Ekonomická fakulta
Faculty of Economics

Jihočeská univerzita v Českých Budějovicích
University of South Bohemia in České Budějovice

JIHOČESKÁ UNIVERZITA V ČESKÝCH BUDĚJOVICÍCH

EKONOMICKÁ FAKULTA

KATEDRA APLIKOVANÉ MATEMATIKY A INFORMATIKY

Bakalářská práce

Kryptografická měna Bitcoin

Vypracoval: Petr Aleš

Vedoucí práce: RNDr. Josef Milota

České Budějovice 2019

JIHOČESKÁ UNIVERZITA V ČESKÝCH BUDĚJOVICÍCH
Ekonomická fakulta
Akademický rok: **2017/2018**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Petr ALEŠ**
Osobní číslo:	**E16249**
Studijní program:	**B6208 Ekonomika a management**
Studijní obor:	**Obchodní podnikání**
Název tématu:	**Kryptografická měna Bitcoin**
Zadávající katedra:	**Katedra aplikované matematiky a informatiky**

Zásady pro vypracování:

Bitcoin je jednou z digitálních měn, které v současné době nabývají na popularitě. Cílem práce je popsat vznik, vývoj, dnešní stav této měny a ukázat principy, na jejichž základě tato digitální měna funguje, rozebrat přednosti a slabiny, porovnat přístupy jiných kryptoměn a popsat fungování systému této kryptoměny z technického hlediska. Dále se zaměřit na otázku bezpečnosti systému a anonymitu uživatelů a ukázat využití při zacházení s citlivými daty, případně provést experiment v této oblasti.

Metodický postup:

1. Analyzovat fungování technologie blockchain, popis historie a vývoje.
2. Popsat principy fungování kryptoměn, smart contracts, porovnání různých technologií, diskutovat vliv na fungování finančních trhů.
3. Analyzovat otázky anonymity uživatelů, bezpečnosti.
4. Navrhnout oblast využití těchto technologií, ve které bude ukázáno jejich využití při zacházení s citlivými daty.
5. Závěr a diskuze výsledků.

Rozsah grafických prací: **dle potřeby**

Rozsah pracovní zprávy: **40 - 50 stran**

Forma zpracování bakalářské práce: **tištěná**

Seznam odborné literatury:

1. **Antonopoulos, Andreas M. (2015).** *Mastering bitcoin.* **Sebastopol CA: O'Reilly.**
2. **Harrigan Martin. (2011).** *An analysis of anonymity in the bitcoin system.* **Dostupné z: http://arxiv.org/abs/1107.4524**
3. **Heilman, E., Baldimtsi, F., Goldberg, S. (2016). Blindly signed contracts: Anonymous on-blockchain and off-blockchain bitcoin transactions. In** *Financial Cryptography and Data Security - FC 2016 International Workshops, BITCOIN, VOTING, and WAHC.* **Christ Church, Barbados, pp. 43-60. [online]. Dostupné z: https://doi.org/10.1007/978-3-662-53357-44**
4. **Narayanan, Arvind. (2016).** *Bitcoin and cryptocurrency technologies: a comprehensive introduction.* **Princeton: Princeton University Press.**
5. **Reid, Fergal, & Harrigan, Martin. (2012).** *An Analysis of Anonymity in the Bitcoin System.* **Cornell University Library [online]. USA: Cornell University Library, [cit. 2018-03-22]. Dostupné z: https://arxiv.org/abs/1107.4524**
6. **Swan, Melanie. (2015).** *Blockchain: blueprint for a new economy.* **Sebastopol, CA: O'Reilly.**

Vedoucí bakalářské práce: **RNDr. Josef Milota**
Katedra aplikované matematiky a informatiky

Konzultant bakalářské práce: **doc. Ing. Ladislav Beránek, CSc.**
Katedra aplikované matematiky a informatiky

Datum zadání bakalářské práce: **19. ledna 2018**

Termín odevzdání bakalářské práce: **12. dubna 2019**

doc. Ing. Ladislav Rolínek, Ph.D.
děkan

JIHOČESKÁ UNIVERZITA V ČESKÝCH BUDĚJOVICÍCH EKONOMICKÁ FAKULTA Studentská 13 (26) 370 05 České Budějovice

doc. RNDr. Jana Klicnarová, Ph.D.
vedoucí katedry

V Českých Budějovicích dne 26. března 2018

Prohlášení

Prohlašuji, že svou bakalářskou práci jsem vypracoval samostatně pouze s použitím pramenů a literatury uvedených v seznamu citované literatury.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce práce, a to v nezkrácené podobě elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž elektronickou cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky školitele a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce s databází kvalifikačních prací Theses.cz provozovanou Národním registrem vysokoškolských kvalifikačních prací a systémem na odhalování plagiátů.

V Českých Budějovicích dne 12.4.2019 Petr Aleš

Obsah

1 Úvod

Za posledních deset let prošel Bitcoin spolu se zbytkem kryptměnového světa bouřlivým vývojem. Od měny, která zajímala jen ty nejzarytější kryptografy až po období obrovského mainstreamového zájmu, který z mnoha lidí učinil milionáře, ale mnohé dohnal až na pokraj bankrotu. Dalo by se říct, že kryptoměny a potažmo Bitcoin jsou fenomén naší doby. I přes tento desetiletý bouřlivý vývoj, Bitcoinu ve skutečnosti pouze málo lidí skutečně rozumí. Mnoho lidí má také pocit, že Bitcoin je jako investiční prostředek nebezepečný, vzhledem k tomu, že změny jeho hodnoty se historicky pohybovali i ve stovkách procent. Právě z toho důvodu jsem svou práci zaměřil právě na Bitcoin, a na to do jaké úrovně je to systém opravdu bezpečný.

1.1 Cíl práce

Cílem práce je poskytnout stručný přehled o tom, jaká jsou specifika kryptoměn, co je to Bitcoin, jaký byl jeho vývoj a jak fungují transakce v rámci systému. V praktické části práce je pak cílem zjistit, jak je v současnosti veřejností nahlíženo na Bitcoinový systém, zda je brán jako potenciální alternativní platební prostředek a jakou roli má z ekonomického hlediska bezpečnost a anonymita systému.

2 Kryptoměny

Kryptoměna je digitální měna, pomocí které se dají vykonávat platby kdekoli na světě a to relativně bez prodlení. Digitální měnou se rozumí taková měna, která existuje pouze ve virtuálním prostředí a nelze ji fyzicky vlastnit. Hlavními důvody vzniku kryptoměn bylo zajištění zvýšené rychlosti a bezpečnosti platebních transakcí oproti klasickým bankovním převodům, které mohou být zdlouhavé a poměrně netransparentní. (Antonopoulos, 2015)

Kryptoměny fungují na základě vědní disciplíny kryptografie, což je věda zabývající se šifrováním. Cílem šifrování je odeslat zprávu takovým způsobem, aby jí rozuměl pouze odesílatel a příjemce. V rámci kryptoměn se kryptografie využívá především pro vytvoření decentralizované, distribuované a bezpečné měny pomocí Peer-to-Peer (P2P) sítě. P2P představuje takovou síť, kde mezi sebou komunikují a předávají si informace jednotliví uživatelé, na rozdíl od klasické internetové sítě, kde se uživatelé nejdříve připojují k určitému serveru. (Hardyn.cz, 2018)

Jednou z hlavních předností kryptoměn je zmíněná decentralizace. Decentralizace v tomto případě znamená, že nad danou kryptoměnou nemá nikdo speciální pravomoce. V rámci sítě nelze najít žádnou centrální autoritu ani žádný centrální bod. Kryptoměny zároveň nemohou být jakkoli regulovány státem, bankami či jinými institucemi, ani svými autory. Díky tomu je zaručena určitá důvěra v systém a současně je zabráněno jakémukoli ovlivňování, kontrolování či falšovaní zvnějšku. Jako další výhodu je možné vnímat, že u peněžních transakcí již není potřeba služeb finančních institucí, z čehož pak vyplívají snížené náklady za transakce. Poplatky za provedenou transakci v rámci kryptoměnových systémů totiž vůbec nejsou, nebo jsou několikanásobně menší než u klasických bank. Zároveň díky decentralizaci nemůže být žádná transakce odmítnuta, stornována či jinak zrušena. (Antonopoulos, 2015)

Bitcoin se stal první decentralizovanou kryptoměnou. Základy pro implementaci Bitcoinu byly vytyčeny v roce 2008, kdy osoba nebo skupina osob známá jako Satoshi Nakamoto, publikovala práci „*Bitcoin:A Peer-to-Peer Electronic Cash System*". Nakamoto zkombinoval několik dřívějších invencí ze systémů jako B-money a HashCash, čímž vytvořil první naprosto decentralizovaný peněžní systém. Jeho klíčová inovace však byla distribuční systém nazvaný „Proof-Of-Work". (Nakamoto, 2008)

2.1 Bitcoin

Nalézt opravdu vyčerpávající definici toho, co Bitcoin znamená, je poměrně složitý úkol. Termín „Bitcoin" totiž může zároveň označovat tři různé věci. Za prvé může označovat technologickou platformu blockchain, která je základem pro jeho fungování. Dále pak může znamenat protokol nadřazený blockchainové technologii, který popisuje jak transakce v rámci blockchainu probíhají. Za třetí, Bitcoin představuje digitální měnu, potažmo konkrétní platidlo. Zjednodušeně, Bitcoin může znamenat všechny tyto věci – software, síť i měnu. (Swan, 2015)

Asi nejvýstižnější vymezení lze nalézt u Andrease Antonopoulose (2015), který Bitcoin definuje jako *„sbírku konceptů a technologií, které tvoří digitální peněžní ekosystém"*.

Pomocí tohoto systému jsou pak následně generovány konkrétní jednotky měny – bitcoiny. Je důležité rozlišovat rozdíl mezi Bitcoinem a bitcoinem. Bitcoin totiž označuje již definovaný peněžní systém, zatímco bitcoin označuje jednotku měny. Tyto měnové jednotky – bitcoiny - jsou v rámci Bitcoinového systému používány k uchovávání a přenosu hodnoty mezi uživateli. Uživatelé spolu komunikují na základě bitcoinového protokolu, primárně prostřednictvím internetu. Bitcoinový protokol je open-source software, díky kterému je technologie snadno dostupná a může být spuštěna na široké škále zařízení, od stolních počítačů až po mobilní telefony. (Bitcoinman, 2019)

Je důležité zmínit, že bitcoiny v zásadě naplňují základní znaky peněz – prostředek směny, zúčtovací jednotka a uchovatel hodnot – nicméně nemohou být za plnohodnotné peníze v právem slova smyslu považovány. Bitcoin může být považován pouze za kryptoměnu, a to díky jeho základním vlastnostem, kterými jsou:

1. ***Decentralizace*** – neexistuje žádná centrální autorita ani instituce, která by Bitcoin ovládala. Generování mincí i potvrzování transakcí zajišťují členové P2P Bitcoin sítě kolektivně.

2. ***Anonymita*** – zatímco u klasických elektronických plateb je identita odesílatelů i příjemců známá, uživatelé Bitcoinu operují v pseudoanonymitě. Vzhledem k tomu, že neexistuje centální autorita, uživatelé se při transakcích bitcoinů nemusí identifikovat. Při konkrétní transakci jsou uživatelé představováni

pomocí adres, což jsou 34 znaků dlouhá alfanumerická čísla. Žádné osobní údaje tak nejsou vyžadovány.

3. ***Omezený počet*** – klasické měny mají předem neomezený počet jednotek, které mohou být vydány do oběhu. Ty obvykle emitují centrální banky. V případě Bitcoinu emitování funguje na základě algoritmu. Konečný počet bitconů je předem určen (21 milionů) a prostřednictvím miningu do systému přichází každých 10 minut několik nových jednotek.
4. ***Neměnitelnost*** – na rozdíl od klasických elektronických transakcí, Bitcoinové transakce nelze zpětně zrušit či změnit. Jakmile je jednou transakce zaznamenaná v systému, je nemožné ji změnit, protože neexistuje autorita, která by mohla takovýto příkaz vydat.
5. ***Dělitelnost*** – vzhledem k tomu, že jde o digitální měnu, každý bitcoin lze dále dělit, a to až na nejmenší jednotku zvanou satoshi. Ta představuje jednu miliontinu bitcoinu (což představuje asi jednu setinu amerického dolaru). Tato vlastnost pak umožňuje mikrotransakce, které tradiční elektronické peníze dnes nemohou**.**
6. ***Open source*** – celý systém má veřejné a otevřené zdrojové kódy a kdokoliv se tak může podívat a zkontrolovat přesné fungování vnitřního systému. (Acheson, 2018)

2.2 Předchůdci Bitcoinu

Přestože je dnes Bitcoin neznámější a nejpopulárnější kryptoměnou, není kryptoměnou první. Za prvního vzdáleného předchůdce kryptoměn by se dal považovat systém zavedený na konci osmdesátých let 20. století v Nizozemsku, využívající elektronických peněz. (Reiff, 2018)

2.2.1 Digicash

Zhruba ve stejnou dobu se americký kryptograf David Chaum pokoušel o navržení další formy elektronických peněz. David Chaum přišel s konceptem tokenové měny – což je taková měna, která emuluje fyzické mince a bankovky (jako je dnes např. bitcoinová mince). Tato měna by pak mohla být mezi jednotlivci bezpečně a hlavně anonymně převáděna. Chaum vypracoval tzv. „blinding vzorec", což je rozšíření RSA algortimu

dodnes používaného při šifrování webu. Tento vzorec umožňoval jedné osobě předat druhé osobě číslo, které bylo následně příjemcem upraveno. Pokud by si tento příjemce chtěl uložit svou minci do banky, tato mince by na sobě měla originální podpis (číslo) mincovny, který by ale nebyl stejný, jako číslo, pod kterým byla tato mince „vyražena". Chaumův vzorec tedy umožnil, aby mince neztratily originalitu podpisu mincovny a zároveň mohly být převáděny a upravovány, aniž by mincovna či banka o těchto transakcích věděla. Od toho odvozený název blinding – oslepující. (Grigg, 2014)

