Trends⁵⁰

1.5. Burzy a platební brány

Burzy a platební brány

Nedílnou součástí fungování obchodu s kryptoměnami jsou burzy a směnárny, které umožňují konverzi BTC na fiat měny a obecně obchodování s kryptoměnami. Většina burz funguje na základě nabídky a poptávky jednotlivých uživatelů, z čehož vychází i kurz pro měnovou konverzi. V současné době jednoznačně největší množství objemu finančních transferů prochází právě skrz tyto burzy. Můžeme-li o konceptu bitcoinu potažmo blockchainu hovořit

⁴⁹bitcoincharts[online]. [vid. 23. listopad 2018]. Dostupné z: <https://bitcoincharts.com/>

⁵⁰ Zájem o výraz bitcoin, [vlastní] ..[vid 7. duben 2018]. Dostupné z: <https://trends.google.com/trends/?geo=US>

jako o velmi spolehlivém, pak naopak, burzy, tedy prostředník na cestě kryptoměny do běžného finančního světa, představují jedno z největších rizik. Burzy jsou prakticky permanentně pod útoky hackerů a výjimkou nejsou interní útoky uvnitř společností. To vše je logickým důsledkem vysokého objemu finančních prostředků nacházejících se v těchto institucích v jeden okamžik. A zároveň ve srovnání s fyzickými loupežemi umožňují útočníkům prakticky beze stopy uniknout. Historie bitcoinu je protknuta krachy mnoha burz, z nichž většina patřila k lídrům v této oblasti. Z mnoha můžeme zmínit MTGox nebo BTC-E.⁵¹ Platební brány hrají z pohledu obchodníka, který by se rozhodl přijímat možnost platby bitcoinu, naprosto nedílnou součást modelu plateb. Vzhledem k velmi vysoké volatilitě bitcoinu je velmi obtížné jej dlouhodobě využívat bez přítomnosti platebních bran. Ty eliminují obrovská a neodhadnutelná rizika, daná zmíněnou volatilitou bitcoinu. Obchodník tak je oproštěn od kurzového rizika a systém plateb se v tu chvíli rovná systému plateb přes platební kartu či Paypal. bitcoinová síť je pak využívána čistě k přenosu dat o transakci. Novým rizikem se v tomto případě ovšem může stát provozovatel platební brány. Stejně jako v případě bitcoinových směnárén totiž jakýkoliv vstup třetí strany do bitcoinové transakce znamená riziko, které nelze systémově eliminovat.

Následují příklady burzovních a směnárenských poskytovatelů

Bitstamp

Založení: 2011

Sídlo: Lucembursko

Poplatky za směnu: 0,25-0,10 % (v závislosti na objemu)

Obchodované měny: USD, EUR. BTC, LTC, ETH, XRP

Směnárna Bitstamp patří mezi nejúspěšnější evropské projekty tohoto druhu. Velký podíl na vzestupu Bitstampu byl způsoben krachem konkurenčního projektu Mt.Gox, pro který nabídla spolehlivou alternativu. Ani této společnosti se ovšem nevyhnuly problémy se zabezpečením, kdy v roce 2015 bylo z peněženek společnosti zcizeno 19 000 BTC⁵². Firma od té doby investovala nemalé prostředky do zabezpečení a získání patřičných oprávnění. V roce 2016 obdržela společnost lucemburskou licenci platební společnosti, což jí umožňuje podnikat v rozsahu celé EU. Zároveň jako jeden z mála subjektů mezi krypto směnárnami reagovala na

⁵¹Hereyouwillfind a documented list ofcryptocurrencyexchange hacks, [online].[vid. 27.4 2018].
<https://rados.io/list-of-documented-exchange-hacks/>

⁵² Details of \$5 Million Bitstamp Hack Revealed [online].[vid 7. duben 2015]. Dostupné z:
<https://www.coindesk.com/unconfirmed-report-5-million-bitstamp-bitcoin-exchange>

výzvy nejvyššího státního zástupce pro stát New York k provedení auditu zabezpečení finančních prostředků klientů, kterým úspěšně prošla a plánuje se ucházet o licenci BitLicense.

5354

Coinbase

Založení: 2012

Sídlo: USA

Poplatky za směnu: 0,5 %

Obchodované měny: USD, EUR, BTC, LTC, ETH, fiat měny

V současné době největší směnárna na světě realizuje většinu obchodů ve Spojených státech amerických. Celosvětově měla tato společnost v roce 2017 registrovaných 13 300 000 uživatelů. Tato směnárna nabízí možnost vkladu prostředků nejen standardně bankovními převody, ale i použitím platebních karet či za pomoci služeb PayPal, Stripe či Braintree. Spolu se směnářenskými službami nabízí i služby platební brány a vyvíjí i vlastní verzi kryptoměnové peněženky, což z Coinbase činí nejkomplexnějšího hráče na trhu. Výhodou je i volně přístupné API (programové rozhraní), které mohou partneři Coinbase využívat pro aplikace ve svých programových řešeních.⁵⁵

Kraken

Založení: 2011

Sídlo: USA

Poplatky za směnu: 0,16/0,26 %-0,00/0,10% (prodej/nákup v závislosti na objemu)

Obchodované měny: USD, EUR, BTC, LTC, ETH, fiat měny

Dalším významným poskytovatelem na poli směnářských služeb kryptoměn je firma Kraken sídlící v San Franciscu, USA. Zakladatel firmy Jasse Powell se podílel na odstranění bezpečnostních problémů již zaniklé služby MT.Gox a poté označil právě úroveň zabezpečení za klíčovou pro úspěch podobných služeb. Po dvou letech vývoje byla služba spuštěna, tedy v roce 2013, kdy nabízela konverze mezi kryptoměnami bitcoin, Litecoin a Eurem. V roce 2013 rovněž uzavřela klíčové spojení s německou bankou Bafin, což službě nově umožnilo přijímat SEPA platby. Na rozdíl od většiny ostatních velkých hráčů se negativně postavila

⁵³Bitstamp.[online]. [vid. 23. listopad 2018]. Dostupné z: <https://www.bitstamp.net/>

⁵⁴ BitLicenseRegulatoryFramework.[online]. [vid. 23. 7 2013]. Dostupné z: https://www.dfs.ny.gov/legal/regulations/bitlicense_reg_framework.htm

⁵⁵Coinbase.[online]. [vid. 23. listopad 2018]. Dostupné z: <https://www.coinbase.com/>

k regulaci ve státě New York, kdy zcela odmítla spolupracovat a otevřeně odmítla i možnost se ucházet o licenci BitLicense^{56, 57}.

Binance

Založení: 2017

Sídlo: Japonsko

Poplatky za směnu: 0,10 %

Obchodované měny: USD, EUR, BTC, LTC, ETH, fiat měny

V současnosti kryptoměnová směnárna s největším obchodovaným objemem kryptoměn. Firma Binance byla původně založena v Šanghaji v roce 2017, odkud se musela přesunout v důsledku zákazu používání kryptoměn v Číně. Zamířila tedy do Japonska, kde firma dokázala dosáhnout kapitalizace svého trhu v hodnotě 1,3 miliardy USD, a to na počátku roku 2018. Plánována je expanze do Evropy a Anglie. Binance zcela odmítá BitLicence, což může do budoucna představovat problém v získání přístupu na klíčový trh v USA.⁵⁸

Příklady poskytovatelů platebních bran

CoinbaseCommerce

Coinbase patří k lídrům v oblasti platebních bran, kdy nabízí plné portfolio služeb od směnářenské činnosti, přes řešení platební brány až k vlastním softwarovým prostředkům. Integrace platební brány Coinbase je velmi jednoduchá - postačuje vložení jednoduchého kódu v HTML na web či blog odkazující na vaši peněženku. Nechybí ani podpora široké škály populárních e-commerce řešení jako je WordPress nebo Joomla, pro která jsou vytvořeny jednoduché pluginy. Součástí systému Coinbase je i jednoduchý fakturační systém umožňující vytvářet faktury v kryptoměnách a zasílat je v elektronické podobě klientovi. Bližší technické informace v kapitole 2.1 *Analýza dodavatele*.⁵⁹

BitPay

BitPay patří mezi průkopníky v této oblasti služeb a nabízí rovněž ucelené portfolio služeb. Na rozdíl od Coinbase nabízející své služby především v USA je BitPay velmi aktivní i v České

⁵⁶BitLicenseRegulatoryFramework.[online]. [vid. 23. 7 2013]. Dostupné z: https://www.dfs.ny.gov/legal/regulations/bitlicense_reg_framework.htm

⁵⁷Kraken.[online][vid. 23. 1 2018]. Dostupné z: <https://www.kraken.com/>

⁵⁸Binance.[online]. [vid. 23. 1 2018]. Dostupné z: <https://www.binance.com/en>

⁵⁹Coinbase Commerce.[online]. [vid. 28. 1 2018]. Dostupné z: <https://commerce.coinbase.com/>

republike, potažmo celé EU. Mezi klienty tohoto poskytovatele najdeme renomované firmy Microsoft, Alza a.s. Virgin nebo Shopify.BitPay, jimž garantuje konverzní kurzy v kryptoměnách BTC i BCH (bitcoin cash), které lze směnit za fiat měny. Tímto způsobem zaručuje ochranu před fluktuací kurzu. Systém rovněž umožňuje fakturaci, kterou lze následně otevírat přímo v klientských peněženkách. Základním požadavkem je podpora Paymentprotocolu⁶⁰ v konkrétní zvolené peněžence. Zajímavou alternativou je i možnost využití BitPay platební karty, která je vydávána společností VISA. To umožňuje v rámci mobilní aplikace instantně konvertovat kryptoměny na USD a využívat možností standardní platební karty.⁶¹

Coingate

Coingate je evropská platební brána se sídlem v Litvě, která byla založena v roce 2014. I v tomto případě může uživatel využít konverzí do USD či EUR, a to nejen z bitcoinu, ale i mnoha další kryptoměn. I tento poskytovatel nabízí širokou podporu pro jednoduchou implantaci tohoto řešení do e-commerce. Ať jde o pluginy pro řešení jako je VirtueMart nebo Magento až po otevřenou API. Zajímavou alternativou pro retailery je bitcoin Point ofSale⁶², které nabízí instantní řešení pro možnost akceptace plateb bitcoinem. Coingate sice patří k menším firmám, ale přesto a možná proto vyniká svou flexibilitou a velmi svižným vývojem.⁶³

1.6. Alternativní kryptoměny

V dnešní době se můžeme setkat doslova s tisíci druhy kryptoměn, které se liší v mnoha ohledech. I když je pro laickou veřejnost synonymem pro kryptoměny právě bitcoin, bylo by chybou nepředstavit i několik dalších alternativních měn. Mnoho z nich vychází alespoň z části z konceptu z bitcoinu a prakticky všechny využívají technologii blockchainu. Ta se ukazuje vývojově jako zcela zásadní. Nové kryptoměny se obvykle snaží odstranit nedostatky původního bitcoinu jako je omezená rychlost, počet zpracovaných transakcí či velká energetická náročnost. Mnoho z nich nabízí zcela novou funkčnost a často se tak neomezují pouze na platební transakce, ale najdou uplatnění i v jiných oblastech. Kryptoměny vzhledem

⁶⁰ Bitpay payment protocol.[vid. 3. 12 2018]. Dostupné z <https://support.bitpay.com/hc/en-us/articles/360015839672-Frequently-Asked-Questions-About-BitPay-and-Payment-Protocol-BIP70->

⁶¹ Bitpay .[online]. [vid. 23. 1 2018]. Dostupné z: <https://bitpay.com/>

⁶² Point of Sale.[online]. [vid. 23. 1 2018]. Dostupné z: <https://coingate.com/bitcoin-pos>

⁶³ Coingate .[online]. [vid. 23. 1 2018]. Dostupné z: <https://coingate.com/>

ke způsobu obchodování s nimi jsou velmi úzce propojené a velmi často se tak mezi nimi přenáší i měnová nestabilita a další trendy.