Chaum dal svému konceptu život, když o několik let později založil v Nizozemsku firmu DigiCash. V době spuštění se jednalo o první formu elektronických peněz, která nabízela anonymitu díky kryptografickým protokolům. Už v tomto prvním systému byla implementována kryptografie veřejného a privátního klíče, která se používá i v současných kryptoměnách. Bohužel ale kvůli několika managerským přešlapům a zásahům Nizozemské národní banky se společnosti nedařilo podle představ jejího zakladatele. Přestože Digicash v roce 1998 zbankrotoval, na jeho základech se pak odrazil další vývoj v oblasti digitálních měn. (Grigg, 2014)

2.2.2 B – Money

Jako další z předchůdců, ze kterého Satoshi při navrhování Bitcoinu konkrétně vycházel, byl B-Money. Tento systém byl navržen v roce 1998 kryptografem Wei Danem. Hlavní specifika pro něj byla anonymita a distribuce elektronických peněz. Systém B-Money měl fungovat na základě decentralizované sítě, kde by si lidé skrytí pod digitálními pseudonymy mohli posílat měnu. Dokonce zahrnoval i prostředky pro vymahatelnost dodržení smluv uzavřených v síti, a to bez nutnosti zásahu třetí strany. Nakonec však tento systém zůstal pouze jako koncept, jelikož Wei Dan nikdy nezískal dostatečnou pozornost ani podporu, aby mohl převést svůj návrh do reality. (Reiff, 2018)

2.2.3 Bit Gold

Dalším systémem, ze kterého Bitcoin vycházel je Bit Gold. Byl to další systém elektronických peněz, navržený ve stejné době jako B-Money. Podobně jako B-Money se snažil ustoupit od centralizovanosti a nutnosti být vázaný na autority. Důležitou součástí, kterou později Bitcoin svým způsobem převzal a zadaptoval, je vlastní Proof-

of-Work systém. Tento Proof-of-Work systém fungoval v mnoha ohledech jako současný blockchain – kde jsou záznamy kryptograficky zpracovávány a posléze uveřejněny pro veřejnost. Stejně jako jeho předchůdce, nakonec i tento systém se stal ve své době neúspěšný. (Grigg, 2014)

2.2.4 Hashcash

Naopak úspěšným ve srovnání se svými předchůdci se stal systém pojmenovaný HashCash. Koncepty tohoto systému sahají do roku 1992, kdy výzkumníci Moni Naor a Cynthia Dwork vydali svou práci „Pricing via Processing or Combatting Junk Mail". V této práci se zabývali systémem, který by dokázal redukovat množství příchozích spam e-mailů, a to díky tzv. pricing function protokolu. V rámci tohoto protokolu museli uživatelé nejdříve využít svůj výpočetní výkon na vyřešení zadané funkce, načež jim byl udělen přístup do systému (v tomto případě do e-mailu). Hlavní myšlenkou bylo po uživateli před vstupem do systému požadovat vyřešení složité, ale ne neřešitelné funkce, díky čemuž by se zabránilo zneužití nebo zbytečnému použití systému. (Narayanan, 2016)

O pět let později kryptograf Adam Back navrhl velice podobný systém, se základem právě v práci Naora a Dworkové. Svůj návrh pojmenoval HashCash. Původně se mělo jednat o mechanismus, pomocí kterého by bylo možné kontrolovat systematické zneužívání veřejných a sdílených internetových prostředků, jako jsou například e-maily. (Lielacher, 2018)

V roce 2002 Back publikoval svou práci "Hashcash – A Denial of Service Counter-Measure", kde detailně popsal svůj protokol. V této práci bylo vysvětleno, jak se díky použití pricing funkce docílilo toho, že se z HashCashe stal anti-DOS mechanismus. HashCash totiž vyžadoval, aby uživatelé používali výpočetní výkon svých zařízení jako Proof-of-Work (důkaz o provedené práci). Pro normální uživatele se nic nezměnilo, nicméně pro uživatele s postranními úmysly se tento mechanismus projevil jako těžko překonatelný problém. Pro uživatele, který posílal e-mail byl tento mechanismus takřka nepostřehnutelný, zátěž procesoru se takřka nezměnila, maximálně se poslání e-mailu protáhlo o několik málo sekund. Zato pro spammery, kteří zvládali odeslat i několik desítek tisíc e-mailů za minutu, se jednalo o kritický problém. (Back, 2002)

HashCash bylo nakonec možné přidat do osobního e-mailu přes plugin. Tam byla pomocí kryptografické hash funkce SHA-1 ke každému e-mailu vytvořena a přiřazena známka, která příjemci osvědčovala, že se nejedná o spam. HashCash byl nakonec využíván řadou organizací, ve snaze bojovat se spammery. Mezi nejznámější lze zařadit filtr Spam Assassin, což byl emailový klient Mozilly Thunderbird. Dokonce i Microsoft nějakou dobu využíval upravenou verzi HashCashe. (Back, 2002)

2.3 Vývoj Bitcoinu

Nakamotova práce obsahuje konkrétní odkazy na to, že HashCash posloužil jako inspirace pro implementaci miningu v blockchainu. Přestože jsou si podobné, v zásadních vlastnostech se tyto algoritmy liší. Bitcoin používá kryptografickou funkci SHA-256, která má 256 bitů, na rozdíl od HashCashové SHA-1 se 160 bity. Dále hašovací funkce je v Bitcoinovém systému použita dvakrát (nejprve SHA-256 a posléze RIPEMD160), a to proto, aby byla zvýšena bezpečnost systému vůči různým pokusům o narušení bezpečnosti. V systému HashCash se složitost algoritmu používaného k těžení zvyšovala nebo snižovala o polovinu. V případě Bitcoinu se ale složitost algoritmu přizpůsobuje dynamicky, tak aby průměrná doba vytvoření jednoho bloku činila 10 minut. (Lielacher, 2018)

V roce 2008 pak Nakamoto publikoval svou práci „*Bitcoin: A Peer-to-Peer Electronic Cash System*". Tato práce obsahovala matematický algoritmus, který se snažil vyřešit problémy digitálních měn, a to zejména problém tzv. „double spendingu" – použití jedné mince pro více transakcí. Tato záležitost byla v té době kritickou překážkou pro další vývoj a především pro důvěru v kryptoměny. V dřívějších systémech se jako řešení tohoto problému využíval centrální clearinghouse, přes který musely všechny transakce procházet. Nakamoto však tento problém vyřešil použitím decentralizované sítě počítačů, které každou transakci v systému musí ověřit a následně dojít ke konsensu o stavu těchto transakcí. Díky implementaci tohoto systému je pak problém dvojité útraty z velké části vyřešen. (Antonopoulos, 2015)

Samotné spuštění Bitcoinové sítě proběhlo 3.ledna 2009, kdy byl Nakamotem zároveň vytěžen první blok 0, také známý jako „Genesis blok". Tím vzniklo prvních 50 bitcoinů. Tyto bitcoiny jsou zvláštní tím, že byly vytvořeny takovým způsobem, že je nemožné je utratit. Byly totiž Nakamotem zakódovány naprosto odlišně od zbytku, ale z důvodů

dodnes neznámých. Další vytěžený blok do blockchainu přišel až po celých šesti dnech, což je poměrně značný odstup od klasických deseti minut potřebných na vytěžení bloku. Ohledně této prodlevy panuje několik teorií. Například, že Nakamoto prvních pár dní testoval síť nebo existuje i kuriozní teorie, že čekal šest dní, protože podle knihy Genesis i Bohu trvalo šest dní stvořit Zemi. Nicméně devět dní po spuštění sítě proběhla první transakce mezi Satoshim a programátorem Halem Finneym, který se v budoucnu v rámci Bitcoinu stal velkou osobností.

V roce 2009, kdy Bitcoin široká veřejnost neznala, se o něj víceméně zajímali pouze kryptografové, které zajímal zejména po stránce technické. Nebyl tedy brán jako investiční příležitost a už vůbec ne jako běžně přijatelná měna. Přesto už v říjnu 2009 byl na platformě New Liberty Standart stanoven směnný kurz pro pár Bitcoin a USD, který v tě době byl 2300 bitcoinů za dolar. V roce 2010 pak proběhla první transakce, kde byl Bitcoin směněn za fyzické zboží. Dnes jde již o památnou transakci, při které Laszlo Hanyecz zaplatil 10 000 BTC Jeremy Sturdivantovi, za dvě pizzy dovezené od Papa John's. Rok 2010 byl také rokem, kdy se o projekt začínali ve větší míře zajímat investoři, a právě proto byla založena první bitcoinová burza Bitcoin Market. V tomtéž roce se o Bitcoin začala zajímat americká FBI a zhruba ve stejné době se z projektu jeho tvůrce Satoshi Nakamoto stáhl, předal zdrojový kód Gavinu Andersonovi a nikdy se zpět nevrátil. Ohledně Nakamotovy identity dodnes panuje nejistota. Původně se myslelo, že jde o kryptografa žijícího v Japonsku, nicméně tato hypotéza nebyla nikdy potvrzena. Podle e-mailové korespondence bylo zřejmé, že šlo o jedince s bezchybnou angličtinou. Doba, kdy byly prováděny úpravy na síti naznačovala, že žil spíše na západě. Někteří lidé se dokonce domnívají, že se jednalo o skupinu lidí, nicméně podle výpovědí jeho kolegů, kteří s ním byli v kontaktu, je pravděpodobnější, že se jednalo pouze o jednoho člověka. Způsob jakým psal a komunikoval byl příliš specifický na to, aby ho bylo schopno udržovat více lidí. Za dobu, po kterou Nakamoto pracoval na Bitcoinu vytěžil přes milion bitconů, ty však nebyly nikdy použity a stále zůstávají uloženy v původní Nakamotově peněžence. (Narayanan, 2016)

Rok 2011 se pro Bitcoin stal velkým milníkem. Devátého února totiž Bitcoin dosáhl parity s americkým dolarem. Po tomto milníku se zájem o Bitcoin i jeho cena začaly prudce zvyšovat. Za pouhé čtyři měsíce pak Bitcoin více než ztřicetinásobil svou cenu a obchodoval se v poměru 1BTC/31,91$. Nicméně v této době začala měnu provázet i řada kontroverzí. Bitcoin byl totiž ve velkém používán jako platidlo na darkwebové

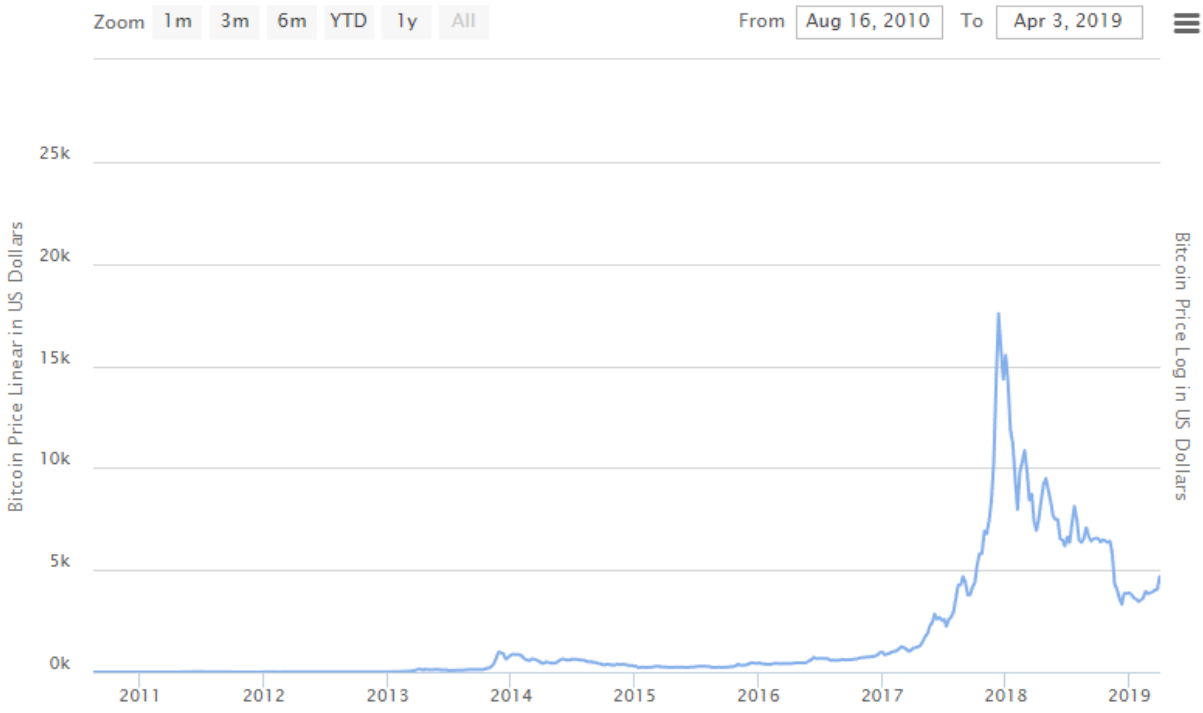
platformě Silk Road, kde se ve velkém prodávaly zbraně či drogy, takže se o něm začalo mluvit jako o měně drogových dealerů. Také bylo poprvé upozorněno na bezpečnost systému, když byla napadnuta burza Mt.Gox a bitcoinová síť byla na určitou dobu ochromena. V důsledku těchto událostí se začal Bitcoin potýkat s poměrně značnou volatilitou. (Vigna, Casey, 2016)

Rok 2012 představoval pro Bitcoinovou komunitu rok, kdy bylo třeba ujistit veřejnost o bezpečnosti systému. Vývojářská komunita se tedy zaměřila na dodatečné úpravy bezpečnostní stránky. Zároveň byla ukončena činnost platformy Silk Road. Právě z těchto důvodů pak cena Bitcoinu začala vzrůstat. První půlení, kdy je odměna za vytěžení bloku zredukována o polovinu, proběhlo 28. října 2012. V té době dosahoval jeden bitcoin hodnoty blížící se 200 dolarům. O rok později pak bitcoin dosahoval cenové parity s uncí zlata, což bylo více než tisíc dolarů. V roce 2014 pak Bitcoin postihla velmi nepříjemná událost, kdy v té době největší světová burza Mt.Gox pozastavila všechno obchodování a o týden později vyhlásila bankrot. Na této burze se odehrávalo přes sedmdesát procent všech bitcoinových transakcí a v důsledku vyhlášení bankrotu bylo ztraceno přes sedm set tisíc bitcoinů. Dále začaly také snahy velkých hráčů jako Číny a USA o regulaci této měny. Po tomto sledu událostí došlo očekávaně k výraznému oslabení a Bitcoin se pohyboval na úrovni 300USD. Ke konci roku 2014 naštěstí začala diskuse o tom, zda by blockchainová technologie měla využití i v jiných oblastech jako například v administrativě či registračních systémech. V návaznosti na to pak začal být Bitcoin podporován PayPalem a i Microsoft začal akceptovat bitcoinové platby, což předznamenalo velký mainstreamový zájem. (Vigna, Casey, 2016)

Tento nově nalezený entuziazmus naštěstí přetrval a bitcoinová komunita se nadále rozrůstala. Bitcoin se začal dostávat do povědomí širší veřejnosti a čím dál více platforem začalo přijímat platby Bitcoinem. Začalo tak období pomalého, ale stabilního růstu. Tento trend pokračoval až do začátku roku 2017, kdy se kryptoměny a zejména Bitcoin staly předmětem obrovského boomu. Z původní hodnoty 1000 USD se za méně než rok vyšplhal na neuvěřitelných 20 000 dolarů. Tento vývoj měl hned několik důvodů, jako první očekávaný update protokolu nazvaný SegWit, který částečně vyřešil problém pomalého zpracovávání transakcí. Dále i přístup vlád k Bitcoinu se změnil, v některých se dokonce stal legálně přijímaným platidlem pro uhrazování plateb. Bitcoin se také stal více důvěryhodným finančním instrumentem, což pak přidávalo obchodování s Bitcoinem legitimitu. Tomuto vývoji určitě přispěla i popularizace

kryptoměn v médiích a podpora známých osobností jako byl například Bill Gates. Nicméně se ukázalo, že tento vývoj je neudržitelný a někteří lidé toto období přirovnávají ke kryptografické bublině. Již na začátku roku 2018 došlo ke korekci, kdy cena spadla na hodnotu 9000 dolarů a v tomto trendu dále pokračovala. V tomto období docházelo k vysoké volatilitě, nicméně hodnota Bitcoinu nadále klesala. Se sníženou důvěrou v Bitcoin jako investiční prostředek a dalšími nepříjemnými událostmi, jako byly například soudní spory, pak cena stabilně klesala. V polovině roku 2018 se hodnota pohybovala na hodnotě 5000 dolarů, ale s výrazně sníženou volatilitou. Pokles ceny pokračoval až na hodnotu kolem 3000 dolarů, nicméně od té doby poměrně stabilně roste, dnes se pohybuje v rozmezí od 3 do 4 tisíc dolarů. Mohlo by tedy znovu dojít k období pomalého stabilního růstu. Takový vývoj by Bitcoinu prospěl co se týče obnovy důvěry veřejnosti. (Vigna, Casey, 2016)

Graf 1 Historie cen Bitcoinu



(Bitcoin Price History Chart (Since 2009)

2.4 Hašovací funkce

Hašovací funkce je taková funkce, která vezme vstupní hodnotu a převede ji na výstup s předem definovanou délkou (u Bitcoinu 256 nebo 160 bitů). Tento výstup je označován jako miniatura, otisk nebo hash. Pro jeden konkrétní vstup musí při každém

použití této funkce vždy vycházet stejný výstup. Dalo by se tedy říci, že jde o funkci deterministickou, tedy že pro každý vstup existuje předdefinovaný výstup. Zároveň se jedná o funkci jednosměrnou, což znamená, že z konečného výstupu (hashe) se nedá zpětně získat původní vstup. (Narayanan, 2016)

Aby funkce mohla být považována za hašovací, musí být schopna odolat všem známým typům kryptoanalytických útoků. Proto musí mít hašovací funkce určité vlastnosti. Těmi jsou:

- *Kompresnost* – schopnost převést vstup libovolné délky na výstup, který má předem definovanou bitovou délku a zároveň je snadno vypočitatelný.
- *Odolnost argumentu* – pro všechny výstupy by mělo být výpočetně neproveditelné nalézt takový vstup, který by hašoval na daný výstup. Jinými slovy tato vlastnost zajišťuje jednosměrnost.
- *Odolnost druhého argumentu* – je výpočetně neproveditelné nalézt takový druhý vstup, který by hašoval na stejný výstup jako předem určený první vstup. Tato vlastnost je důležitá zejména v případě ověřování digitálních podpisů. Jinak by totiž mohla nastat situace, kde by mohl být ověřen podpis za použití falešné identity.
- *Odolnost proti kolizím* – je výpočetně neproveditelné nalézt jakékoliv dva vstupy, které by hašovali na stejný výstup.

U podmínky odolnosti proti kolizím by se mohlo zdát, že jde o stejnou podmínku jako v předchozím případě. Důležitý rozdíl je ale v tom, že si můžeme první vstup zvolit libovolně. V praxi mají totiž tyto podmínky jiný výpočet pravděpodobnosti náhodného nalezení kolizí. Útoky na systémy, které nemají odolnost proti kolizím jsou totiž o mnoho snazší. Jedná se o útoky hrubou silou, které jsou v tomto případě nazývány jako tzv. *narozeninové útoky* (podle narozeninového paradoxu). (Kment, 2005)

2.4.1 SHA-256

SHA-256 (Secure Hash Algoritmus) je hlavní hašovací funkcí používanou v Bitcoinu. Jde o jednu z řady hašovacích funkcí SHA-2 navrženou americkou Národní bezpečnostní agenturou. Oproti původním funkcím z řady SHA-1 (jejichž délka byla 160bitů) je konečný výstup funkcí SHA-2 delší, a to 224, 256, 384 nebo 512 bitů. Podle délky bitů výstupů se pak nazývají konkrétní funkce - SHA-224, SHA-256, SHA-384,

SHA-512, SHA-512/224 a SHA-512/256. Zvýšením délky výstupů se zvýšila odolnost proti útokům nalezení kolize nebo vzoru. Za zmínku stojí, že do dnešního dne nebyla tato funkce jakkoliv prolomena. (Katz, Lindell, 2008*)*

Její použití je v rámci Bitcoinu především k vytváření a ověřování elektronického podpisu a také je použita v Proof-of Work algoritmu u Bitcoinového těžení.

3 Způsoby získání bitcoinů

V současnosti existují tři možnosti jak bitcoiny získat. Jedná se o nákup, prodej a formu specifickou pro kryptoměny – mining .

3.1 Nákup

Nejspíše nejjednodušším způsobem jak k bitcoinům přijít je klasický nákup. Před tím, než je bitcoiny možné koupit, je ale potřeba splnit několik kroků. Za prvé je třeba založit Bitcoinovou peněženku, pomocí které je pak možné kontrolovat transakce. To je poměrně rychlý proces, založení takové peněženky je totiž pouze otázka stažení příslušného softwaru a vyplnění příslušných údajů. Dnes je na trhu obrovské množství zprostředkovatelů této služby, takže záleží na uživatelských požadavcích, pro kterou se rozhodne. Potom co je založena peněženka je už možné bitcoiny nakupovat. To lze pomocí tradičních elektronických platebních metod jako jsou kreditní karty, debetní karty čí bankovní převody. Potom co proběhne platba, jsou bitcoiny převedeny na danou peněženku. Stojí za zmínku, že z technického hlediska tyto bitcoiny nejsou uloženy přímo v peněžence, ale nacházejí se tam klíče, které uživatele opravňují k operacím s nimi. (Bajpai, 2019)

Dnes jsou nejvyužívanější tři platformy pro nákup bitcoinů, a to bitconové směnárny, bitcoinové burzy a bitcoinové automaty. Existují samozřejmě i jiné možnosti jak nakoupit bitcoiny, například nákup osobně, nicméně tyto způsoby jsou v poměru s těmito třemi nevýznamné. (Miksa, 2018)

Bitcoinové směnárny jsou digitální tržiště, kde mohou obchodníci nakupovat a prodávat bitcoiny pomocí různých národních měn či jiných kryptoměn. Jde tedy o online platformu, která slouží jako prostředník mezi nakupujícími a prodávajícími. Směnárny fungují jako tradiční burzy, kde nakupující přichází do směnárny s “bid” cenou a prodávající s “ask” cenou, a v momentě kdy se tyto ceny střetnou pak může dojít k uskutečnění transakce. Vzhledem k tomu, že je zde využívána služba třetí strany je pochopitelné, že je za ni také nutno zaplatit poplatek. Poplatky jsou vybírány za každou uskutečněnou transakci a mají v průměru velikost 0,25% z hodnoty dané transakce. Pravděpodobně největší současnou bitcoinovou směnárnou je Coinbase, což je americká směnárna, na které lze obchodovat pomocí široké škály měn a to ve velmi intuitivním uživatelském prostředí. Z českých směnáren lze zmínit např. platformy Simplecoin.cz a

Easycoin.cz, které mají za sebou roky provozu a obchody v rámci milionů korun. (Guttmann, 2013)

Druhou možností jak koupit bitcoin je prostřednictvím bitcoinové burzy. Na rozdíl od bitcoinových směnáren se zde obchoduje v daleko větších objemech, na druhou stranu ale také za mnohem výhodnějších cen. Bitcoin se zde kupuje a prodává pomocí měnových párů, a to zejména BTC/USD a BTC/EUR, které zajišťují nejvyšší likviditu. Na rozdíl od směnáren je na burzách poskytována také větší anonymita, jelikož do určitého objemu obchodování stačí pouze registrace účtu na dané burze. Proces nákupu probíhá tak, že se zadá požadovaná cena a objem a následně se buď vybere z dostupných nabídek nebo se zadá příkaz nový. Na burzách se dá také využívat klasických burzovních nástrojů jako je například obchodování s pákovým efektem, nicméně takové obchodování je vhodné spíše pro spekulanty a zkušené investory, kteří obchodují Bitcoin hlavně s vidinou zisku. Nejznámější Bitcoinové burzy jsou Bitstamp, Bitfinex a GDAX, z těch českých pak burza Coinmate. (Guttmann, 2013)

Další možností jak koupit bitcoin je pomocí bitcoinového automatu. Jedná se o automat podobný bankomatu, který uživateli umožňuje nakoupit bitcoiny pomocí kreditní nebo debetní karty. Některé automaty nabízejí i obousměrnou funkci, která umožňuje jak nákup, tak i prodej bitcoinů za hotovost. Automaty jsou připojené k internetu a podle toho o jaký typ se jedná se pak tyto automaty připojují buď přímo k bankovnímu účtu nebo pouze k Bitcoinové směnárně. Nákup probíhá tak, že do automatu je vložen patřičný obnos v bankovkách, následně je pomocí čtečky QR kódů načtena adresa peněženky a po zpracování platby je nákup potvrzen a vydána účtenka. Dnes se jedná o poměrně populární nástroj pro nákup krypotměn a na našem území lze nalézt již 39 takovýchto automatů, z nichž se většina nachází v Praze. (Guttmann, 2013)

3.2 Prodej

Dalším způsobem jak získat bitcoiny, je prodej ve smyslu prodávání zboží či služeb výměnou za platbu v bitcoinech. Tuto možnost nejčastěji využívají větší podniky s důrazem na nové technologie, u nás například Alza. S rozvojem kryptoměn se počet míst akceptujících bitcoinové platby pomalu zvyšuje, a dnes se dá pomocí bitcoinu zaplatit například i káva v kavárně. Podniky akceptující bitcoinové platby mají tuto schopnost umožněnou díky tzv. „Bitcon Payment Services" – Bitcoinovým platebním

službám. Jedná se o službu třetí strany, která podniku poskytne technologii podobnou jako u plateb kreditními kartami. Zákazníkovi se při uhrazování platby zobrazí hodnota transakce, směnný kurz, adresa a QR kód, na který je třeba transakci odeslat. Potom co je odeslána, je zákazníkova platba považována za splněnou, i když ve skutečnosti přijde až o několik desítek minut později. Tato platba ale přichází do systému provozovatele Bitcoinové platební služby, který pak tuto platbu posílá zpět podniku využívajícího jeho služeb. Platbu může zaslat buď v bitcoinech nebo v měně podle jejich výběru. Nejčastěji však podniky stojí o platby v klasických měnách, jelikož se tak vyhnou případné volatilitě, která by mohla být s kryptoměnou spojená. (Seth, 2018)

3.3 Mining

Vzhledem k tomu, že Bitcoin funguje na základě decentralizované sítě vyvstává otázka, jak jsou vlastně mince vůbec emitovány. V případě klasických peněz se o tento problém stará vláda (skrze národní banky), Bitcoin ale žádnou vládu nemá. Jak už bylo dříve řečeno, neexistuje žádná centrální autorita ani instituce, která by Bitcoin vlastnila či ho nějak kontrolovala. V rámci systému jsou bitcoiny vydávány díky procesu známému jako mining – těžení.