XRP

Vznik: 2014

Market Cap: 15 102 009 025\$

Ripple se svým měnovým označením XRP patří mezi nejpopulárnější kryptoměny, i když už označení samo „kryptoměna“ je kontroverzní. Na rozdíl od většiny ostatních kryptoměn totiž princip Ripple není založen na proofofwork, tedy zpracování transakcí za účelem ověření. Všechny tokeny XRP byly vygenerovány tzv. premined procesem. Tedy vznikly samovolně a do značné míry popírají základní ideu decentralizované sítě. Samotní tvůrci XRP, tedy společnost XRP Labs, vlastní šedesát procent tokenů z celkového počtu. Síť je tak kontrolována de facto několika subjekty. Tato částka je ovšem uschována pod časovým zámekem na escrow účtu. To zaručuje, že tokeny budou uvolňovány postupně a nenastane tak situace, že by kvůli nepřiměřenému uvolnění tokenů došlo k ovlivnění trhu. Díky principu uzavírání plateb na základě rozhodnutí většiny a faktu, že velkou část ověřovacích serverů v rámci sítě tvoří velké finanční instituce, banky nebo přímo RippleLabs, probíhají platby v Ripple síti prakticky okamžitě v řádu několika sekund a s minimálními poplatky. Což je v kontrastu se sítí bitcoin, která díky spekulacím bývá dost často přetížena. Technologie a principy, na kterých pracuje Ripple jsou zajímavé především z pohledu finančních institucí, jimž nabízí řešení, které lze snadno implementovat do současných systémů.⁶⁴

Ethereum

Vznik: 2015

Market Cap: 12 017 746 988\$

Ethereum na rozdíl od kryptoměny Ripple přímo navazuje na koncept bitcoinu, a i z tohoto důvodu je často označována jako bitcoin 2.0. Je dílem kanadského programátora Vitalika Buterina, který zde využil zkušenosti nasbírané za svého působení ve vývojovém týmu bitcoinu. Hlavním rozdílem je funkčnost obou kryptoměn. Jestliže je bitcoin vytvořen za účelem směny a je tedy především platebním nástrojem, pak možnosti Etherea jsou podstatně rozmanitější. I v tomto případě jde o decentralizovanou kryptoměnu využívající technologii blockchainu,

⁶⁴Ripple, [online].[vid. 30. 11 2018]. Dostupné z: <https://www.investopedia.com/terms/r/ripple-cryptocurrency.asp>

navíc s využitím i na správu smart contract⁶⁵. Chytré kontrakty mají nabízet široké možnosti využití decentralizované architektury, především v oblasti zabezpečených databází. Výhodou je i větší otevřenost celého řešení, kdy ve srovnání s bitcoinem nabízí možnost tvorby vlastních programů využívajících tuto síť. V podstatě je tak možné využít tento koncept k nabízení výměny informací i komodit všeho druhu. Stejně jako bitcoin využívá k ověřování procesů proof of work, kdy těžaři těží pomyslné palivo Ether, kterým jsou pak nové projekty poháněny. Těžení je v tomto případě koncipováno tak, aby i jednotlivec či člen malého poolu (sdružení více těžařů) měl šanci dosáhnout na úspěšný výsledek na úkor profesionálních řešení typů ASIC.⁶⁶

bitcoin Cash

Market Cap: 3 171 170 061 \$

Poslední kryptoměnou, kterou jsem se rozhodl v této práci zmínit, je bitcoin Cash. Jde o zajímavý derivát bitcoinu, který vznikl rozvětvením tzv. forkem⁶⁷ (rozštěpením), kdy se účetní kniha od určitého okamžiku rozdělila na dvě. Tím vznikla nová kryptoměna BCH, kdy důvodem byla především technická omezení bitcoinu. Ta se projevila především v roce 2017, kdy s enormním zájmem o BTC došlo k výraznému zvýšení počtu transakcí, které bylo nutné zapsat do bloků. Vzhledem k technickému omezení, které představuje velikost bloku 1 MB často docházelo díky překročení tohoto limitu k odmítnutí zapsání bloku do blockchainu. Tím se síť výrazně zpomalila a rychlost transakcí se rapidně zvedla. Na druhé straně bitcoin Cash v dnešní době nabízí velikost bloku 8 MB, čímž bylo dosaženo výrazného nárůstu výkonu sítě. Hlavním účelem bitcoin Cash by tak mělo být zaměření na transakce menších plateb na což ostatně odkazuje již samotný název kryptoměny.⁶⁸

⁶⁵ How Do Ethereum Smart Contracts Work? [online].[vid. 30. 11 2018]. Dostupné z: <https://www.coindesk.com/information/ethereum-smart-contracts-work>

⁶⁶Ethereum, [online].[vid. 30. 11 2018]. Dostupné z: <https://www.ethereum.org/>

⁶⁷

⁶⁸ bitcoin Cash, [online].[vid. 30. 11 2018]. Dostupné z: <https://www.bitcoincash.org/>

Cryptocurrency Market Capitalizations

Thu, Nov 29th, 2018

? Help

USD ♥

download

Name	Symbol	Last	%Chg	Volume	Market Cap ▼	Supply
 Bitcoin	BTC	4,290.20	+1.00%	\$3,499,271,946	\$73,509,164,537	17,399,771
 Ripple	XRP	0.380601	-2.78%	\$638,959,132	\$15,181,497,171	40,327,341,704
 Ethereum	ETH	118.3310	-2.55%	\$1,537,827,503	\$12,025,471,826	103,506,012
 Bitcoin-Cash	BCH	185.6160	-3.63%	\$118,213,100	\$3,133,219,002	17,484,327
 Stellar	XLM	0.162818	+1.35%	\$95,450,994	\$3,118,691,926	19,154,499,439
 EOS	EOS	3.040320	-7.71%	\$815,943,697	\$2,689,536,417	906,245,118
 Litecoin	LTC	33.99220	-1.53%	\$401,441,632	\$1,985,208,848	59,361,149

Tabulka 1 Srovnání kapitalizace trhu jednotlivých kryptoměn k 30.11 2018

1.7. Zákonná definice, účtování a vykazování kryptoměn

Situace v ČR

Stanovisko Ministerstva financí ČR a ČNB ke kryptoměnám bylo zpočátku poměrně zdrženlivé a bez uvedení jasného právního rámce. Prvním vyjádřením ČNB z 10. února 2014 byl definován vztah této instituce k bitcoinu a způsob přístupu k této kryptoměně. (přístupovat). Ministerstvo financí definovalo svůj postoj k digitálním měnám (kryptoměnám) a jejich způsobu účtování až 15. května 2018.

Postoj ČNB k bitcoinu

„Data evidovaná v protokolu bitcoin („bitcoin“) nemají charakter pohledávky držitele bitcoinů za jinou osobou, nejsou to tedy bezhotovostní peněžní prostředky ani elektronické peníze (§ 4 ZPS), resp. peněžní prostředky ve smyslu ustanovení § 2 odst. 1 písm. c) ZPS. Nákup či prodej bitcoinů na vlastní účet nepředstavuje žádnou z platebních služeb podle § 3 odst. 1 ZPS ani bezhotovostní obchod s cizí měnou [§ 2 odst. 1 písm. e) ZPS]. Stejně tak nepředstavuje žádnou platební službu ve smyslu ZPS provedení transakce v rámci protokolu bitcoin (např. zaslání

určitého množství bitcoinů jinému uživateli protokolu) ani „vedení účtu v bitcoinech“ (kdy za vlastníka bitcoinů spravuje jeho bitcoiny, typicky v rámci „virtuální peněženky“ na internetové stránce, jiná osoba). V případě směny (resp. nákupu) bitcoinů za české koruny nebo jinou měnu také nejsou splněny znaky směnárenského obchodu, který je definován jako „směna bankovek, mincí nebo šeků znějících na určitou měnu za bankovky, mince nebo šeky znějící na jinou měnu“ (§ 2 odst. 1 ZSČ), tj. není splněn znak hmotné podoby předmětu směny ani znak „znějící na určitou měnu“. bitcoiny nevykazují ani znaky investičního nástroje podle § 3 ZPKT, protože nemají povahu cenného papíru (ani zaknihovaného, mj. v nich není vtěleno žádné právo) ani derivátu. Obchodování s bitcoiny proto nevyžaduje povolení ČNB (takové povolení ČNB ani nemůže udělit) a nepodléhá dohledu ČNB. Z tohoto hlediska se neuplatní ani informační povinnosti vůči ČNB.⁶⁹

Definice digitální měny (kryptoměny) dle Ministerstva financí

„Podle sdělení MF ČR se digitální měnou rozumí digitální nositel hodnoty. Jedná se o nehmotné aktivum, které je elektronicky vytvořeno a uloženo. Digitální měny nejsou vydávány či regulovány centrální bankou ani orgánem veřejné moci a nemají právní status měny. Digitální měny jsou však akceptovány některými fyzickými či právními osobami jako majetek, který je možné převádět, uchovávat, anebo s ním obchodovat.“⁷⁰

Jak účtovat digitální měny

„Ministerstvo financí doporučuje účtovat a vykazovat digitální měny jako zásobu „svého druhu“ ve smyslu § 9 vyhlášky č. 500/2002 Sb., kterou se provádějí některá ustanovení zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, pro účetní jednotky, které jsou podnikateli účtujícími v soustavě podvojného účetnictví (dále „vyhláška“). Pro ocenění digitálních měn se použije § 25 odst. 1 písm. c), d) a l) a odst. 4 a 5 zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů (dále „zákon“). Pro ocenění digitálních měn v okamžiku jejich nabytí se dále použije § 49 vyhlášky a pro ocenění digitálních měn k rozvahovému dni § 55 vyhlášky upravující tvorbu a použití opravných položek. Stejně tak jako

⁶⁹ CNB Stanovisko, [online].[vid. 10.2 2014]. Dostupné z:

https://www.cnb.cz/miranda2/export/sites/www.cnb.cz/cs/faq/stanoviska_a_odpovedi/pdf/obchodovani_s_bitcoiny.pdf

⁷⁰Sdělení Ministerstva financí k účtování a vykazování digitálních měn, [online].[vid. 15.5 2018]. Dostupné z:

<https://www.mfcr.cz/cs/verejny-sektor/ucetnictvi-a-ucetnictvi-statu/ucetnictvi-podnikatelu-a-neziskoveho-sek/aktuality-a-metodicka-podpora/2018/sdeleni-ministerstva-financi-k-uctovani-31864>

na ostatní složky aktiv, vztahuje se i na digitální měny povinnost provést jejich inventarizaci k okamžiku, ke kterému účetní jednotka sestavuje účetní závěrku ve smyslu § 29 zákona. Vzhledem ke specifickému fungování a uložení digitálních měn je nutné dbát na řádně provedenou inventarizaci doloženou zejména dokumentací např. stavu virtuální peněženky. Digitální měny se v rozvaze doporučuje vykázat, v souladu se zvoleným způsobem účtování, na samostatném řádku v rámci položky „C.I.2. Nedokončená výroba“, „C.I.3.1. Výrobky“ nebo „C.I.3.2. Zboží“. Lze využít § 4 odst. 1 vyhlášky a vykázat digitální měnu odděleně o ostatních položek zásob. V příloze v účetní závěrce se uvedou informace o záměru nabytí a držení digitálních měn a způsob jejich ocenění, včetně případné tvorby opravné položky.“⁷¹

Situace v EU

Evropská centrální banka zatím nepředstavila způsob, jakým hodlá regulovat kryptoměny, ale na začátku roku 2018 jasně deklarovala, že regulace v budoucnu je nutností. Řešení pak chce hledat ve spolupráci s Financial Stability Board, který je poradním orgánem pro organizaci nejvyspělejších států G20. Zatím ještě není známo datum návrhu zákonné regulace kryptoměn, nicméně se očekává, že zlomovým bude právě nadcházející rok 2019⁷². První definici virtuálních měn vydal tento poradní orgán v roce 2012, kde právě na příkladu bitcoinu definoval jejich způsob fungování a možná rizika plynoucí z jejich použití⁷³.