Těžení je proces, při kterém jsou nové bitcoiny uvolňovány do oběhu. Dále slouží také k tomu, aby bránilo systém proti podvodným transakcím, či transakcím, které mají jako záměr útok dvojité útraty. Těžení provádějí těžaři (miners), kteří Bitcoinové síti propůjčují svůj výpočetní výkon, aby měli možnost tyto nově emitované bitcoiny získat. (Antonopoulos, 2015)

Těžaři ověřují všechny nové transakce a zaznamenávají je do veřejně přístupné databáze známé jako blockchain. Potvrzené transakce se do blockchainu zadávají ve formě bloků, což je v podstatě soubor shromažďující několik transakcí. Každý takovýto blok je „vytěžen" jednou za 10 minut a tyto transakce jsou následně ve formě bloku přidány na konec blockchainu. Je důležité si uvědomit, že každý další blok musí potvrzovat všechny transakce vytvořené od vzniku blockchainu. Poté, co jsou tyto transakce potvrzené a zaznamenané v blockchainu, dochází k převodu vlastnictví konkrétních bitcoinových mincí. (Antonopoulos, 2015)

3.3.1 Proces těžení

Nyní se dostáváme k tomu, jak těžení konkrétně probíhá. Vezměme v úvahu, že do systému byla právě přijata transakce "A". Je to transakce nová, tudíž čekající na potvrzení. Ve stejnou chvíli ale do systému přichází další nepotvrzené transakce. Vzhledem k tomu, že těžaři jsou rozmístěni všude po světě, ke každému se transakce dostávají v jiném pořadí. Všichni těžaři se pak snaží vytvořit další blok, nicméně naše transakce "A" v něm bude vždy na jiném místě (v závislosti na poloze těžaře a době přijetí transakce).

Těžaři tedy vezmou transakce, které doposud nebyly zaznamenané v žádném předcházejícím bloku a snaží se vytvořit blok nový. Nové bloky vznikají pomocí hašovací funkce SHA-256, o které už byla řeč. Vytvoření haše z těchto transakcí by bylo snadné, nicméně těžení funguje přesně naopak. Těžaři mají totiž stanovený *cíl* (target), ke kterému musejí nalézt takový vstup, který by hašoval na stejnou nebo menší hodnotu jako má tento cíl. (Swan, 2015)

Cíl je 256 bitů dlouhé číslo stanovené bitcoinovým programem, sdílené všemi těžaři v síti. Úkolem těžařů je překódovat data z nepotvrzených transakcí tak, aby hašovala na hodnotu stanovenou cílem (nebo na hodnotu menší). Tento problém se však nedá vyřešit žádným algoritmem, tudíž se zde musí aplikovat metoda pokus omyl. Těžaři se k požadovanému vstupu dostanou pouze za použití hrubé síly – náhodným zkoušením různých vstupů. Je zřejmé, že tato metoda je velice náročná, zároveň se ale správný hash dá lehce ověřit. Tomuto hashi se také jinak říka Proof of Work. Těžař, který tento hash nalezne jako první, získá odměnu za těžení a všechny poplatky z transakcí zahrnutých v bloku. Dále je tento blok odeslán zbytku Bitcoinové sítě a je připojen k hlavnímu řetězci. Tento proces se pak opakuje pro další nepotvrzené transakce. (Swan, 2015)

3.3.2 Proof of Work

Vzhledem k tomu, že na správný vstup může těžař přijít jen náhodně, musel zřejmě vynaložit značné úsilí na to, aby se mu to povedlo. Od toho je odvozen název Proof of Work – důkaz o vynaložené práci. Dnes je to nejvyužívanější algoritmus zajišťující bezpečnost kryptografických měn.

Vygenerování nějakého hashe pro řadu bitcoinových transakcí by bylo pro moderní výpočetní techniku triviální, takže pro to, aby se opravdu jednalo o "práci", je bitcoinovou sítí vytvářena určitá míra obtížnosti. Tato obtížnost je nastavena tak, že systém vezme v úvahu výpočetní výkon celé sítě a podle toho je nastaven cíl tak, aby průměrná doba nalezení řešení byla 10 minut. Konkrétně, každých 2016 bloků (což jsou zhruba dva týdny) porovnává bitcoinový klient předpokládaný čas se skutečným časem, který byl na vytěžení těchto blok potřeba. Pokud je mezi těmito hodnotami rozdíl, je cíl upraven právě o tento procentní rozdíl. (Antonopoulos, 2015)

Podle toho jaký je výpočetní výkon v síti je pak upravena složitost každého cíle. Vzhledem k tomu, že cíl je 256 bitů dlouhé číslo, v praxi je složitost udávána tím, jak dlouhý je řetězec nul na začátku. Čím více výkonu tedy síť má, tím více nul na začátku má požadovaný cíl (a tím menší je požadované číslo). (Khatwani, 2018)

Když vezmeme v úvahu, že jedna sada dat (soubor nepotvrzených transakcí) může vygenerovat pouze jeden hash, vyvstává otázka, jak těžaři pomocí těchto dat dokáží nalézt stanovený cíl. Toho je dosaženo tak, že se k datům při každém hashování přidá celočíselná hodnota, nazývaná *nonce* (number used once) – jde o jednou použité číslo náhodně vybrané v intervalu od 0 do 4 294 967 296. Díky tomu pak každý takovýto vstup generuje naprosto jiný výstup při zachování údajů o transakcích. (Frankenfield, 2018)

Jak lze vidět, těžení je sice soutěž, ale jde spíše o loterii než o závod. I samotný těžař s omezeným výkonem totiž může mít štěstí a vytěžit blok před uživateli sdružujícími se v mining poolech s nesrovnatelně vyšší výpočetní kapacitou.

3.3.3 Mining pools

Mohlo by se zdát, že když jde v zásadě o loterii, těžení bitcoinů by mohlo být pro jedince dobrou možností pro přivýdělek. A opravdu, v době kdy Bitcoin začínal a obtížnost těžení byla relativně jednoduchá, tak v podstatě kdokoli mohl začít těžit bitcoiny a vydělat na tom. V té době stačilo těžit na domácím počítači za využití procesoru. Nicméně čím více lidí začalo objevovat těžení, tím se také tento proces stával náročnější. Místo procesorů se na šifrování začali používat grafické karty, které se ukázaly jako daleko efektivnější. Postupem času se začali vyvíjet technologie speciálně navržené jen k těžbě kryptoměn jako například ASIC. Jde o specializovaný

hardware, který využívá počítačový čip uzpůsobený právě na to, aby opakovaně prováděl funkci potřebnou k těžení. V současnosti je dalším problémem také cena elektřiny. Těžení je totiž vysoce energeticky náročné a ve většině západních zemí se z tohoto důvodu stává neefektivní. Proto někteří podnikatelé, kteří těží ve velkém, přesouvají svůj těžařský hardware na východ. V současnosti dominuje masovému těžení Čína se svou levnou elektřinou, kam se tito podnikatelé také uchylují nejvíce. (Heilman, Baldimtsi, Goldberg, 2016)

Z těchto důvodů je dnes pro jedince těžení zřídkakdy výnosnou činností. Právě proto začali vznikat společenství sdružující tyto samostatné jedince, které se nazývají mining pools. V těchto společenstvích všichni těží jako obvykle, když ale některý člen nalezne vítězný hash, odměnu si nenechá, ale rozdělí se mezi celé společenství. Odměna se dělí podle množství práce, kterou přispěli k zvýšení pravděpodobnosti nalezení bloku (nestačí tak pouze být členem společenství). Podíl z odměny je pak nejčastěji vyplacen těm, kteří předloží alespoň částečný Proof of Work. (Heilman, Baldimtsi, Goldberg, 2016)

Hlavními výhodami těchto společenství je pak stabilní odměna za prováděnou práci. Na druhou stranu, jako u všech podobných společenství je třeba platit členské poplatky. V tomto případě jsou ale vybírány tak, že těžařům je vyplacena pouze bitcoinová odměna, zatímco peníze z transakčních poplatků si ponechává správce. Dalším problémem pak může být fakt, že jde o organizaci řízenou třetí osobou, tudíž je pak důležitým faktorem důvěra a prověřenost společenství. (Swan, 2015)

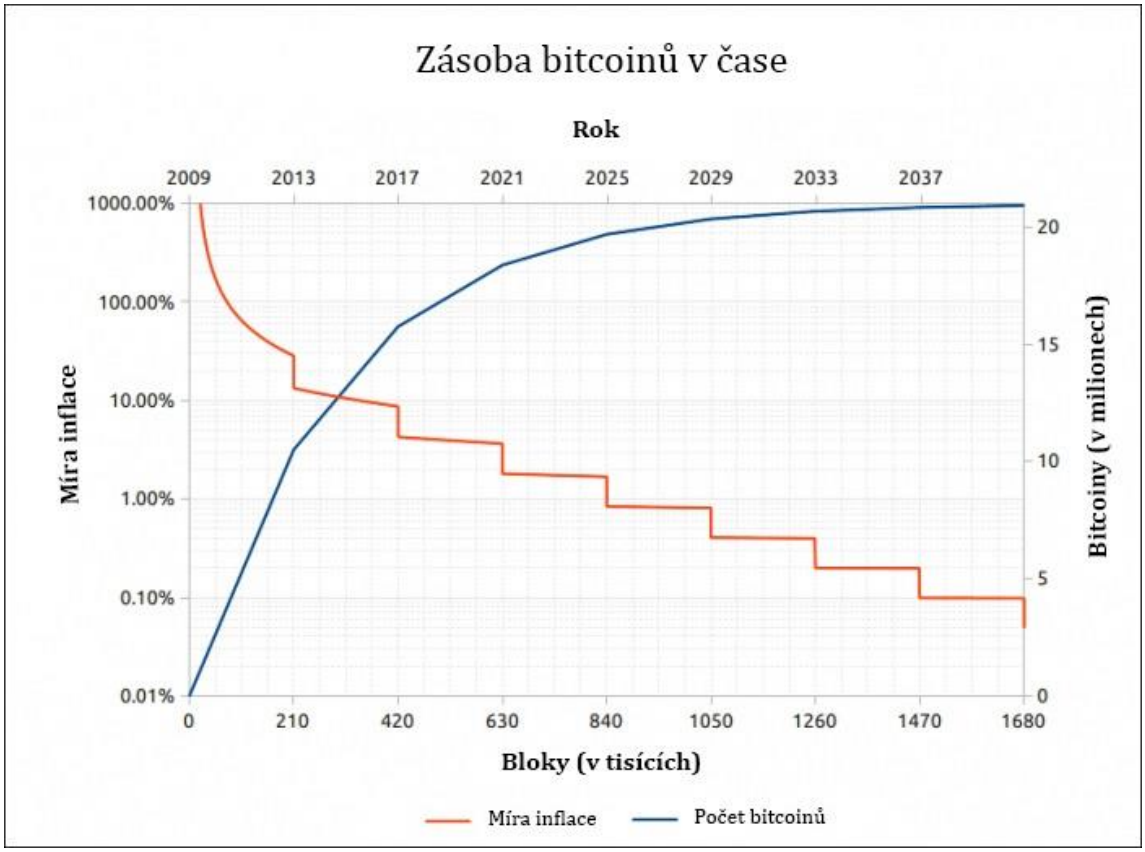
Je pak tedy na každém, zda chce pokoušet štěstěnu a těžit sám, nebo se připojit do společenství a mít jistou, ale nižší odměnu. Nicméně při dnešní obtížnosti je všem těžařům silně doporučeno sdružovat se do společenství, jelikož při sólovém těžení by na odměnu mohli čekat i v řádech let.

3.3.4 Odměny

Za těžení bloků jsou těžaři odměňováni dvěma způsoby. Novými mincemi, které jsou vytvořeny s každým novým blokem nebo transakčními poplatky, které jsou spojeny s těžením bloků. Čím více transakcí je zaznamenáno v blockchainu, tím více se také mění struktura těchto dvou odměn (tvorba klesá a poplatky stoupají).

Konečný počet vydaných bitcoinů byl stanoven Nakamotem již při vzniku systému. Je to tedy pro všechny známé číslo, které by mělo odpovídat 21 milionům mincí. Bylo předem stanoveno, že počet vydávání nových mincí bude kontrolován pomocí procesu zvaného půlení. Při vzniku systému byla frekvence vydávání nových bitcoinů 50 za blok, tedy 50btc/10 min. Za určitou dobu se počet vydaných bitcoinů za jeden blok sníží o polovinu. Tato doba však není určena časově, nýbrž počtem vytěžených bloků, a to konkrétně 210 000 bloky. Časově by tento počet měl odpovídat přibližně čtyřem rokům.

Graf 2 Zásoba bitcoinů v čase



(BitcoinClock, 2019)

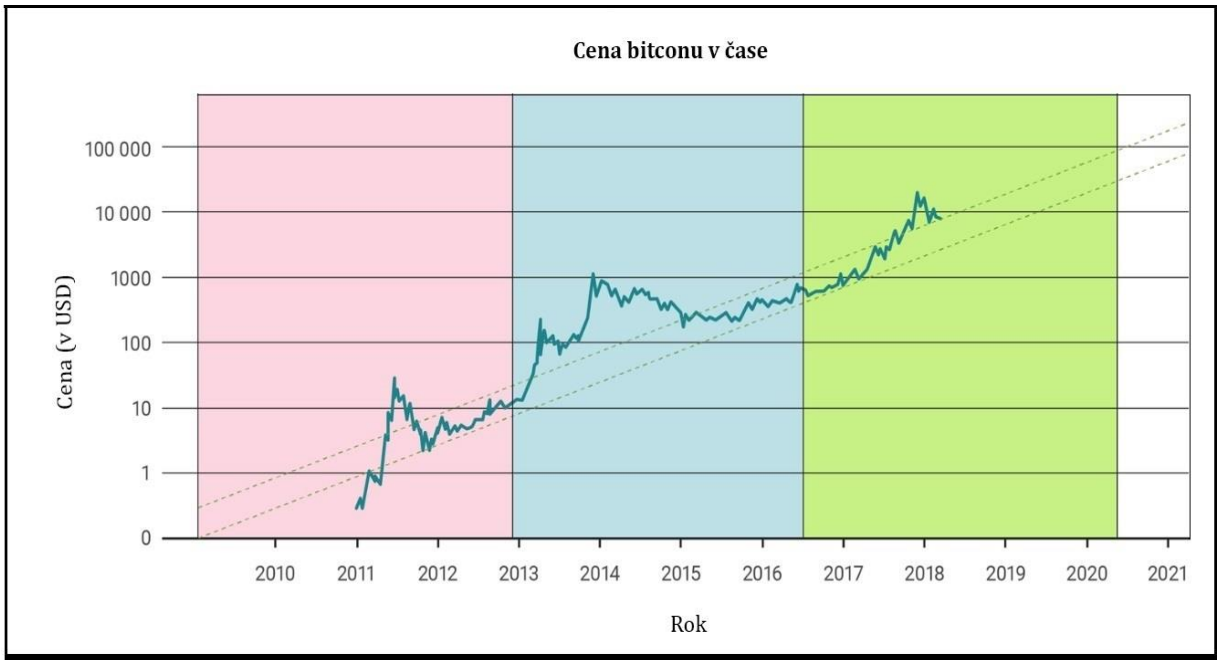
Se zvyšujícím se objemem bitcoinů v oběhu a stále se snižující odměnou za jejich těžení je třeba motivovat těžaře, aby nenastala situace, kdy by pro nikoho těžení nebylo nadále výhodné. Toho je dosahováno pomocí poplatků za transakce. Každá transakce tento poplatek může obsahovat, a to ve formě přebytku bitcoinů mezi vstupem a výstupem v dané transakci. V současnosti tyto poplatky představují asi půl procenta všech příjmů v rámci těžení. S postupem času se však poplatky budou přizpůsobovat tak, aby vynahradily příjmy snížené právě půlením. Po vytěžení posledního bitcoinu tak nastane

situace, kdy všechny příjmy z těžení bloků budou pouze z poplatků. (Antonopoulos, 2015)