1.8. Zhodnocení dopadů a působení kryptoměn na světovou ekonomiku a odvětví retailu

Vliv kryptoměn na celosvětovou ekonomiku je stále poměrně malý. Přestože se v roce 2017 bitcoin díky velmi rychlému růstu kurzu dostal do povědomí veřejnosti, tak využití této technologie čeká na zásadní průlom využití v retailu a e-commerce. Podle zjištění Nizozemské národní banky⁷⁴ je celosvětová akceptace bitcoinu poměrně malá. V oblasti e-commerce se tato úroveň pohybuje okolo pouhých 2 %. U běžných retailerů je akceptace zcela minimální. Přestože koncepčně se bitcoin již osvědčil, tak jeho rozšíření brání především malý zájem ze strany zákazníků. Většina populace považuje kryptoměny a bitcoin především za investiční

⁷¹ Sdělení Ministerstva financí k účtování a vykazování digitálních měn, [online].[vid. 15.5 2018]. Dostupné z: <https://www.mfcr.cz/cs/verejny-sektor/ucetnictvi-a-ucetnictvi-statu/ucetnictvi-podnikatelu-a-neziskoveho-sek/aktuality-a-metodicka-podpora/2018/sdeleni-ministerstva-financi-k-uctovani-31864>

⁷² European Central Bank: Cryptocurrencies Must Be Regulated Within EU, [online].[vid. 26.2 2018]. Dostupné z: <https://www.newsbtc.com/2018/02/26/european-central-bank-rather-than-waiting-for-global-policies-to-be-enacted-cryptocurrencies-must-be-regulated-within-eu/>

⁷³ Virtual Currencies, [online].[vid. 10.10 2012]. Dostupné z: <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>

⁷⁴ What drives bitcoin adoption by retailers?, [online].[vid. 10.2 2018]. Dostupné z: https://www.dnb.nl/binaries/Working%20Paper%20No.%20585_tcm46-373269.pdf

nástroj se závratným potencionálem zhodnocení. V důsledku vývoje, který jsme mohli sledovat v roce 2017, se bitcoin dostal nejen do povědomí laické veřejnosti, ale zaujal i investory z Wall Street. Ti již připravují burzu kryptoměn, která by již měla být plně regulována⁷⁵. To ovšem není zcela dobrá zpráva pro e-commerce a retailery, protože to ve svém důsledku může znamenat větší regulaci kryptoměn a konec jedné z konkurenčních výhod, kterou je decentralizace.

2. Posouzení využitelnosti kryptoměn

Pro posouzení využitelnosti bitcoinu a několika vybraných kryptoměn jsem se rozhodl použít několik základních metod strategické analýzy pro zhodnocení využitelnosti bitcoinu a kryptoměn v retailu/e-commerce. Jen v průběhu psaní této práce ztratil bitcoin šedesát procent své hodnoty, což je pro funkční způsob využití v retailu/e-commerce velmi problematické. A právě vzhledem dlouhodobým a velmi těžko řešitelným problémům s volatilitou je prakticky jedinou možností pro hodnocení využitelnosti přistoupení na využití platebních bran. To na druhou stranu s sebou přináší další bezpečnostní rizika i nutnost platby poplatků za transakce, ovšem se zaručením ochrany proti výkyvům trhu. V první části jsem provedl analýzu poskytovatelů, kde jsem zhodnotil jednotlivé poskytovatele platebních služeb. V další části jsem se zaměřil na analýzu konkurence, kam jsem zahrnul nejen standardní platební běžně dostupné metody, ale i dvě další kryptoměny, a to XRP a BCH. V analýze SWOT jsem zhodnotil silné i slabé stránky spolu s potencionálními příležitostmi a hrozbami. Rozhodl jsem se hlouběji analyzovat především rizika plynoucí zavedením plateb bitcoinem. Na závěr jsem provedl dva nezávislé průzkumy, kdy jsem se rozhodl zkoumat obecné povědomí o kryptoměnách ve společnosti a potenciál, který představují.

Analýza dodavatelů

V první části strategické analýzy se zaměřím na analýzu poskytovatelů. Pro tento účel jsem vybral tři základní řešení od největších poskytovatelů platebních bran na trhu. Hodnotícím kritériem jsou technické podmínky jako je samotná dostupnost služeb, úroveň integrace do softwarových řešení a zabezpečení.

⁷⁵Wall Street'sembracecouldbreak bitcoin
, [online].[vid. 7.9 2018]. Dostupné z: <https://www.technologyreview.com/s/611981/wall-streets-embrace-could-break-bitcoin/>

Analýza konkurence

Dalším bodem strategické analýzy je zhodnocení konkurence. V této části zkoumám přímé konkurenční způsoby plateb, které jsou běžně používány. Zahrnuty jsou nejen standardní bankovní i nebankovní převody, ale i platby kartami nebo konkurenčními kryptoměnami. Z pohledu potencionálního obchodníka, který se rozhodne akceptovat kryptoměny jsou hlavními otázkami rychlost transakcí, zabezpečení, a rovněž míra náročnosti používání jednotlivých řešení. A to nejen z pohledu obchodníka, ale i uživatele.

SWOT

V případě SWOT analýzy využiji jednoduchý a přehledný způsob, jak upozornit na všechny silné i slabé stránky spojené s použitím bitcoinu v e-commerce a retailu.



Rizika

V této části jsem zdůraznil hlavní problémy, které mohou nastat při využívání bitcoinu. Zaměřil jsem se na teoretické problémy, které mohou nastat s ověřováním transakcí jako fork či split blockchainu, double spending (dvojitá útrata) nebo ovládnutí sítě většinou. Z pohledu uživatele, který se rozhodne využívat bitcoin jako platební alternativu, je rovněž nutné řešit rychlost sítě a poplatky z transakcí. Nechybí ani zdůraznění možných komplikací způsobených chováním trhu.

Průzkum

V dotazníkových průzkumech jsem se rozhodl zjistit obecné povědomí náhodného vzorku obyvatel na kryptoměny, jejich zkušenosti a ochotu případně kryptoměny využívat. Analýza dodavatelů

2.1. Analýza dodavatelů

Pro provedení analýzy dodavatelů jsem vybral tři poskytovatele platebních bran pro kryptoměny. V této části zhodnotíme a přímo srovnáme nabízené služby a možnosti integrace do vlastních softwarových řešení.

Poplatky, klíčové vlastnosti a možnosti integrace

Název	Poplatky za transakce	Klíčové vlastnost	Integrace	Nevýhody
Coingate	Fixní sazba 1%	Podporován Point ofSale formou aplikace pro Android a iOS. Podpora více než 40 kryptoměn Ověření účtu do jedné hodiny Možnost přijímání plateb v EUR/USD Podpora 24/7	Plugin e-commerce řešení: WooCommerce, Magento, OpenCart, ZenCart, PrestaShop API včetně dokumentace pro programovací jazyk RUBY a PHP	API nemá dokumentaci pro JAVA, Python a .net
BitPay	Nulová sazba při dodržení podmínek v rámci 30 dní nesmí platby přesáhnout částku 1000 USD za den a 10000 USD za rok. Při překročení sazba 1%. V případě rizikových společností.	Možnost nastavení rychlosti transakcí podle vašich požadavků. Možnost fakturace ve 40+ jazycích 150 měnách Podpora BIP 70 a 73 pro zvýšení zabezpečení. Jednoduchá možnost refundace.	Podpora většiny e-commerce řešení formou plugin. Kompatibilní s POS systémy Ingenico, NCR Silver, DC POS a dalšími Kompatibilní s účetními systémy NetSuite, Paydici, InvoiceNinja a dalšími. Knihovny pro Ruby, Python, C#, Java, Perl, PHP, Go and Elixir, Android SDK, iOS SDK, and Cordova SDK.	Bankovní vklady pouze v 38 zemích: Austrálie, Nový Zéland, USA, UK, Mexico, JAR a země EU (SEPA) Možné další poplatky v případě rizikových společností.

Coinbase Commerce	Zdarma ukládání financí v BTC. 1% za konverzi do lokální měny při překročení prodeje nad 1 000 000 USD	Možnost Instantní konverze pro výplaty Podpora fakturace přes email a mikrotransakcí v BTC	Knihovny pro Ruby, Python, PHP, Node.js, Java, Android SDK a iOS SDK. E-commerce pluginy pro WordPress, WooCommerce, Magento, ZenCart, foxycart!, Spreecommerce.	
-------------------	---	--	--	--

Tabulka 2 - Srovnání možností integrace jednotlivých poskytovatelů platebních bran a poplatky. Zdroj: <https://commerce.coinbase.com>, <https://coingate.com/>, <https://bitpay.com/>.

Denní vyrovnání ve fiat měnách a bitcoinu

Název	Podporované fiat měny	Podporované kryptoměny	Účetní vyrovnání BTC	Rychlost vyrovnání mezi bankami v EUR
Coingate	EUR, USD	BTC, ETH, BCH, LTC, SRN	Denní	1-2 dny (SEPA)
BitPay	AUD, EUR, GBP, MXN, NZD, USD, ZAR	BTC, BCH, GUSD, PAX, USDC	Denní	1-2 dny (SEPA)
Coinbase Commerce	AUD, EUR, SGD, USD, GBP	BTC, BCH, ETH, ETC, LTC, USDC, ZEC, ZRX	Denní	1-2 dny (SEPA)

Tabulka 3 – Srovnání možností jednotlivých platebních bran, co se týče podpory fiat měn a nepoužívanějších kryptoměn. Zároveň jsou zde srovnány časové rámce, ve kterých jsou prováděna účetní vyrovnání.

Zabezpečení

Všichni tři vybraní poskytovatelé nabízejí standardní úroveň zabezpečení s možností dvoufázového⁷⁶ přihlašování, a to buď za pomoci specializované aplikace, typu volně dostupného Google Authenticator⁷⁷ nebo standardní SMS zprávy. V doposud největší hloubkové analýze⁷⁸ zabezpečení kryptoměnových burz a platebních bran bylo zjištěno to, že 54 %⁷⁹ z testovaných služeb má ve svých řešeních bezpečnostní chyby. Ty představují potenciální nebezpečí a možnost zneužití elektronickým útokem.

⁷⁶two-factor authentication (2FA), [online]. [vid. 4.4 2015]. Dostupné z: <https://searchsecurity.techtarget.com/definition/two-factor-authentication>

⁷⁷WhatIs Google Authenticator (and How to Use It), [online]. [vid. 21.4 2018]. Dostupné z: <https://www.tomsguide.com/us/google-authenticator-how-to-use,news-26819.html>

⁷⁸Exchange Security Report, [online]. [vid. 2.10 2018]. <https://icorating.com/report/exchange-security-report/>

⁷⁹54% of Cryptocurrency Exchanges Have Security Hole, [online]. [vid. 2.10 2018]. Dostupné z: <https://news.bitcoin.com/54-of-cryptocurrency-exchanges-have-security-holes/>

Název	Konzolové chyby	Uživatelská bezpečnost	Registr a doména	Zabezpečení webu	Celkové skóre
Coingate	N/A	N/A	N/A	N/A	N/A
BitPay	2/2	3/4	2/5	2/5	47 %
Coinbase Commerce	2/2	4/4	3,5/5	5/5	89 %

Srovnání zabezpečení bohužel není zcela kompletní, protože firma Coingate nebyla součástí auditu. Přesto je vcelku z dokumentu jasné, že Coinbase je v současnosti v oblasti bezpečnosti lídrem. Kompletní analýza i chyby, které byly nalezeny při testování jsou součástí závěrečné zprávy⁸⁰.

Nutné technické prostředky pro provoz

Co se týče technických prostředků pro akceptaci plateb bitcoinem jsou požadavky zcela minimální. Hlavní podmínkou je připojení k internetu, které by v případě retailerů a provozovatelů e-commerce mělo být prakticky samozřejmostí, především pak v důsledku zavedení či zavádění elektronické evidence tržeb, jež připojení rovněž vyžaduje. Samotný proces platby již probíhá v aplikacích dodávaných samotnými poskytovateli platebních bran. Obvykle se realizace platbou provádí s využitím QR kódu a použitím mobilního zařízení se standardní bitcoinovou peněženkou. Všichni tři vybraní poskytovatelé nabízejí vlastní verzi Point of Sale řešení, tedy řešení pro samotného prodejce. Rozdíly mezi jednotlivými řešeními jednotlivých poskytovatelů nejsou zásadní a nepřinášejí pro žádného z nich zásadní konkurenční výhodu.

2.2. Analýza konkurence

Po zvážení všech dostupných informací ohledně poskytovatelů platebních bran a jejich službách jsem zvolil službu Coinbase jako referenční. Pro analytické srovnání jsme vybrali

⁸⁰54% of Cryptocurrency Exchanges Have Security Hole, [online].[vid. 2.10 2018]. ⁸⁰two-factor authentication (2FA), [online].[vid. 4.4 2015]. Dostupné z: <https://searchsecurity.techtarget.com/definition/two-factor-authentication>

⁸⁰WhatIs Google Authenticator (and How to Use It), [online].[vid. 21.4 2018]. Dostupné z: <https://www.tomsguide.com/us/google-authenticator-how-to-use,news-26819.html>

⁸⁰Exchange Security Report, [online].[vid. 2.10 2018].<https://icorating.com/report/exchange-security-report/>

⁸⁰54% of Cryptocurrency Exchanges Have Security Hole, [online].[vid. 2.10 2018]. Dostupné z: <https://news.bitcoin.com/54-of-cryptocurrency-exchanges-have-security-holes/><https://news.bitcoin.com/54-of-cryptocurrency-exchanges-have-security-holes/>

platební konkurenční standardní služby jako je VISA, Paypal a porovnali je s možnostmi kryptoměn BTC, XRP a BCH.

VISA

Platební systém VISA patří jednoznačně k nejvyužívanějším. S celkovým ročním objemem 11 trilionů USD prakticky nemá konkurenci⁸¹, jak je ostatně patrné z tabulky analýzy jednotlivých konkurentů. Podle vyjádření zástupců VISA je infrastruktura této sítě schopna pracovat s maximálním výkonem 24.000 transakčních zpráv za vteřinu (s teoretickou maximální propustností 60000 tps). Reálně je využitý pouze zlomek tohoto výkonu⁸². Velkou konkurenční výhodou je podpora více jak 160 fiat měn a dostupnost služeb prakticky po celém světě⁸³. Konkurenční výhodou je rovněž uživatelsky velmi jednoduchá obslužnost zvláště při využití RFID⁸⁴ bezdrátových technologií, ať už ve formě platebních karet nebo s využitím mobilních zařízení (v ČR zatím pouze Google Pay⁸⁵).

PayPal

Platební systém, který jako jeden z prvních nabídl uživatelům možnost instantních plateb v rámci sítě PayPal bez ohledu na geografickou lokaci. V roce dosáhl objem realizovaných plateb hodnoty 451 miliard USD a připsal meziroční přírůstek 27 %⁸⁶. Hlavní výhodou platebního systému Paypal je rychlost transakcí, která jsou instantní platby a vysoká míra využití v e-commerce. Maximální propustnost sítě Paypal je ve srovnání s sítí VISA i XRP poměrně nízká a to 193 transakčních zpráv za vteřinu. Nevýhodou jsou rovněž poměrně vysoké poplatky, které jsou často přenášeny na zákazníka.

XRP

XRP, tedy Ripple byl od počátku koncipován jako nástroj, který by měl být přímou konkurencí zavedeným technologiím jako je VISA či Paypal. Teoreticky dokáže síť Ripple díky svému unikátnímu způsobu schvalování transakcí nabídnout prakticky stejnou rychlost jako síť VISA

⁸¹ Payments statistics for 2016, [online].[vid. 2.10 2018]. Dostupné z: <https://www.ecb.europa.eu/press/pdf/pis/pis2016.pdf?be9989f6bd72483ebe27d8dfae1f0362>

⁸²bitcoin and Ethereum vs Visa and PayPal, [online].[vid. 22.4 2017]. Dostupné z: <https://altcointoday.com/bitcoin-ethereum-vs-visa-paypal-transactions-per-second/>

⁸³What is VISA, [online].[vid. 30.6 2017]. Dostupné z: <https://usa.visa.com/dam/VCOM/download/corporate/media/visanet-technology/aboutvisafactsheet.pdf>

⁸⁴ Co je RFID, [online].[vid. 30.6 2017]. Dostupné z: https://www.rfidportal.cz/index.php?page=rfid_obecne

⁸⁵Co je Google Pay?, [online].[vid. 30.9 2018]. Dostupné z: <https://support.google.com/pay/answer/9026749?co=GENIE.Platform%3DDesktop&hl=cs>

⁸⁶PayPal's annual payment volume from 2012 to 2017, [online].[vid. 30.9 2018]. Dostupné z: <https://www.statista.com/statistics/419783/paypals-annual-payment-volume/>

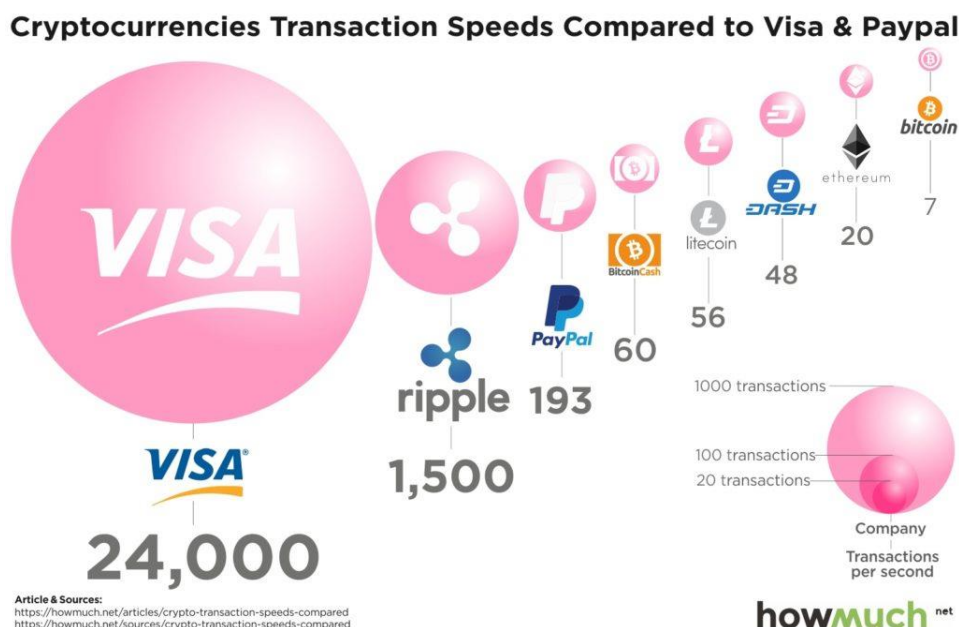
byť v současné době zdaleka nevyužívá svůj maximální potenciál. Výhodou je velmi dobrá škálovatelnost výkonu řešení XRP.

bitcoin Cash

Bitcoin Cash vznikl jako reakce na technické omezení bitcoinu, kdy především díky větší velikosti bloku (8 MB), do kterého jsou ukládány transakce nabízí násobně vyšší výkon než BTC. Součástí původní ideje bylo pravidelně provádět vylepšení protokolů i koncepce bitcoin Cash k čemuž mají posloužit pravidelné dělení sítě (fork). Bohužel v poslední době i přes růst kurzu je komunita okolo BCH názorově rozdělena ohledně budoucnosti a směřování vývoje této kryptoměny. To se pochopitelně negativně projevuje především na výkonu celé sítě.

Srovnání výkonu jednotlivých sítí

Jak je patrné z níže uvedeného srovnání, tak síť bitcoinu je v důsledku technologickým limitům značně omezena. I přesto, že uvedená rychlost 7 tps je při standardní zátěži stále využitelná, tak do budoucnosti představuje zásadní problém pro škálovatelnost výkonu. Východiskem bylo změnění velikosti jednoho bloku ze současného limitu 1 MB, což si uvědomili i tvůrci Bitcoin Cash, který vznikl hard forkem (tvrdým rozdělením) právě z bitcoinu. Ani nově vzniklá kryptoměna Bitcoin Cash však nedokáže výkonnostně konkurovat XRP, které ze všech mainstreamových kryptoměn nabízí největší potenciál.