Když byl Bitcoin v roce 2009 spuštěn, odměna za vytěžení jednoho bloku činila 50 bitcoinů, zatímco poplatky za transakce byly nulové. V roce 2012, kdy bylo v oběhu deset a půl milionu bitconů, se odměna za vytěžení zredukovala o polovinu na 25. Poplatek za jednu transakci v tomto období odpovídal průměrně 0,01 USD. Dnes činí odměna za vytěžení bloku 12,5 bitcoinu s průměrnou hodnotou 0,2 dolaru za transakci. Další snížení přijde v roce 2020, a to na 6,25 bitcoinu za blok. Tento trend by měl pokračovat až do roku 2140, kdy by měl být vytěžen poslední bitcoin. Už v roce 2030 by ale mělo být vytěženo přes 98% z celkového počtu bitcoinů. (BitcoinClock, 2019)

Vzhledem k tomu, že po každém půlení klesají výnosy těžařů o polovinu, dalo by se předpokládat, že pro řadu těžařů to bude znamenat značné snížení výnosnosti. Nicméně těžaři jsou na tuto událost připraveni a po každém půlení se cena přizpůsobí tak, aby těžení nadále zůstalo výnosné . Na grafu č.3 lze vidět, že po každém půlení nastupuje poměrně silný býčí trend. (BitcoinClock, 2019)

Graf 3 Cena Bitcoinu po půlení



(Ihodl,2019)

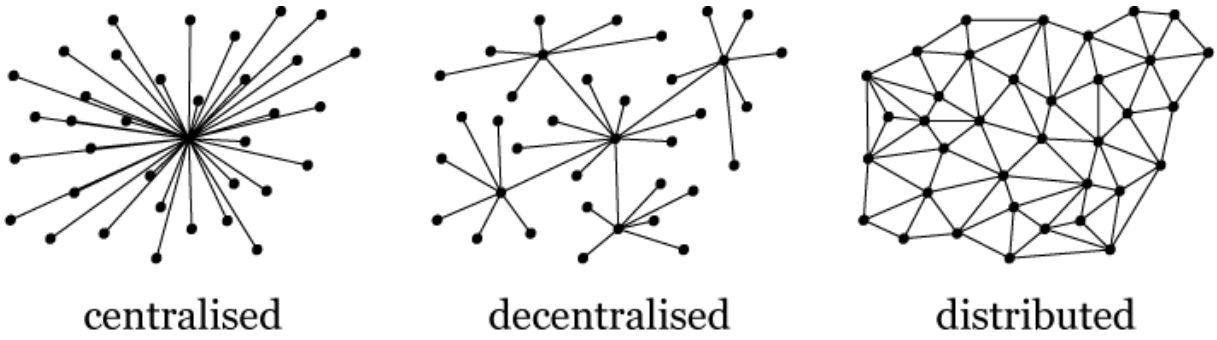
4 Blockchain

Blockchain je decentralizovaná, volně přístupná „účetní kniha", do které se zaznamenávají transakce, které v systému proběhly. Je to databáze, která je sdílená všemi síťovými uzly, aktualizovaná težaři a není nikým vlastněna ani kontrolována . (Swan, 2015)

Decentralizovaná databáze v tomto případě znamená, že neexistuje žádná centrální jednotka ani autorita, která by blockchain ovládala. Data se nešíří pouze z jednoho místa, ale jsou distribuovaná skrze síť uzlů (počítačů), které obsahují kopii blockchainu. V rámci sítě nelze nalézt takový uzel, jehož výpadek by znamenal kompletní odstavení sítě. Z tohoto důvodu je to zároveň databáze distribuovaná. (Narayanan, 2016)

Stojí za zmínku, že přestože blockchain vznikl jako decentralizovaná technologie, dají se dnes najít i centralizované blockchainy. Používají se zejména v mezinárodním finančním průmyslu pro obchodní transakce. Jedná se o soukromé či konsorciové blockchainy, které udělují přístup k transakcím pouze členům dané sítě či konsorcia. Obecně však převažuje názor, že používání těchto blockchainů je zbytečně nákladné a pro tyto účely je efektivnější využití současných standartních databázových systémů.

Obrázek 1 Centralizovaná, decentralizovaná a distribuovaná síť



(Commons, 2019)

Princip blockchainu není myšlenka nová, jeho základy by se daly najít v práci Habera a Stornetty z roku 1991. V jejich práci se zabývali metodou, jak zabezpečit časové označení vzniku digitálních dokumentů takovým způsobem, aby s těmito označeními nebylo možné zpětně manipulovat. Toho se snažili dosáhnout pomocí tzv. časového razítka. Jeho úkolem bylo poskytnout přibližnou představu o tom, kdy daný dokument vznikl. Pravděpodobně ještě důležitější je, že toto časové razítko přesně určovalo pořadí

vytvoření dokumentů. Pokud jeden dokument vznikl před druhým, časové razítko tuto skutečnost také odráželo. (Narayanan, 2016)

Původní koncept fungoval tak, že když server obdržel dokument, podepsal ho spolu s aktuálním časem. K této informaci pak byl také přidán odkaz (link) na dokument předcházející. V pozdější verzi pak byl přidán návrh jak systém zefektivnit. Místo aby se každý dokument podepisoval samostatně, začal se vždy určený počet dokumentů shromažďovat do bloků, které pak odkazovaly na bloky předcházející. Tímto se vytvořil řetězec bloků. V rámci bloků na sebe dokumenty stále odkazovaly, ale za použití stromové struktury (místo předchozí lineární). Je vidět, že tento koncept představuje základní kostru současného blockchainu. (Narayanan, 2016)

Samotný blockchain je tvořen dvěma typy záznamů – transakcemi a bloky. Transakce představují data, která do databáze vkládají samotní uživatelé, nejčastěji jde o převody kryptoměny z jedné peněženky do druhé. Bloky jsou pak souborem těchto transakcí, které těžaři shromažďují a potvrzují. Vytvořené transakce se volně předávají mezi uzly v závislosti na tom, kdo je v síti právě připojen. (Finex, 2018)

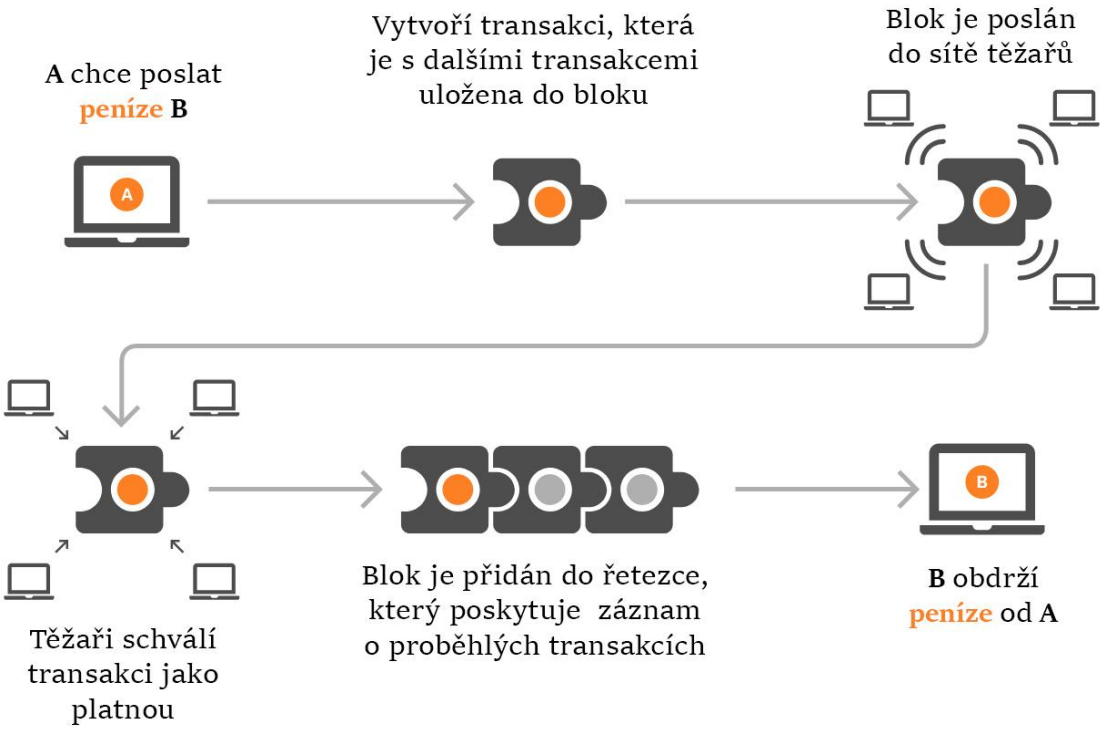
Aby transakce v rámci blockchainu mohla být považována za platnou, musí nejprve splňovat několik podmínek:

- Musí obsahovat platný elektronický podpis uživatele
- Musí být patrný pohyb v peněžence uživatele
- Musí splňovat další podmínky, jako je např. odměna pro těžaře

Po vytvoření transakce se těžaři snaží vytvořit blok, kterým se transakce potvrdí a zařadí do blockchainu. Tento blok se pak napojí na blok předcházející, čímž vznikne „řetězec bloků“ (od toho název blockchain).

Každý blok je vytvořen zhruba jednou za deset minut tak, aby průměr odpovídal šesti vytvořeným blokům za hodinu. Maximální možná velikost jednoho bloku je 1 MB, po jeho naplnění musí daná transakce počkat na vytvoření bloku dalšího. Všechny transakce je možné zpětně dohledat až k úplně prvnímu bloku celého blockchainu (tzv. Genesis bloku). (Nakamoto, 2008)

Obrázek 2 Průběh transakce v blockchainu



(Thompsonreuters, 2019)

4.1 Problém dvojité útraty

S příchodem digitálních měn se objevil problém, který je specifický právě pro ně a vůči kterému jsou kryptoměny zejména zranitelné. Jde o tzv. problém dvojité útraty.

Problém dvojité útraty je potenciální nedostatek kryptoměn nebo i jiných forem digitálních peněz, kdy tu samou digitální minci je možné použít na více než jednu transakci. To je možné z toho důvodu, že tato mince je tvořena digitálním souborem, který lze duplikovat nebo zfalšovat.

Při použití peněz v hotovosti nemůže tento problém nikdy nastat. Po zaplacení dané transakce opouštějí peníze naše fyzické vlastnictví a není tedy možné ty samé peníze použít při transakci další. V případě digitálních peněz v tradičních onlinových finančních systémech se využívá clearingové centrum, které ověřuje každou transakci a tento problém tudíž eliminuje. U kryptoměn ovšem nastává velký problém. Vzhledem k tomu, že decentralizace je jednou z předností systému, použití clearingového centra k ověřování transakcí by bylo přinejmenším kontraproduktivní.

Stojí za zmínku, že do příchodu blockchainu byla tato clearingová centra kryptoměnami skutečně využívaná. Nové systémy měli totiž pouze dvě možnosti – využít služeb těchto center, nebo se smířit s tím, že jejich systém bude existovat se zneužitelnou chybou, kvůli které eventuálně celý systém přijde o svou důvěryhodnost. Využití těchto center bylo zároveň velmi nákladné, jelikož bylo třeba zajistit, aby tato třetí strana byla pokud možno co nejvíce důvěryhodná. Často jimi tedy byly vlády, kreditní společnosti či banky.

Lze tedy vidět jak použití blockchainu a Peer-to-Peer sítě bylo pro fungování kryptoměn revoluční. Přestože je problém double spendingu v kryptoměnách díky blockchainu prakticky vyřešen, teoreticky by stále mohlo docházet k pokusům o duplikace.Tyto pokusy se nazývají útoky dvojité útraty. V současnosti stále existuje několik možností, jak by v blockchainu mohlo dojít k duplikaci jedné mince. Tyto útoky budou podrobněji rozebrány v praktické části této práce.