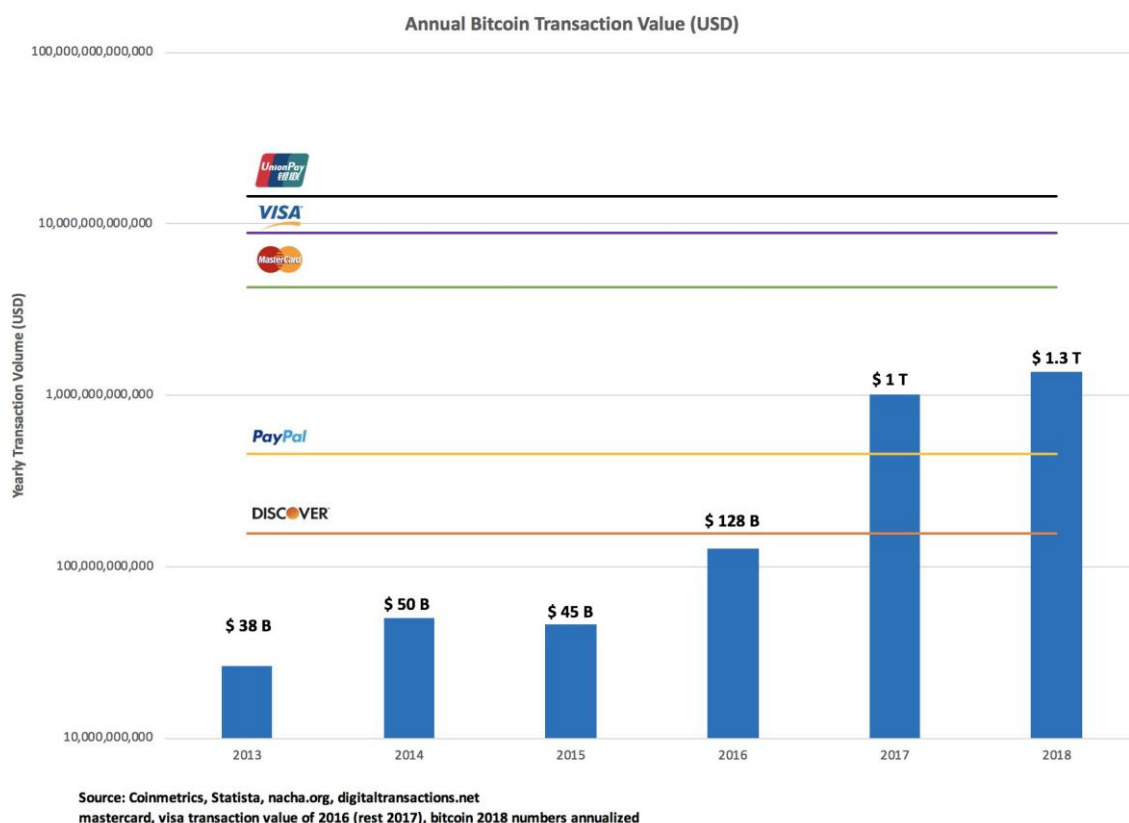


Obrázek 7- Srovnání reálné propustnosti jednotlivých transakčních sítí⁸⁷

⁸⁷ Cryptocurrency speed compared [online].[vid. 30.9 2018]. Dostupné z: <https://howmuch.net/articles/crypto-transactions-speeds-compared>

Srovnání meziročního objemu transakcí

Jedním z hlavních argumentů zastánců bitcoinu je transakční objem, který dramaticky meziročně narostl. Jak je patrné z grafu, tak v minulém roce dosáhl hodnoty jednoho triliónu USD, čímž překonal obchodovaný objem PayPal. Je nutné zmínit i fakt, že většina transakcí proběhla čistě v rámci spekulativního jednání uživatelů skrze burzy a směnárny. Nelze tedy z této hodnoty odvozovat nárůst využití bitcoinu pro platby v retailu a e-commerce. Pozitivně lze hodnotit fakt, že nárůst objemu pokračoval i přes to, že směnný kurz BTC ku USD byly poměrně stabilní.



Tabulka 4 Meziroční růst objemu transakcí v USD⁸⁸

Srovnání poplatků obchodníků v jednotlivých sítích

Ve srovnání nákladů vychází jako nejvýhodnější příjem plateb VISA, což je důsledek regulace Evropského parlamentu z roku 2015. U BTC se poplatek pohybuje v rozmezí 0-1% v závislosti na platební bráně a obchodovaném objemu.

⁸⁸ Cryptocurrency speed compared [online].[vid. 30.9 2018]. Dostupné z: <https://howmuch.net/articles/crypto-transactions-speeds-compared>

Paypal		Visa		Coinbase (BTC)	
0.00 CZK - 70,000.00 CZK	3.4% + 10.00 CZK	Flat rate	0,2-0,3%	Flat rate	1%
70,000.01 CZK - 280,000.00 CZK	2.9% + 10.00 CZK				
280,000.01 CZK - 1,500,000.00 CZK	2.7% + 10.00 CZK				
1,500,000.01 CZK - 3,000,000.00 CZK	2.4% + 10.00 CZK				
> 3,000,000.00 CZK	1.9% + 10.00 CZK				

Tabulka 5 - Srovnání výše poplatků PayPal, VISA a Coinbase

2.3. Rizika

V této části jsem se zaměřil jak na možná rizika plynoucí z používání bitcoinu v retailu a e-commerce, tak i na rizika plynoucí ze samotné koncepce této kryptoměny. Technologická část je zaměřená na problémy, které mohou teoreticky nastat vzhledem k principům a pevně stanoveným pravidlům bitcoinu. Rizika plynoucí z chování trhu a státu se pak zaměřují na možné problémy, které mohou reálně nastat a nejsou uživatelem ovlivnitelné.

Útok 51% většinou a dvojitá útrata

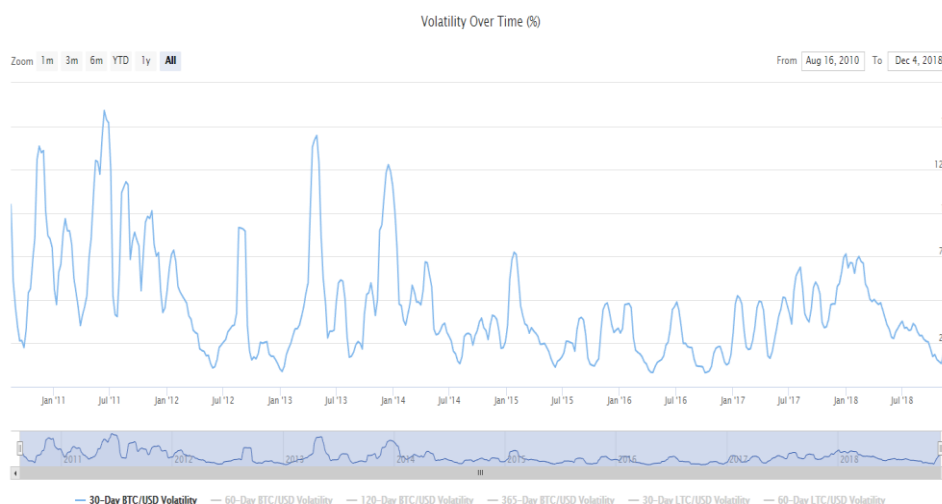
Celý princip ověřování transakcí v síti bitcoin je založen na presumpci většinové pravdy, v důsledku čehož je teoreticky možné provést útok 51 % většinou. K tomu, aby takový útok byl úspěšný by musel útočník mít pod svou kontrolou 51 % výkonu celé decentralizované sítě. V tu chvíli by mohl (útočník) libovolně rozhodovat o validitě transakcí. Mohl by tak teoreticky rozhodnout, že je možné jeden bitcoin použít ve více než jedné transakci a tím vytvořit dvojitou útratu. V rámci sítě bitcoin je možné přijmout rovněž i neověřenou platbu, kdy uživatel nečeká na potvrzení a ověření. To se týká především situace, kdy je nutné akceptovat platbu bez odkladu, což může být i případ retailu. V tomto případě hrozí, že plátce může situaci zneužít a provést platbu stejnou mincí při více transakcích. Tento jev není specifikem bitcoinu, ale týká se většiny forem úhrady, kde je nutné provést ověřování, které nefunguje instantně. To ostatně platí rovněž u platebních karet typu VISA⁸⁹. V případě podobného podvodu v rámci sítě bitcoin je pravděpodobnost úspěchu velmi malá, protože útočník by musel disponovat značnými prostředky, aby celý útok úspěšně provedl. Obtížnost roste s počtem uzlů, ke kterým je prodejce při inicializaci platby připojen. Důležité je ale upozornit rovněž na to, že ani při jednom typu

⁸⁹Debitcardglitchmeansthousandschargedtwice, [online].[vid. 5.9 2018].<https://www.bbc.com/news/uk-england-45400234>

útočnicka není možné jakýmkoliv způsobem získat přístup k peněženkám ostatních uživatelů a jejich uloženým prostředkům.⁹⁰

Volatilita

Největším současným problémem bitcoinu je velmi vysoká volatilita způsobující nekontrolovatelné výkyvy v kurzech, které nelze jednoduchým způsobem eliminovat. Z tohoto důvodu je dnes nemožné akceptovat bitcoin bez využití prostředníka v podobě platební brány. Dalším důsledkem volatility je rovněž nerovnoměrné zatížení sítě, kdy se při extrémních výkyvech znatelně zpomaluje rychlost transakcí a zvyšuje jejich cena v rámci sítě bitcoin. Je rovněž otázkou, jakým způsobem se další případný propad v hodnotě bitcoinu promítne na výpočetní výkon sítě, kdy už nebude těžení dostatečně rentabilní, a to i s přihlédnutím k rostoucím cenám energií.



Graf 6 Volatilita trhu bitcoin v čase⁹¹

Zprostředkovatelé

služeb

Pokud pomineme volatilitu, pak největším aktuálním rizikem jsou prostředníci směň z BTC na fiat měny spolu se směnárny/burzami. Jestliže je dnes možné o konceptu blockchainu tvrdit, že je skutečně prověřenou a bezpečnou technologií, pak právě prostředníci jsou z perspektivy útočníka tím nejlákavějším a nejzranitelnějším cílem. Jak jsme se již zmínili v kapitole *Analýza*

⁹⁰Blockchain: how a 51% attack works (double spend attack), [online].[vid. 5.10 2018].<https://medium.com/coinmonks/what-is-a-51-attack-or-double-spend-attack-aa108db63474>

⁹¹ Volatilita v čase, [vlastní].[vid. 5.12 2018]. <https://bitvol.info/>

dodavatelů, tak zabezpečení provozovatelů směnárny i platebních bran není dostatečné. Útoky na tyto prostředníky způsobily největší majetkové škody a zároveň byly i důvodem proč byly bitcoiny, co se týče bezpečnosti, zpochybňovány. Pokud se podíváme do historie bitcoinu, tak prakticky není rok, kdy by tímto způsobem nebyl poškozen některý z velkých poskytovatelů služeb⁹².

Právní ukotvení

V části této práce jsem se věnoval rovněž přístupu Ministerstva financí a ČNB v otázce případné regulace i způsobu, jak kryptoměny správně účtovat. Přestože je tento problém již v dnešní době řešen prakticky na všech úrovních⁹³, tak stále neplatí žádná jednoznačná právní definice ani regulace. Právě případná regulace nebo dokonce odmítnutí bitcoinu či kryptoměn obecně může způsobit znatelný pokles využitelnosti těchto řešení.

Nízký zájem veřejnosti

Technologie, kterou využívá většina kryptoměn, tedy blockchain, již dokázal oslovit nejen technologické nadšence, ale i profesionály v oboru bankovníctví a půjček⁹⁴. Co se týče bitcoinu samotného, tak ten se díky překotnému vývoji kurzu rovněž dostal do podvědomí široké veřejnosti. Nicméně drtivá většina zpráv bitcoin spojuje pouze s investiční příležitostí, bez hlubšího zkoumání výhod decentralizované sítě a jejího možného využití. Obecně nelze pozorovat výrazný nárůst poptávky po platbách v BTC a ani v jiných konkurenčních kryptoměnách, což může mít za následek zpomalení vývoje.

⁹²Here you will find a documented list of cryptocurrency exchange hacks, [online]. [vid. 27.4 2018].

<https://rados.io/list-of-documented-exchange-hacks/>

⁹³Communiqué G20 bod 9, [online]. [vid. 20.3 2018]. https://back-g20.argentina.gob.ar/sites/default/files/media/communique_g20.pdf

⁹⁴Online lenders showing interest in blockchain technology, [online]. [vid. 12.4 2018]. <https://www.finder.com/online-lenders-showing-interest-in-blockchain-technology>

2.4. SWOT

Ve SWOT strategické analýze bitcoinu jsem se rozhodl porovnat silné a slabé stránky spolu s příležitostmi a hrozbami. To vše z pohledu obchodníka v retailu a e-commerce, jenž by uvažoval o zavedení plateb Bitcoinem.

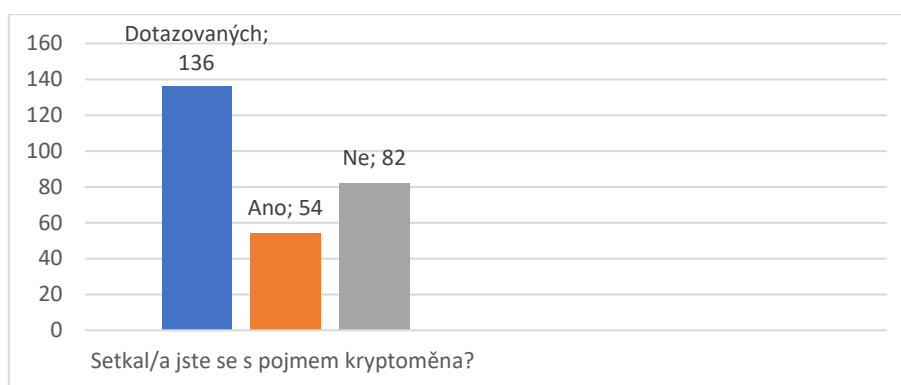
	Pozitivní		Negativní/Škodlivé	
	Silné stránky		Slabé stránky	
INTERNÍ	STRENGTHS		WEAKNESSES	
	1	Decentralizovaný koncept	1	Volatilita
	2	Nízké poplatky	2	Nelze platit všude
	3	Jednoduchá integrace platebních služeb	3	Pomalejší transakce
	4	Minimální vstupní náklady	4	Třetí strany vstupující do procesu konverze z fiat měn
	5	Neměnná historie blockchain	5	Omezení velikosti bloku 1 MB
	6		6	Právní ukotvení
EXTERNÍ	Příležitosti		Hrozby	
	OPPORTUNITIES		THREATS	
	1	Široké možnosti aplikace blockchain technologie	1	Ceny energií mohou ovlivnit činnost při těžení a tím i rychlost transakcí
	2	V případě rozpadu měnových unií	2	Hackerské útoky na řešení třetích stran
	3	Nahrazení služeb typu Paypal	3	Legislativní změny
	4	Hlubší integrace se současnými bankovními řešeními	4	Deflace měny, která může nastat spolu se snižováním dostupnosti BTC

2.5. Dotazování

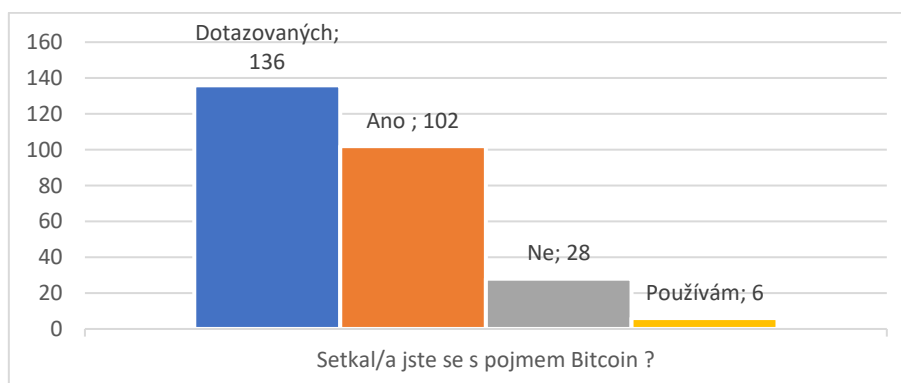
Část první: Povědomí a zkušeností s kryptoměnami běžných uživatelů

Jako další metodu kvantitativního výzkumu jsem se rozhodl provést průzkum dotazováním⁹⁵. Cílem bylo zjistit obecné znalosti kryptoměn a bitcoinu u laické veřejnosti v ČR. Jako metodu dotazování jsem zvolil internetové (online) dotazování. Průzkumu se účastnilo celkem 136 náhodně vybraných osob s věkovým průměrem 42 let.⁹⁶

Výsledky dotazování



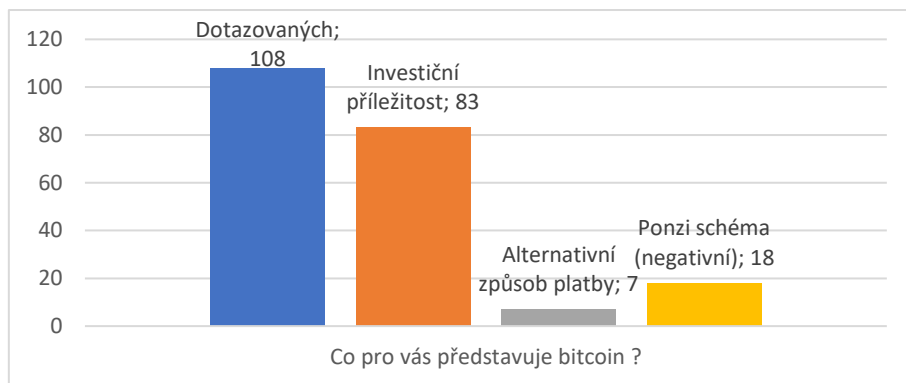
Otázka z obecnou znalostí termínu kryptoměna. Jasně ukazuje, že mediální obraz kryptoměn do značné míry představuje bitcoin o kterém měli dotazovaní větší povědomí.



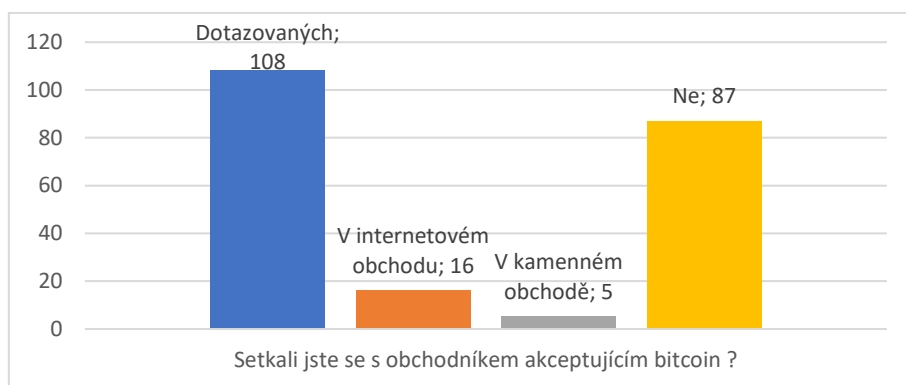
Další otázka je již spojena přímo se znalostí bitcoinu. Z dotazovaných používá bitcoin pouze 4,5 % a povědomí o této kryptoměně má 75 % tázaných. V případě negativní odpovědi už byl dotazník pro dotazovaného ukončen.

⁹⁵ HENDL, Jan. Kvalitativní výzkum: základní teorie, metody a aplikace. 3. vyd. Praha: Portál, 2012. ISBN 978-80-262-0219-6.

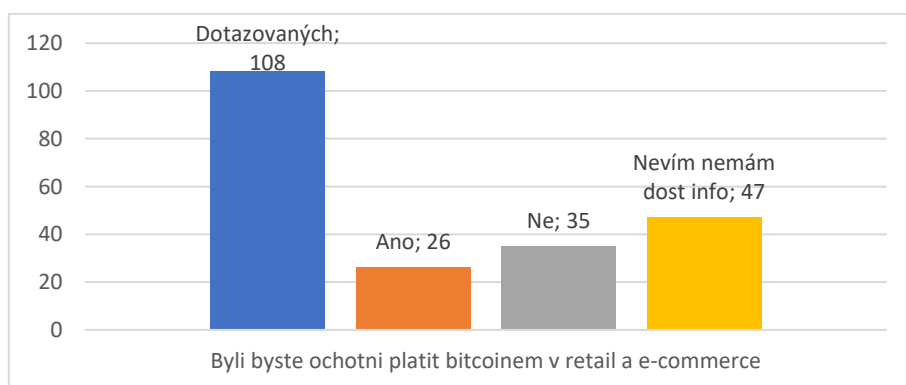
⁹⁶



Cílem třetí otázky je zjistit, co pro dotazované představuje bitcoin. Poměrně překvapivé je vysoké procento (16,6 %) dotazovaných, kteří vnímají bitcoin negativně. Jen malý zlomek (6,4 %) uživatelů pak uvažuje o bitcoinu, co by alternativním způsobu plateb.



Čtvrtá otázka je již přímo spojena s retail a e-commerce. Z celkového počtu dotazovaných pouze 19,4 % se setkala s prodejními místy akceptujícími bitcoin. Z čehož 76,1 % představuje e-commerce.



Poslední otázka je spojena s ochotou dotazovaných bitcoin využívat k platbě v retailu a e-commerce. Ochotných okamžitě využívat plateb bitcoinem je pouze 24 % a 43,5 % dotázaných konstatovalo, že nemá dostatečné informace pro takové rozhodnutí.

Závěr:

Hlavním účelem této práce bylo zhodnocení využitelnosti bitcoinu/kryptoměn v oblasti retailu a e-commerce. Především pak bylo cílem nabídnout (možnost) přímé srovnání možností, které nabízí bitcoin a okrajově ostatní kryptoměny v porovnání s běžně používanými způsoby plateb. V úvodu jsem nastínil způsob, jakým funguje proces decentralizované sítě bitcoinu a které kroky jsou nutné pro ověření transakcí. Zároveň jsem popsal fungování základních prvků bitcoinu, které je nutné pro pochopení a další využívání této kryptoměny. V dalších kapitolách jsem se věnoval tomu, jakým způsobem bitcoin vůbec vznikl a také jeho pestré, byť krátké historii. Nedílnou součástí, která vyplynula z potřeby konverze bitcoinu na fiat měny, byl vznik směnárny a burz. Zmínil jsem následně rizika plynoucí z využívání těchto služeb. Z pohledu případného zájemce o integraci plateb do retailu a e-commerce je představení platebních bran, které do určité míry eliminují značný problém volatility kurzu. V krátkosti jsem rovněž představil několik vybraných alternativních kryptoměn, které sice v mnohém navazují na bitcoin, ale vývojově již představují novou generaci s novými možnostmi. Další nezbytnou kapitolou je zákonná definice bitcoinu a kryptoměn z pohledu státu. Provedl jsem srovnání několika poskytovatelů platebních bran, které jsou pro jednoduché využití v retailu či e-commerce nezbytné. V následující kapitole jsem již srovnal možnosti bitcoinu s možnostmi běžně využívaných platebních prostředků. Možnosti bitcoinu jsem rovněž zhodnotil z pohledu možných rizik, které mohou ohrozit využitelnost této kryptoměny. V poslední části jsem provedl krátký průzkum ohledně obecných znalostí náhodně vybraných uživatelů prostřednictvím internetového dotazování.