4.2 Vlastnictví a transakce

Vlastnictví Bitcoinu je zajištěno pomocí digitálních klíčů, bitcoinových adres a digitálních podpisů. Digitální klíče nejsou uloženy v síti, ale jsou vytvořeny a uloženy koncovým uživatelem, nejčastěji do jednoduché databáze známe jako *peněženka*. Klíče v peněžence jsou naprosto nezávislé na bitcoinovém protokolu a mohou být vygenerovány a spravovány peněženkovým softwarem, který nemusí mít přístup na internet ani k blockchainové databázi. (Antonopoulos, 2015)

4.2.1 Klíče

Aby bitcoinová transakce mohla být zaznamenaná do blockchainu, je potřeba platného digitálního podpisu, který ověřuje vlastnictví Bitcoinového účtu. Ten je možné vygenerovat pouze platnými digitálními klíči, které k danému Bitcoinovému účtu náleží. Ke každému účtu náleží právě dva klíče (někdy označované také jako adresy), a to soukromý a veřejný klíč. Soukromý klíč se používá k podepisování zpráv (v tomto případě transakcí) a veřejný klíč slouží k ověření, zda je tento podpis platný. (Antonopoulos, 2015)

Generování tohoto páru klíčů probíhá na základě kryptografie veřejného klíče (asymetrické kryptografie). Jako základ pro své šifrování používá Bitcoin kryptografii eliptických křivek. Pomocí této kryptografie se vytvoří pár klíčů, které umožňují přístup k bitcoinům. Mezi soukromým a veřejným klíčem existuje matematický vztah, díky kterému je umožněno generovat na zprávách (transakcích) platné digitální podpisy. Funkce jimiž je vygenerování klíčů zprostředkováno jsou jednostranné, což znamená že v případě odhalení veřejného klíče je prakticky nemožné z něho získat klíč soukromý (teoreticky to možné je, ale i dnešnímu nejvýkonnějšímu počítači světa by to trvalo miliardy let). (Mahler, 2018)

4.2.1.1 Soukromý klíč

Soukromý klíč je alfanumerické 256 bitů dlouhé číslo, které je obvykle vytvořeno v okamžiku založení peněženky. Lze si ho zjednodušeně představit jako PIN, kterým se při transakcích ověřuje vlastnictví Bitcoinového účtu. Je důležité si uvědomit, že soukromý klíč je v podstatě řetězec náhodně vygenerovaných znaků, které by si uživatel teoreticky mohl stanovit i sám. Softwarové programy generující tyto klíče jsou ale navrženy tak, aby stupeň náhodnosti vybraných znaků zajišťoval co možná největší ochranu před potenciálními útoky. Stupeň náhodnosti a unikátnosti daného klíče pak odpovídá kryptografické funkci použité k jeho vygenerování. (Khatwani, 2018)

V případě Bitcoinu se vlastnictví soukromého klíče rovná vlastnictví bitcoinů samých. Právě proto nesmí být za žádných okolností s nikým sdílen a mělo by se řádně dbát o jeho zabezpečení. Zároveň by měl být zálohován , neboť jeho případná ztráta znamená, že přístup k účtu je navždy ztracen, jakožto i všechny bitcoiny na něm se nalézající. (Antonopoulos, 2015)

Příklad náhodně vygenerovaného soukromého klíče:

5K1j6otY1i4SRdeDddFZX3MVHMjExCVkuPzVo2trKvQ99SUv2LF

4.2.1.2 Veřejný klíč

Stejně jako v případě soukromého klíče se jedná o alfanumerické číslo, které je však odvozeno právě z klíče soukromého. Toho je dosaženo pomocí znásobení na eliptické

křivce. Každý veřejný klíč má délku 256 bitů, ale po konečném hashi je jeho délka zredukována na 160bitů. Veřejný klíč je pak obvykle zastoupen bitcoinovou adresou.

Příklad veřejného klíče vygenerováného z předešlého soukromého klíče:

1ArEtYG3PnXKFbniuMAYMg8pueS6hUvAa

4.2.2 Adresa

Bitcoinová adresa je řetězec písmen a číslic, které slouží jako identifikátor při transakcích kryptoměn. Podobně jako při posílání e-mailů se při transakci posílají bitcoiny právě na jednu z adres příjemce. Adresy mohou být volně a bezplatně generovány jakýmkoli uživatelem Bitcoinu, a to i v případě, že uživatel nemá přístup k internetu ani k Bitcoinové databázi. To z toho důvodu, že Bitcoinová adresa není trvalá, měla by totiž sloužit jako identifikátor pouze pro jednu transakci. Na rozdíl od peněženek, na adrese nikdy nemůže být zůstatek. (Antonopoulos, 2015)

Adresa samotná sestává ze 26 až 35 znaků, začínajících na číslo 1 nebo 3, které označují použitou hash funkci při vygenerování adresy. Použité znaky mohou být jakékoli číslice a velká či malá písmena, s výjimkou velkého „O", malého „i", velkého "I" a čísla "0", to z důvodu zamezení nejasností. (Heilman, Baldimtsi, Goldberg, 2016)

Samotné vygenerování adresy je odvozeno z veřejného klíče uživatele. Pomocí hashing algoritmu SHA-256 se jednosměrnou funkcí z veřejného klíče získá výstup o libovolné velikosti. Následně je tento výstup použit v dalším hashing algoritmu RIPEMD160, který tento výstup převede na 160 bitů dlouhou, námi požadovanou adresu. (Antonopoulos, 2015)

Typické příklady převodu veřejného klíče na adresu mohou vypadat takto:

Adresa vygenerovaná pomocí P2PKH skriptu:

0c273679050900d7ccd20e2ec12bda20b0dada93d8864edcf7789f9b8e4b8d09

1NdvXKxxfM4up6MzynD9FiTFY5iVo6JaVR

Adresa vygenerovaná pomocí P2SH skriptu:

8462c59a79d16743a5f85e55daecad433206c65448f0a2b1a11932e517717da5

33bVpw5mjkS4pQBB2srXYU5xeRxhs89vmc

4.2.3 Peněženky

Peněženky slouží k ukládání privátních klíčů a zároveň k uskutečňování samotných plateb. Podle způsobu uložení lze peněženky rozdělit na několik druhů :

Softwarové peněženky - jde o peněženky, kde jsou privátní klíče a údaje ukládány v programech , na serverech či v digitálním prostředí

1. *Počítačové* - jde o počítačové programy, které ukládají měnu lokálně v počítači či notebooku. Všechny potřebné informace jsou pak tedy uloženy na hard disku počítače. Hlavní výhoda těchto peněženek je naprostá kontrola nad vlastní měnou, bez nutnosti být závislý na službách třetí strany. Na druhou stranu, jako nevýhoda se může jevit skutečnost, že veškeré zabezpečení je právě v rukou konečného uživatele. Právě proto se v některých případech přistupuje k takovému řešení, že se tyto peněženky ukládají na záložní počítače bez přístupu k internetu. (Guttmann, 2014)

2. *Webové/Online* – jedná se o peněženky, kde jsou informace a klíče uložené na webové stránce poskytovatele Bitcoinových služeb. Přístup k nim jde získat odkudkoli, z jakéhokoliv zařízení a zároveň mohou být propojeny s počítačovými peněženkami. Jedná se o nejčastěji využívanou peněženku, alespoň co se týče menších obnosů. Zatímco tedy přístupnost a rychlost jsou nespornými výhodami těchto peněženek, za nevýhodu oproti ostatním lze určitě považovat to, že klíče jsou uloženy v úložišti třetí strany. Konečný uživatel si tedy musí být při výběru poskytovatele jistý o jeho důvěryhodnosti a stupni zabezpečení. (Guttmann, 2014)

3. *Mobilní* – jde o aplikaci, která je nainstalována na mobilním telefonu. Mobilní peněženky mohou mít dvě formy. První ukládá mince lokálně v telefonu a tudíž poskytuje stejné výhody a nevýhody jako počítačové peněženky. Druhá využívá jako úložnu online servery, ke kterým skrze aplikaci získává přístup. Tato forma má tedy výhody a nevýhody shodné s webovými peněženkami. (Guttmann, 2014)

Hardwarové peněženky – jde o peněženky, kde jsou privátní klíče a údaje ukládány na konkrétní fyzické nosiče

1. *Hardwarová peněženka* - je zvláštním typem bitcoinové peněženky, která ukládá privátní klíče do hardwarového zařízení speciálně vytvořeného právě k tomuto účelu. Mohou mít formu např. bitcoin „kreditních karet", kovových peněženek využívajících technologii Bluetooth, nebo USB zařízení ne nepodobných flash diskům . Oproti softwarovým peněženkám mají řadu výhod, např. odolnost vůči počítačovým virům nebo otevřenost zdrojového kódu, díky kterému lze celou činnost zařízení ověřit. (Tuwiner, 2019)

2. *Papírová peněženka* - další možností, jak ukládat bitcoiny, je takzvaná papírová peněženka. Jde o prosté vytisknutí údajů na papír, který je pak uschován na bezpečné místo. Papírové peněženky obvykle ukládají klíče dvěma způsoby – jako 2D barcode a 58 číselný zápis. Jedná se o nejbezpečnější způsob úschovy, samozřejmě za předpokladu, že místo uložení je opravdu dobře zabezpečené. (Narayanan, 2016)

Obrázek 3 Papírová peněženka

(CoinCube, 2019)

5 Výhody a nevýhody

Zpočátku čelil Bitcoin spoustě kritiky z celého světa a některými byl dokonce považován za podvod kvůli několika negativním faktorům. S postupem času a zvyšující se úrovní porozumění technologii, na kterých Bitcoin funguje (zejména blockchainu), se začaly kryptoměny vnímat daleko více pozitivně a začaly se odhalovat jejich přednosti. Oproti standartním peněžním systémům má mnoho výhod, jako každý systém má ale i své nevýhody.

Výhody:

1. **Anonymita –** jednou z největších výhod Bitcoinu je schopnost obrany proti krádežím skrze anonymitu. Díky Bitcoinu je možné zachovat si při transakcích skrytou identitu a být zastoupen pouze veřejnou adresou, která žádné personální údaje neposkytuje. Z veřejné adresy by nemělo být možné získat jakoukoli informaci o tom, kdo je skutečným vlastníkem bitcoinů, potažmo bitcoinové peněženky.
2. **Rychlost a globálnost –** oproti bankovním převodům jsou transakce v rámci Bitcoinu opravdu velmi rychlé. Jakmile je transakce odeslána, je okamžitě obsažena v síti a následně v řádu desítek minut i potvrzena. Vzhledem ke globální povaze sítě je lokalita odkud je transakce odesílána nepodstatná, jelikož doba potvrzení transakce bude vždy stejná.
3. **Nízké poplatky** – v porovnání s klasickými elektronickými převody má dnes Bitcoin nízké poplatky. V současnosti je průměrná hodnota poplatku 0,2 USD za každý převedený bitcoin, zatímco u klasických převodů může poplatek někdy dosahovat až 5% z odesílané částky.
4. **Transparentnost** – všechny proběhlé transakce je možné v blockchainu zpětně dohledat a je tak možné zjistit tok každé mince. Zároveň je ale chráněna identita účastníků dané transakce, jelikož jsou reprezentováni pouze jejich veřejnou adresou
5. **Bezpečnost a kontrola** – díky tomu, že uživatelé mají kontrolu a veškeré informace o svých transakcích, je pro uživatele systém bezpečnější a důvěryhodnější. Prodejci si nemohou účtovat žádné další poplatky, protože v síti jsou všechny informace veřejné a dostupné. Anonymní povaha transakcí pak zajišťuje ochranu proti krádežím identity. Technologii Bitcoinu je také skoro

nemožné prolomit. Privátní klíče jsou prakticky nemožné útočníky odhalit, pokud samozřejmě nedojde k pochybení při zajištění jejich ochrany.

6. **Dělitelnost** – schopnost Bitcoinu rozdělit každou minci na extrémně malé částky (až na jednu miliontinu). Umožňuje tak mikroplatby, které současné elektronické peněžní systémy nedovolují

Nevýhody:

1. **Nenávratnost –** jakmile je transakce odeslána, je nemožné jakýmkoliv způsobem dostat prostředky zpět. Z hlediska prodejců může jít o kladnou vlastnost, jelikož po odeslání platby si mohou být jistí, že za produkt či službu obdrží platbu. Z pohledu odesílatele jde ale o poměrně nepříjemnou záležitost, kdy si musí být vždy naprosto jistí, že adresa, na kterou je platba odesílána, je správná.
2. **Volatilita –** cena u Bitcoinu je vysoce volatilní a zvyšuje či snižuje se v ohromných řádech. To je výhodné spíše pro spekulanty, kteří se toho snaží využít, nicméně pro investory je toto poměrně riskantní vlastnost, která brání plnému využití Bitconu jako investičnímu prostředku.
3. **Nedostatek povědomí a míst akceptujících Bitcoin –** přestože je možné se s kryptoměnami setkávat už skoro deset let, počet lidí, kteří jim rozumí a využívají, je stále poměrně nízký. V návaznosti na to, i počet míst akceptující Bitcoinové platby je stále nízký, což zpomaluje jeho vývoj. Alespoň trend růstu je pozitivní, jelikož počet těchto míst stabilně, ačkoli velmi pomalu stoupá.
4. **Černý trh –** původně byl Bitcoin ve velkém využíván na černém trhu pro praní špinavých peněz, kde díky anonymní povaze plateb mohli lidé provozující nelegální činnosti dostávat zaplaceno. Ačkoli jsou tyto dny z velké části pryč, u některých lidí stále tato negativní konotace zůstává. Na druhou stranu, možnost použití kryptoměn jako prostředku pro platby za nelegální činnosti v určité formě přetrvala.
5. **Nejistý vývoj –** kryptoměny jsou stále záležitost poměrně nová a Bitcoin i všechny ostatní se dále vyvíjí. S ohledem na jejich dosavadní vývoj, vysokou volatilitu a další problémy je tak nemožné říct, zda další rozvoj bude pozitivní nebo negativní.

6 Praktická část

Cílem praktické části je zjistit, jakou roli hraje bezpečnost a anonymita v rámci Bitcoinového systému a určit současné potenciálně nejvíce nebezpečné útoky.

Praktická část bude rozdělena do tří částí – dotazníku, analýzy potenciálních útoků a příkladů konkrétních provedených útoků.

Pomocí dotazníku budu zjišťovat, jak je česká veřejnost seznámena s Bitcoinem. Budu se ptát zda vůbec ví o co se jedná, jestli znají jeho hodnotu nebo jestli ho někdy použili. Dále se budu ptát co považují za největší nevýhody Bitcoinového systému. Chci zjistit, jak je důležitost bezpečnosti systému vnímána jak lidmi, kteří o Bitcoinu jen slyšeli, tak i lidmi s Bitcoinem více seznámenými. Na základě těchto dat pak také chci určit, do jaké míry ovlivňuje bezpečnost a způsoby jejího narušení hodnotu Bitcoinu.

V rámci analýzy potenciálních útoků chci zjistit jaká možná narušení bezpečnosti existují, a jestli představují opravdové nebezpečí pro fungování systému. Útoky rozdělím podle způsobu jejich provedení, a to na útoky zaměřující se na Proof-of-Work algoritmus a na útoky spojené s obchodováním Bitcoinů. U každého útoku bude rozebrán způsob jeho provedení, zasažené subjekty, následky a možné způsoby jeho prevence. Na základě zjištěných informací chci určit potenciálně nebezpečné útoky narušující Bitcoinový systém.

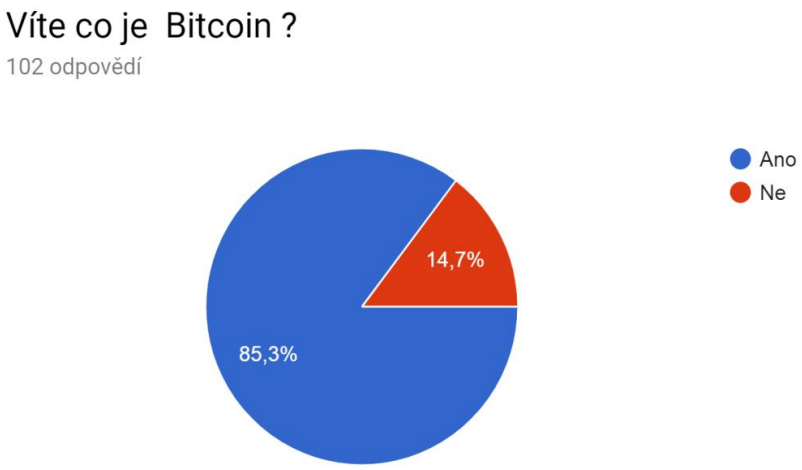
V poslední části chci rozebrat několik skutečně provedených útoků na Bitcoin. Vyberu útoky, které byly do počtu ukradených Bitcoinů co největší, aby bylo patrné, jaký efekt mají na hodnotu Bitcoinu. Dále u těchto útoků proberu způsob jejich provedení a pokusím se určit, jaké typy útoků byly v praxi skutečně úspěšně provedeny Výstupem by pak mělo být zjištění, kde je v Bitcoinu nejslabší místo co se bezpečnosti týče.

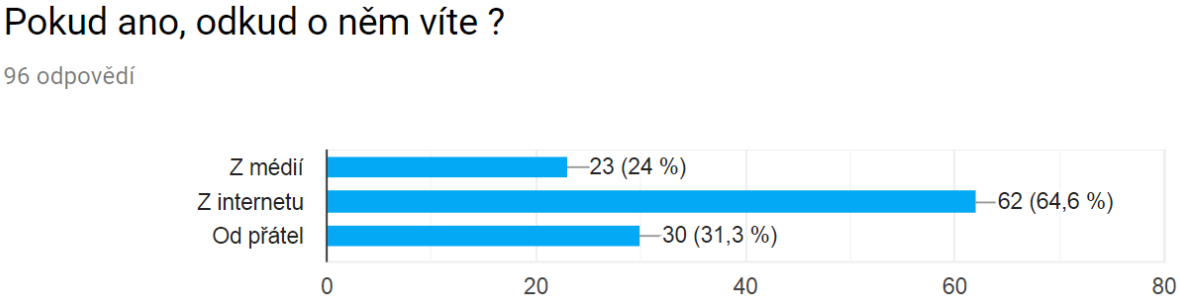
6.1 Dotazníkové šetření

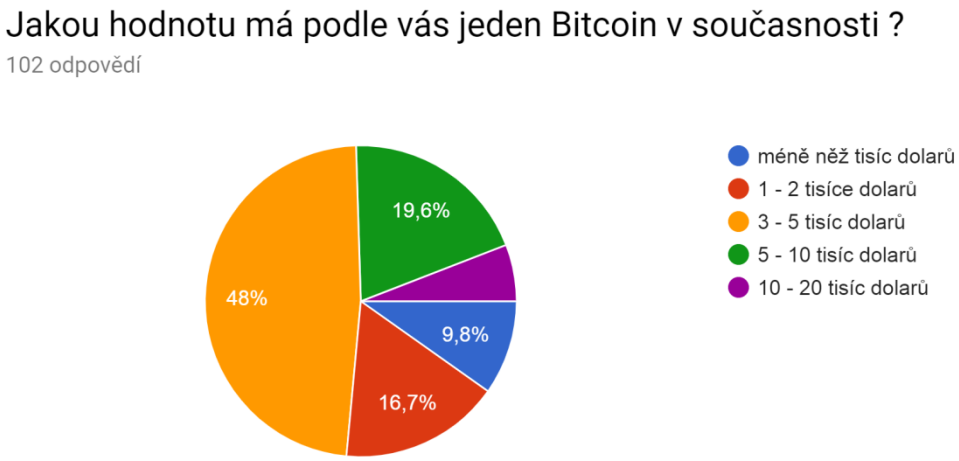
Jako první část praktické části jsem vytvořil dotazník, jehož cílem bylo stanovit do jaké míry hraje bezpečnost roli pro potenciální (i reálné) používání Bitcoinu širší veřejností. Dotazník byl strukturován do tří částí podle předmětu otázek. První část se zaměřovala na obecné znalosti o Bitcoinu, druhá část pak na bezpečnost a výhody a nevýhody spojené s Bitcoinem. Poslední částí byly identifikační otázky, na jejichž základě jsem jednu z otázek rozebral ještě podrobněji.

1. část

Hlavním cílem první části dotazníku bylo zjistit, do jaké míry je česká veřejnost s Bitcoinem seznámena, zda zná jeho hodnotu nebo ho i využívá.





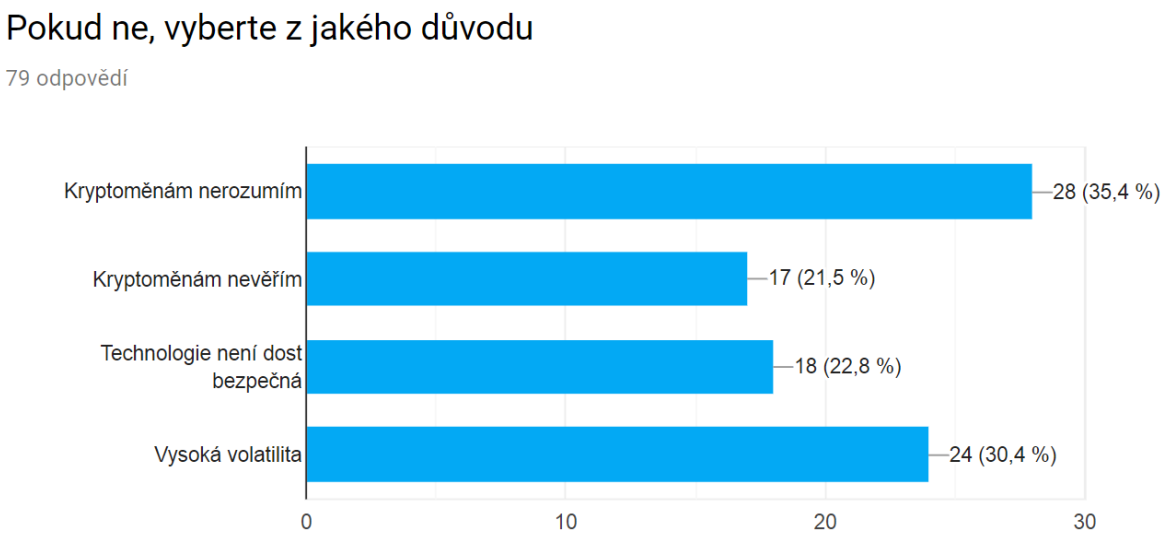


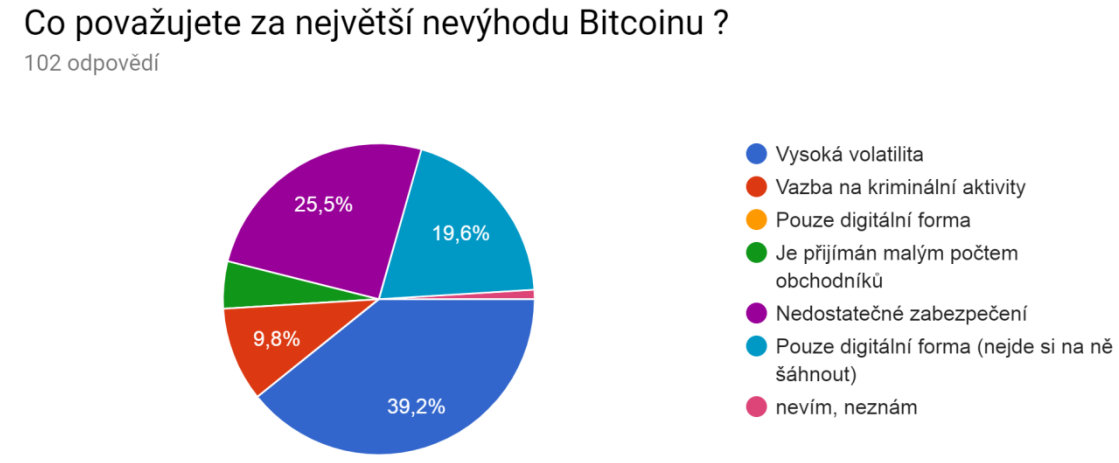
Z výsledků lze vidět, že většina respondentů má určité povědomí o tom co Bitcoin je, nicméně pouze 19% ho někdy vlastnilo či použilo. Nejčastějším zdrojem informací je podle očekávání internet, následován přáteli a médii. Zajímavým zjištěním je, že většina lidí zná současnou hodnotu Bitcoinu, která se v současnosti pohybuje na hranici 4 tisíc dolarů. To je pro mě překvapení, jelikož dnes se již o Bitcoinu nemluví tolik, jako v dobách jeho největšího růstu (2017-2018), kdy člověk o Bitcoinu slyšel na každém kroku a jeho cena dosahovala až 20 tisíc dolarů. Druhá část dotazníku by nám měla poskytnout lepší informace o tom, z jakých důvodů jsou lidé váhaví k použití Bitcoinu.

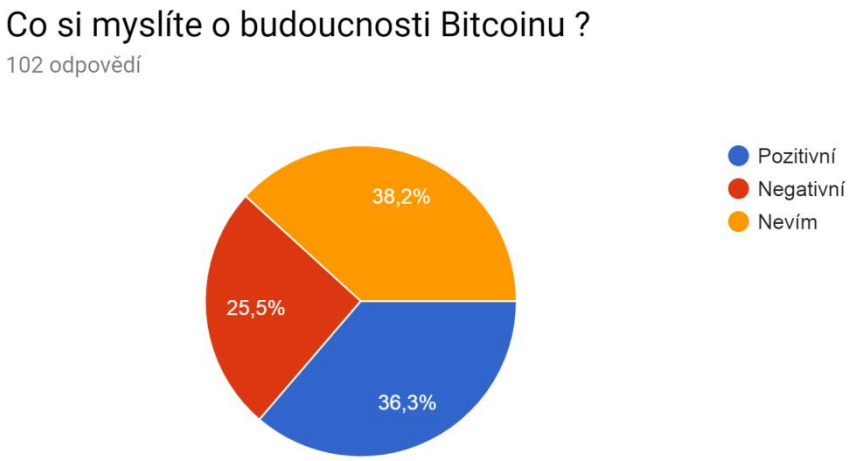
2. část

V druhé části dotazníku jsem se zaměřil na otázky s problematikou bezpečnosti a anonymity. Hlavním cílem bylo určit, zda jsou kryptoměny považovány za bezpečné a pokud ne, tak z jakých důvodů. Dále jsem se ptal, jestli je anonymita brána jako výhoda

či nevýhoda, vzhledem k tomu, že je na ni možno nahlížet z obou úhlů. Nakonec jsem se zeptal, co si respondenti myslí o budoucnosti Bitcoinu.





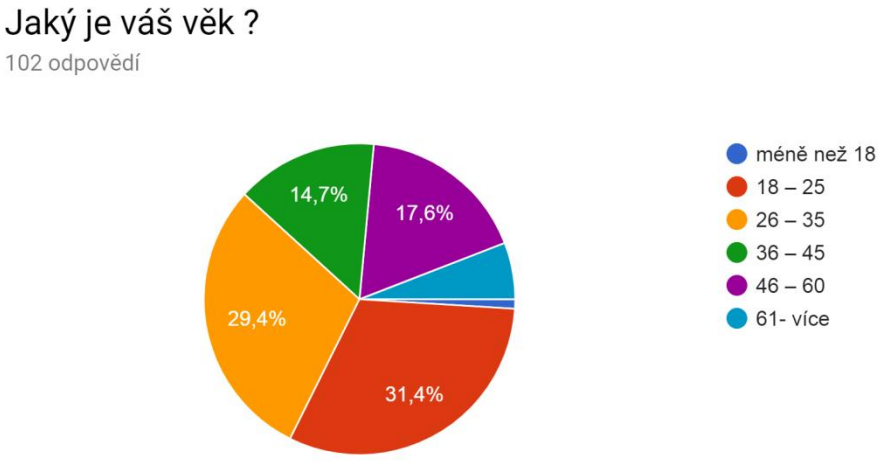


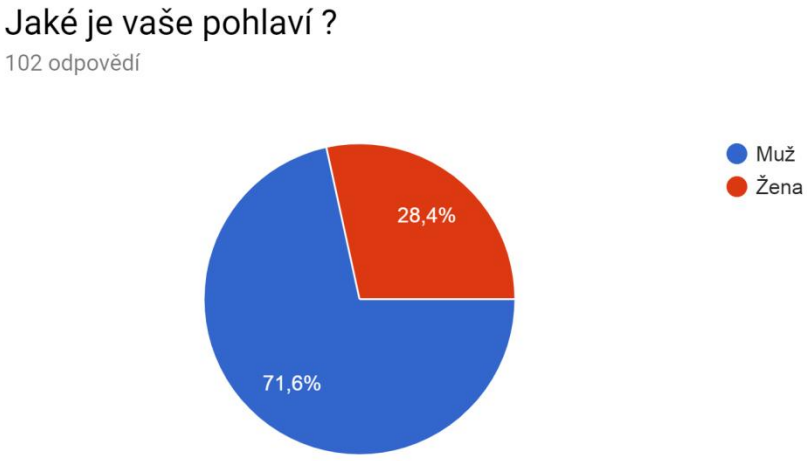
Z odpovědí vyplývá, že většina respondentů nepovažuje kryptoměny za bezpečný investiční nástroj. Jako nejčastější důvod je pak uváděno, že kryptoměnám nerozumí. Dalšími důvody jsou pak vysoká volatilita a nedůvěra v bezpečnost technologie. Pokud tedy vezmeme v úvahu respondenty, kteří Bitcoinu do určité míry rozumí, pak jsou pro ně volatilita a bezpečnost největšími překážkami. Pokud přejdeme k další otázce, kde se ptám na nevýhody celého systému, pak volatilita je na první pozici s 39%, následována zabezpečením s necelými 26 %. Zvážíme-li skutečnost, že vysoká volatilita je jedním z důsledků, které následují po prolomení bezpečnosti systému, můžeme řict, že bezpečnost je jedním z hlavních důvodů nedůvěry v Bitcoin. Ohledně anonymity panuje mezi respondenty menší nerozhodnost, nicméně 56% ji považuje jako výhodu. Osobně jsem očekával vyšší hodnotu, ale tato nižší hodnota nejspíše proudí z přetrvávajícího spojování Bitcoinu s kriminálními aktivitami . Podobná situace nastala i u otázky

týkající se budoucnosti Bitcoinu, kde nejčastější odpověď byla nevím, následovaná pozitivní a negativní.