Bitcoin je v současné podobě, a to i díky velmi sofistikovaným řešením platebních bran možné nasadit do prostředí e-commerce i retailu během velmi krátké doby. Rychlou adaptaci brzdí především poměrně malý zájem veřejnosti o využívání bitcoinu k běžným platbám. Rovněž potencionálním problémem může být poměrně špatná výkonová škálovatelnost konceptu bitcoinu. Zde vidím riziko výrazného snížení zpracování platebních transakcí při masivnějším rozšíření bitcoinu, a to v důsledku technických omezení současného řešení. V tomto ohledu většina alternativních kryptoměn nabízí výrazně pružnější řešení. Bitcoin momentálně nenabízí z pohledu provozovatele retail či e-commerce skutečnou konkurenční výhodu při srovnání běžně využívanými platebními službami a jeho využitelnost je diskutabilní.

Seznam zdrojů

Seznam použité literatury

Antonopoulos, Andreas, Masteringbitcoin: Unlocking Digital Cryptocurrencies.
USA: O'Reilly Media, Inc, 2017. 398 s. ISBN 9781491954386

Swan, Melanie, Blockchain: Blueprintfor a New Economy,
USA: O'Reilly Media, Inc, 2015. 152 s. ISBN 9781491920497

Raval, Siraj, DecentralizedApplications
USA: O'Reilly Media, Inc, 2015. 150 s. ISBN 9781491924549

Václav, Matyáš, Jan, Krhovják a kolektiv, Autorizace elektronických transakcí a autorizace dat i uživatelů. ČR:
Masarykova univerzita, 2008. 128 s. ISBN 9788021045569

Řezanková, H.: Analýza dat z dotazníkových šetření. 4. doplněné vydání.
ČR: ProfessionalPublishing, Praha, 228 s. ISBN 978-80-906594-8-3.

Arvind, Narayanan. Blockchains: Past, Present, and Future. Houston (USA), 2018: SIGCSE

'18, 2018. ISBN: 978-1-4503-4706-8.

Stefan, Dziembowski. Introduction to Cryptocurrencies. Houston (USA), 2015: CCS '15 Proceedings of the 22nd
ACM SIGSAC Conference on Computer and Communications Security, 2015. 978-1-4503-3832-5.

Debasis, Bhattacharya. Bitcoins, Blockchains and Cybersecurity. Baltimore, Maryland, (USA), 2018: SIGCSE
'18, 2018. ISBN: 978-1-4503-5103-4.

Alexandra, Dmitrenko. Secure Wallet-Assisted Offline Bitcoin Payments with Double-Spender Revocation. bu
Dhabi, (Spojené Arabské Emiráty), 2017: ASIA CCS '17 Proceedings of the 2017 ACM on Asia Conference on
Computer and Communications Security, 2017, ISBN: 978-1-4503-4944-4

HENDL, Jan. Kvalitativní výzkum: základní teorie, metody a aplikace. 3. vyd. Praha: Portál, 2012. ISBN 978-
80-262-0219-6.

Seznam online článků

TREVOR I. KIVIAT.: REGULATING BLOCKCHAIN TRANSACTIONS. [online]. [vid. 30. 11 2018].
Dostupné z: <https://dlj.law.duke.edu/article/beyond-bitcoin-kiviat-vol65-iss3/>

CryptocurrencyDefinition | Oxforddictionaries [online]. [vid. 1. listopad 2018]. Dostupné z:
<https://en.oxforddictionaries.com/definition/cryptocurrency>

What is cryptocurrency [online]. [vid. 14. srpen 2018]. Dostupné z:
<https://www.thestreet.com/investing/bitcoin/what-is-cryptocurrency-14679467>

How bitcoin works [online]. [vid. 11. únor 2018]. Dostupné z:
<https://steemit.com/cryptocurrency/@jonvickers/how-bitcoin-works>

Genesis Block[online]. [vid. 16. duben 2015]. Dostupné z:
<https://www.investopedia.com/terms/g/genesis-block.asp>

Blockchain size [online]. [vid. 18. červen 2018]. Dostupné z:

<https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/>

Blockchain[online]. [vid. 18. červen 2018].Dostupné z:

https://i.investopedia.com/image/png/1542048203442/screen_shot_20181112_at_1.43.06_pm.png

Choose your Bitcoin wallet [online]. [vid. 7. prosince 2018]. Dostupné z:

<https://bitcoin.org/en/choose-your-wallet>

bitcoinWallet[online]. [vid. 16. března 2018]. Dostupné z:

<https://bitcoinwallet.com/>

bitcoinAdress[online]. [vid. 29. leden 2018]. Dostupné z:

<https://www.coindesk.com/information/how-do-bitcoin-transactions-work>

bitcoinMining: A CloserLookUnderthe Hood[online]. [vid. 12. duben 2017]. Dostupné z:

<https://news.bitcoin.com/bitcoin-mining-closer-look-hood/>

Bitcoin Emission: How Many Coins We Have, How Many Are to Come And Why Is It So [online]. [vid. 31. květen 2018]. Dostupné z:

<https://thecoinshark.net/bitcoin-emission-how-many-coins-we-have-how-many-are-to-come-and-why-is-it-so/>

Nearly 4 Million Bitcoins Lost Forever [online]. [vid. 25. listopad 2017]. Dostupné z:

<http://fortune.com/2017/11/25/lost-bitcoins/>

Bitcoin Private Keys: Everything You Need To Know [online]. [vid. 15. září 2018].

Dostupné z: <https://coinsutra.com/bitcoin-private-key/>

Hašovací funkce [online]. [vid. 29. listopad 2017]. Dostupné z:

http://crypto-world.info/klima/2005/cryptofest_2005.htm

Jak těžké je uhodnout hodnotu hashe SHA-256? [online]. [vid. 28. července 2017]. Dostupné z:

<https://www.root.cz/zpravicky/jak-tezke-je-uhodnout-hodnotu-hashe-sha-256/>

bitcoinMining: A CloserLookUnderthe Hood[online]. [vid. 12. duben 2017]. Dostupné z:

<https://news.bitcoin.com/bitcoin-mining-closer-look-hood/>

Bitcoin Emission: How Many Coins We Have, How Many Are to Come And Why Is It So [online]. [vid. 31. květen 2018]. Dostupné z:

<https://thecoinshark.net/bitcoin-emission-how-many-coins-we-have-how-many-are-to-come-and-why-is-it-so/>

Nearly 4 Million Bitcoins Lost Forever [online]. [vid. 25. listopad 2017]. Dostupné z:

<http://fortune.com/2017/11/25/lost-bitcoins/>

Everything you need know about mining[online]. [vid. 20. listopad 2018]. Dostupné z:

<https://www.bitcoinmining.com/>

Application-Specific Integrated Circuit [online]. [vid. 31. března 2018]. Dostupné z:

<https://www.techopedia.com/definition/2357/application-specific-integrated-circuit-asic>

bitcoinDifficulty Chart and Graph.[online]. [vid. 31. březen 2018]. Dostupné z:

<https://www.coinwarz.com/difficulty-charts/bitcoin-difficulty-chart>

Bitcoin's energy usage is huge – we can't afford to ignore it. [online]. [vid. 17. leden 2018].

Dostupné z: <https://www.theguardian.com/technology/2018/jan/17/bitcoin-electricity-usage-huge-climate-cryptocurrency>

Spotřeba elektřiny v Česku stoupla na nový rekord. [online]. [vid. 24. květen 2018]. Dostupné z:

<https://zpravy.aktualne.cz/ekonomika/spotreba-elektřiny-v-cr-loni-vzrostla-na-rekordnich-73-8-twh/r~688d7a705f3011e8bddd0cc47ab5f122/>

bitcoinEnergyConsumption Index. [online]. [vid. 31. březen 2018]. Dostupné z:

<https://digiconomist.net/bitcoin-energy-consumption>

Bitcoin Block Reward Halving Countdown. [vid. 7. prosinec 2018].Dostupné z:

<https://www.bitcoinblockhalf.com/>

BitNodes[online]. [vid. 27. listopad 2018]. Dostupné z:

<https://bitnodes.earn.com/>

Bitcoin History: Timeline, Origins and Founder.[online]. [vid. 17. srpen 2018]. Dostupné z:

<https://www.thestreet.com/investing/bitcoin/bitcoin-history-14686578>

What Is Bit Gold? The Brainchild of Blockchain Pioneer Nick Szabo.[online]. [vid. 22. květen 2018]. Dostupné z:

<https://coincentral.com/what-is-bit-gold-the-brainchild-of-blockchain-pioneer-nick-szabo/>

Bitcoin's Quirky Genesis Block Turns Eight Years Old [online]. [vid. 3. leden 2018]. Dostupné z:

<https://news.bitcoin.com/bitcoins-quirky-genesis-block-turns-eight-years-old-today/>

bitcoin foundation[online]. [vid. 10. listopad 2018]. Dostupné z:

<https://bitcoinfoundation.org/>

bitcoin foundation[online]. [vid. 10. listopad 2018]. Dostupné z:

<https://bitcoinfoundation.org/>

WhatisthebitcoinFoundation, and WhatDoesit Do? [online]. [vid. 18. duben 2018]. Dostupné z:

<https://www.investopedia.com/tech/what-bitcoin-foundation-and-what-does-it-do/>

WikiLeaks Asks For Anonymous Bitcoin Donations [online]. [vid. 14. červen 2011].

Dostupné z: <https://www.forbes.com/sites/andyygreenberg/2011/06/14/wikileaks-asks-for-anonymous-bitcoin-donations/#c38dc144f73b>

Whatis bitcoin[online]. [vid. 10. listopad 2012]. Dostupné z:

<https://www.weusecoins.com/>

BitPay Exceeds 1,000 Merchants Accepting Bitcoin [online]. [vid. 11. září 2012]. Dostupné z:

<https://www.businesswire.com/news/home/20120911005855/en/BitPay-Exceeds-1000-Merchants-Accepting-Bitcoin>

Thailand bans Bitcoin [online]. [vid. 30. července 2013]. Dostupné z:

<https://www.ft.com/content/c08a26df-537c-3bd1-a10b-734050003839>

The History of Silk Road: A Tale of Drugs, Extortion & Bitcoin [online]. [vid. 20. listopadu 2018]. Dostupné z:

<https://blockonomi.com/history-of-silk-road/>

THE INSIDE STORY OF MT. GOX, BITCOIN'S \$460 MILLION DISASTER [online]. [vid. 3. březen 2014]. Dostupné z:

<https://www.wired.com/2014/03/bitcoin-exchange/>

All Bitfinex clients to share 36% loss of assets following exchange hack [online]. [vid. 7. květen 2016]. Dostupné z:

<https://www.theguardian.com/technology/2016/aug/07/bitfinex-exchange-customers-receive-36-percent-loss-tokens/>

Bitcoin's Hashrate Crosses exahash.[online]. [vid. 7. květen 2016]. Dostupné z:

<https://news.bitcoin.com/bitcoin-hashrate-four-exahash-per-second/>

Bitcoin's Roller-coaster Ride May Get Wilder. [online]. [vid. 23. prosinec 2017]. Dostupné z:

<https://www.voanews.com/a/bitcoin-wild-ride/4176331.html>

Legality of bitcoin by country or territory [online]. [vid. 7. prosinec 2018]. Dostupné z:

https://en.wikipedia.org/wiki/Legality_of_bitcoin_by_country_or_territory

Kypr je pátou zemí eurozóny, která kvůli krizi žádá o finanční pomoc. [online]. [vid. 25. červen 2012]. Dostupné z:

<https://domaci.ihned.cz/c1-56296040-kypr-je-patou-zemi-eurozony-ktera-kvuli-krizi-zada-o-financni-pomoc>

CHINA OFFICIALLY BANS ALL CRYPTO-RELATED COMMERCIAL ACTIVITIES [online]. [vid. 22. květen 2018] Dostupné z:

<https://bitcoinist.com/china-officially-bans-crypto-activities/>

THE INSIDE STORY OF MT. GOX, BITCOIN'S \$460 MILLION DISASTER [online]. [vid. 3. březen 2014]. Dostupné z:

<https://www.wired.com/2014/03/bitcoin-exchange/>

bitcoincharts[online]. [vid. 23. listopad 2018]. Dostupné z: <https://bitcoincharts.com/>

Zájem o výraz bitcoin, [vlastní] ..[vid 7. duben 2018]. Dostupné z: <https://trends.google.com/trends/?geo=US>

Hereyouwillfind a documented list ofcryptocurrencyexchange hacks, [online].[vid. 27.4 2018].

<https://rados.io/list-of-documented-exchange-hacks/>

Details of \$5 Million Bitstamp Hack Revealed [online].[vid 7. duben 2015]. Dostupné z:

<https://www.coindesk.com/unconfirmed-report-5-million-bitstamp-bitcoin-exchange>

Bitstamp.[online]. [vid. 23. listopad 2018]. Dostupné z:

<https://www.bitstamp.net/>

BitLicenseRegulatoryFramework.[online]. [vid. 23. 7 2013]. Dostupné z:

https://www.dfs.ny.gov/legal/regulations/bitlicense_reg_framework.htm

Coinbase.[online]. [vid. 23. listopad 2018]. Dostupné z:

<https://www.coinbase.com/>

BitLicenseRegulatoryFramework.[online]. [vid. 23. 7 2013]. Dostupné z:

https://www.dfs.ny.gov/legal/regulations/bitlicense_reg_framework.htm

Kraken.[online][vid. 23. 1 2018]. Dostupné z:

<https://www.kraken.com/>

Binance.[online]. [vid. 23. 1 2018]. Dostupné z:

<https://www.binance.com/en>

Coinbase Commerce.[online]. [vid. 28. 1 2018]. Dostupné z:

<https://commerce.coinbase.com/>

Bitpay payment protocol.[vid. 3. 12 2018]. Dostupné z

<https://support.bitpay.com/hc/en-us/articles/360015839672-Frequently-Asked-Questions-About-BitPay-and-Payment-Protocol-BIP70->

Bitpay .[online]. [vid. 23. 1 2018]. Dostupné z:

<https://bitpay.com/>

Point of Sale.[online]. [vid. 23. 1 2018]. Dostupné z:

<https://coingate.com/bitcoin-pos>

Coingate .[online]. [vid. 23. 1 2018]. Dostupné z:

<https://coingate.com/>

Ripple, [online].[vid. 30. 11 2018]. Dostupné z:

<https://www.investopedia.com/terms/r/ripple-cryptocurrency.asp>

How Do Ethereum Smart Contracts Work? [online].[vid. 30. 11 2018]. Dostupné z:

<https://www.coindesk.com/information/ethereum-smart-contracts-work>

Ethereum, [online].[vid. 30. 11 2018]. Dostupné z:

<https://www.ethereum.org/>

bitcoin Cash, [online].[vid. 30. 11 2018].

Dostupné z: <https://www.bitcoincash.org/>

CNB Stanovisko, [online].[vid. 10.2 2014]. Dostupné z:

https://www.cnb.cz/miranda2/export/sites/www.cnb.cz/cs/faq/stanoviska_a_odpovedi/pdf/obchodovani_s_bitcoiny.pdf

Sdělení Ministerstva financí k účtování a vykazování digitálních měn, [online].[vid. 15.5 2018]. Dostupné z:

<https://www.mfcr.cz/cs/verejny-sektor/ucetnictvi-a-ucetnictvi-statu/ucetnictvi-podnikatelu-a-neziskoveho-sek/aktuality-a-metodicka-podpora/2018/sdeleni-ministerstva-financi-k-uctovani-31864>

Sdělení Ministerstva financí k účtování a vykazování digitálních měn, [online].[vid. 15.5 2018]. Dostupné z:

<https://www.mfcr.cz/cs/verejny-sektor/ucetnictvi-a-ucetnictvi-statu/ucetnictvi-podnikatelu-a-neziskoveho-sek/aktuality-a-metodicka-podpora/2018/sdeleni-ministerstva-financi-k-uctovani-31864>

European Central Bank: Cryptocurrencies Must Be Regulated Within EU, [online].[vid. 26.2 2018]. Dostupné z:

<https://www.newsbtc.com/2018/02/26/european-central-bank-rather-than-waiting-for-global-policies-to-be-enacted-cryptocurrencies-must-be-regulated-within-eu/>

Virtual Currencies, [online].[vid. 10.10 2012]. Dostupné z:

<https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>

What drives bitcoin adoption by retailers?, [online].[vid. 10.2 2018]. Dostupné z:

https://www.dnb.nl/binaries/Working%20Paper%20No.%20585_tcm46-373269.pdf

two-factor authentication (2FA), [online].[vid. 4.4 2015]. Dostupné z:

<https://searchsecurity.techtarget.com/definition/two-factor-authentication>

What Is Google Authenticator (and How to Use It), [online].[vid. 21.4 2018]. Dostupné z:

<https://www.tomsguide.com/us/google-authenticator-how-to-use,news-26819.html>

Exchange Security Report, [online].[vid. 2.10 2018]. Dostupné z:

<https://icorating.com/report/exchange-security-report/>

¹54% of Cryptocurrency Exchanges Have Security Hole, [online].[vid. 2.10 2018]. Dostupné z:

<https://news.bitcoin.com/54-of-cryptocurrency-exchanges-have-security-holes/>

54% of Cryptocurrency Exchanges Have Security Hole, [online].[vid. 2.10 2018]. Dostupné z:

<https://news.bitcoin.com/54-of-cryptocurrency-exchanges-have-security-holes/>
<https://news.bitcoin.com/54-of-cryptocurrency-exchanges-have-security-holes/>

Payments statistics for 2016, [online].[vid. 2.10 2018]. Dostupné z:

<https://www.ecb.europa.eu/press/pdf/pis/pis2016.pdf?be9989f6bd72483ebe27d8dfae1f0362>
bitcoin and Ethereum vs Visa and PayPal, [online].[vid. 22.4 2017]. Dostupné z:

<https://altcointoday.com/bitcoin-ethereum-vs-visa-paypal-transactions-per-second/>
What is VISA, [online].[vid. 30.6 2017]. Dostupné z:

<https://usa.visa.com/dam/VCOM/download/corporate/media/visanet-technology/aboutvisafactsheet.pdf>
Co je RFID, [online].[vid. 30.6 2017]. Dostupné z:

https://www.rfidportal.cz/index.php?page=rfid_obecne
Co je Google Pay?, [online].[vid. 30.9 2018]. Dostupné z:

<https://support.google.com/pay/answer/9026749?co=GENIE.Platform%3DDesktop&hl=cs>

PayPal's annual payment volume from 2012 to 2017, [online].[vid. 30.9 2018]. Dostupné z:

<https://www.statista.com/statistics/419783/paypals-annual-payment-volume/>

Cryptocurrency speed compared [online].[vid. 30.9 2018]. Dostupné z:

<https://howmuch.net/articles/crypto-transactions-speeds-compared>

Debitcardglitchmeansthousandschargedtwice, [online].[vid. 5.9 2018]. Dostupné z:

<https://www.bbc.com/news/uk-england-45400234>

¹Blockchain: how a 51% attackworks (double spendattack), [online].[vid. 5.10 2018]. Dostupné z:

<https://medium.com/coinmonks/what-is-a-51-attack-or-double-spend-attack-aa108db63474>

Volatilita v čase, [vlastní].[vid. 5.12 2018]. Dostupné z: <https://bitvol.info/>

Hereyouwillfind a documented list ofcryptocurrencyexchange hacks, [online].[vid. 27.4 2018].]. Dostupné z:

<https://rados.io/list-of-documented-exchange-hacks/>

Communique G20 bod 9, [online].[vid. 20.3 2018]. Dostupné z:

https://back-g20.argentina.gob.ar/sites/default/files/media/communique_g20.pdf

Online lendersshowinginterest in blockchain technology, [online].[vid. 12.4 2018]. Dostupné z:

<https://www.finder.com/online-lenders-showing-interest-in-blockchain-technology>

Seznam tabulek:

Tabulka 1 Srovnání kapitalizace trhu jednotlivých kryptoměn k 30.11 2018	24
Tabulka 2 - Srovnání možností integrace jednotlivých poskytovatelů platebních bran a poplatky. Zdroj: https://commerce.coinbase.com , https://coingate.com/ , https://bitpay.com/	30
Tabulka 3 – Srovnání možností jednotlivých platebních bran, co se týče podpory fiat měn a nejpoužívanějších kryptoměn. Zároveň jsou zde srovnány časové rámce, ve kterých jsou prováděna účetní vyrovnání.	30
Tabulka 4 Meziroční růst objemu transakcí v USD	34
Tabulka 5 - Srovnání výše poplatků PayPal, VISA a Coinbase.....	35

Seznam grafů:

Graf 1Znázorňuje uvolňování bitcoinů do oběhu v čase.....	9
Graf 2 Růst obtížnosti výpočtu matematických úloh pro ověření transakcí v závislosti na růstu kurzu BTC/USD	10
Graf 3 - Graf zobrazuje nárůst spotřeby el. energie v rámci sítě bitcoin. Celkový produkovaný výkon	10

Graf 4 Extrémní volatilita kurzu BTC od roku 2012 do roku 2018	17
Graf 5 Zájem o výraz bitcoin (modrý), Litecoin (žlutý) a Cryptocurrency (červený) v Google Trends.....	17
Graf 6 Volatilita trhu bitcoin v čase	36

Seznam obrázků:

Obrázek 1 Základní popis transakce	3
Obrázek 2 Názorný příklad fungování blockchainZákladem jsou těžaři spravující celou databázi, kteří seřazují transakce do bloků, ověřují je a následně řadí do řetězce	5
Obrázek 3 bitcoinwallet pro operační systém MS Windows. Obrázek 4 Peněženka pro mobilní zařízení.	6
Obrázek 5- Příklad zpracování vstupu s pomocí SHA256 šifrování.....	8
Obrázek 6 Koncentrace aktivních nodů sítě bitcoin k 27.11 2018.....	11
Obrázek 8- Srovnání reálné propustnosti jednotlivých transakčních sítí	33