3. část

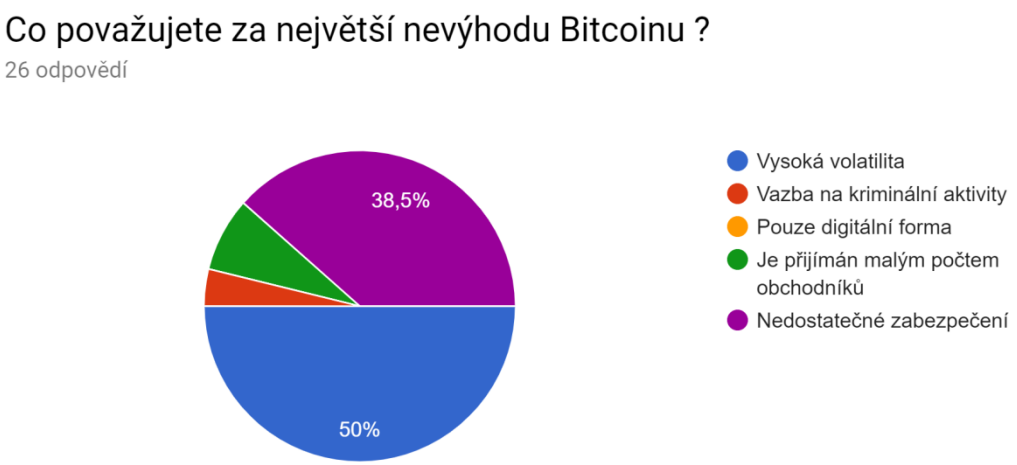
Poslední částí dotazníku byly identifikační otázky.





Věková struktura respondentů byla poměrně rozmanitá a v rámci průzkumu tak byly reprezentovány všechny věkové skupiny. Nejčastější pak byli respondenti ve věku od 18-25 let, následovaní respondenty ve věku od 26-35 let. Respondenty byli nejčastěji muži, konkrétně odpovědělo 74 mužů z celkových 102 respondentů. Nejčastějším nejvýše dosaženým vzděláním pak bylo střední, následované vysokoškolským.

Na základě informací o struktuře respondentů jsem se rozhodl otázku týkajících se nevýhod Bitcoinu rozebrat podle nejvyššího dosaženého vzdělání. Konkrétně mě zajímá, jak na tuto otázku odpovídali vysokoškolsky vzdělaní respondenti. Očekávám totiž, že vysokoškolsky vzdělaní lidé mají s Bitcoinem lepší zkušenosti, a získám tak lepší informace o tom, co je bráno jako největší překážka pro používání Bitcoinu.



Jak si lze všimnout, zcela zmizela odpověď „Bitcoinu nerozumím“ a zvýšilo se procento odpovědí zahrnujících volatitlitu a bezpečnost. Celá polovina respondentů jako největší nevýhodu uvádí vysokou volatilitu a skoro 39% potom nedostatečné zabezpečení. Z odpovědí tedy vyplývá, že volatilita spolu s bezpečností tvoří jedny z hlavních problémů systému. Dále bych se tedy měl také zaměřit na otázku, zda existuje vztah mezi volatilitou a bezpečností.

6.2 Analýza potenciálních útoků

Z předcházející části vyplývá, že bezpečnost je jedním z hlavních problémů, které by uživatelé měli se systémem. Proto jsem se rozhodl provést analýzu potenciálních útoků, které by mohli nějakým způsobem ohrozit bezpečnost Bitcoinového systému. Tyto útoky jsem rozdělil do dvou kategorií, a to - útoky cílící na Bitcoinový systém a útoky cílící na infrastrukturu spojenou s Bitcoinem. První kategorie pojednává především o útocích spojených s dvojitou útratou, které jsou specifické právě pro kryptoměny. Druhá kategorie pak řeší útoky spojené především s obchodováním kryptoměny. U každého útoku bude rozebrán jeho postup, pravděpodobnost jeho uskutečnění a možné způsoby prevence. Poté bude sestavena tabulka shrnující všechny informace. Cílem je určit, zda nejčastější praktické útoky, narušující stabilitu, mají svou podstatu v Bitcoinovém systému či v infrastruktuře s ním spojené. Na závěr budou rozebrány tři konkrétní útoky na Bitcoin, a to z hlediska použitých útoků a cenových dopadů.

6.2.1 Útoky cílící na Bitcoinový systém

Tato část rozebírá útoky přímo cílící na Bitcoinový systém. Zejména jde o útoky spojené s Proof of Work protokolem a se způsoby, jakými jsou v síti šířeny transakce. Jde tedy o útoky cílené na základní stavební kameny celého systému.

6.2.1.1 Většinový útok / útok 51%

Jedná se o útok na blockchain, kdy těžař či skupina těžařů kontroluje více než 50% výpočetního výkonu celé sítě (hashrate). V takovém případě by útočník byl schopen zabránit schvalování nových transakcí. Také by bylo možné, aby zvrátil transakce, které byly uskutečněny, zatímco měl nad sítí kontrolu. Právě díky tomu by pak byl schopen duplikovat mince. Nemohl by však změnit bloky vytvořené a schválené před tímto útokem, a ani by nemohl vytvářet mince nové. (Vijayakumaran, 2018)

V normální situaci, kdy těžař vytvoří platný blok transakcí, odešle ho zbytku těžařů v síti. Ti potom ověří platnost bloku, v důsledku čehož dojde ke konsensu o současném stavu blockchainu. Nicméně těžař, který má k dispozici více než 50% výpočetního výkonu sítě může začít těžit soukromě. Jeho těžba probíhá ve stejném mempoolu (místo, kde transakce čekají na vyřízení) jako ostatních, nicméně transakce zahrnuté

v těchto soukromě vytěžených blocích nejsou zveřejněny zbytku sítě. Výsledkem je pak situace, kdy zbytek sítě těží na základě veřejné verze blockchainu, zatímco náš „dominantní" těžař pracuje na své vlastní verzi, kterou zbytku sítě nezpřístupňuje.

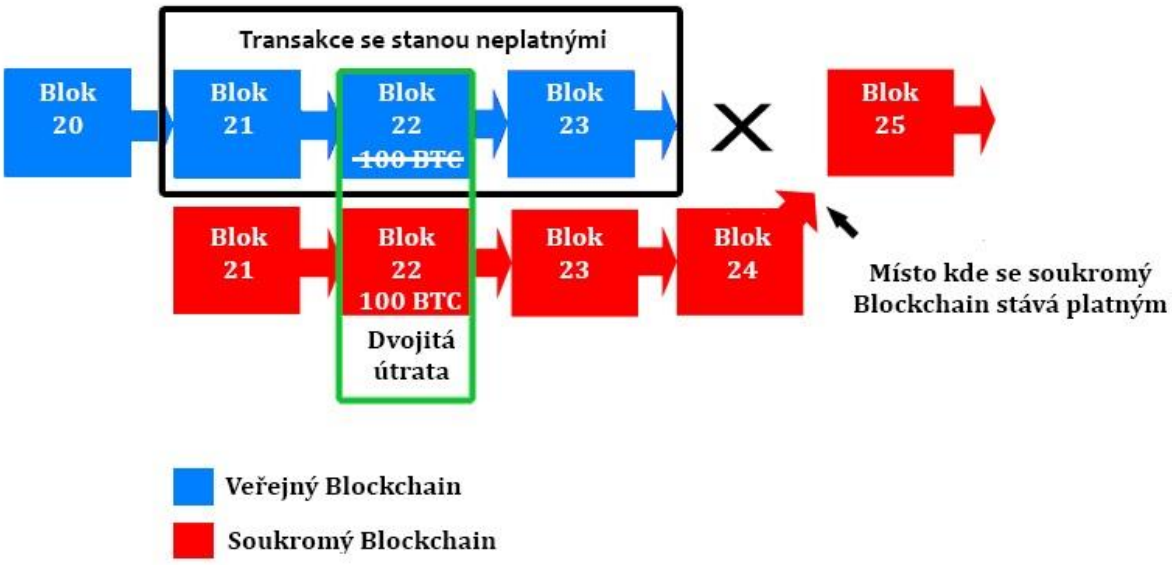
Vzhledem k tomu, že dominantní těžař má více výkonu než zbytek sítě, je také schopen vytvářet bloky rychleji než ostatní a eventuálně tím dosáhnout delšího blockchainu. Na základě pravidla o nejdelším řetězci pak dojde k tomu, že tento soukromý blockchain je automaticky brán jako blockchain platný. Zbytek těžařů je pak na tuto větev blockchainu donucen přejít.

K dvojité útratě by pak došlo konkrétně tak, že dominantní těžař by utrácel své mince na veřejné verzi blockchainu, zatímco do své soukromé verze by tyto transakce nazahrnoval. Následně v momentě, kdy by jeho soukromý blockchain byl uznán za platný, transakce které proběhly ve veřejném blockchainu by se staly neplatnými a zůstatky peněženek by odpovídaly soukromému (nyní platnému) blockchainu.

Pokud uvážíme, že těžaři se dnes ve valné většině sdružují v uskupeních (z důvodu rentability), je možnost tohoto útoku reálnější než kdy dříve. Nicméně potenciální škoda, kterou by takovýto útok způsobil, by i tak nebyla pro měnu likvidační, přestože by pravděpodobně způsobil rozsáhlou paniku a pokles hodnoty. Pro zajímavost, náklady na dosažení takového výpočetního výkonu aby mohlo dojít k úspěšnému většinovému útoku, za předpokladu využití nejefektivnějších těžařských technologií a nejlevnější elektrické energie, by i tak vycházely na závratných 1,4 miliardy dolarů.

Přestože tento útok nebyl dosud nikdy proveden je důležité počítat s jeho možností a dále způsoby, jakými by se mu dalo předejít. Jednou z nejdůležitějších činností je důsledné sledování sítě. Mining pooly by měly být monitorovány a abnormální růst některého z nich by měl být komunikován se zbytkem sítě. Pokud by nastala reálná možnost, že by k tomuto útoku mohlo dojít, měly by do systému být implementovány nástroje, které by uživatele demotivovaly od těžení ve velkých uskupeních.

Obrázek 4 Většinový útok / Útok 51%



(Swahilpages, 2019)

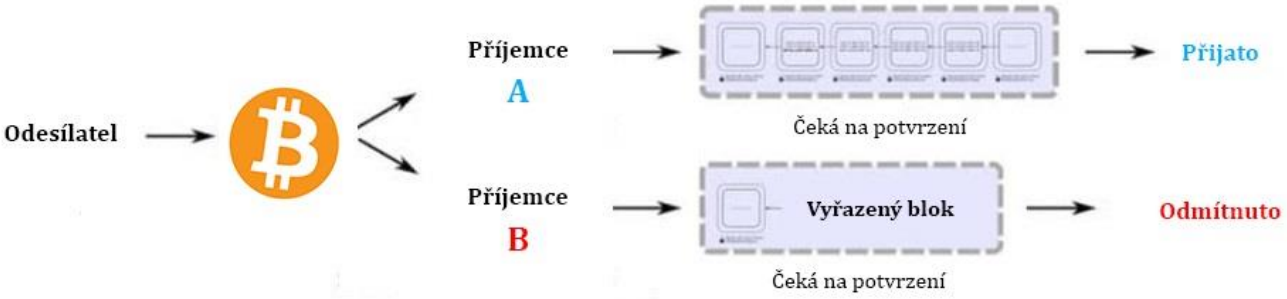
6.2.1.2 Race útok

Druhým možným způsobem, jak by teoreticky mohlo dojít k dvojité útratě jedné mince je tzv. race attack - závod. Ten probíhá tak, že odesílatel pošle v rychlém sledu tu samou minci na dvě různé adresy s vědomím, že pouze jedna z těchto transakcí bude schválena. Odesílatel tedy pošle jednu minci na adresu příjemce (prodávajícího) a zároveň na jednu ze svých adres s nadějí, že první transakce (přijemci) bude stornována. Obě tyto transakce přijdou do fondu nepotvrzených transakcí, kde čekají na schválení těžařů. V případě, že těžaři jednu transakci ověří před druhou, je pak zahrnuta do dalšího bloku, zatímco druhá transakce je sítí shledána jako neplatná. Pokud těžaři přijmou obě transakce zároveň, tak transakce s více potvrzeními bude přijata, zatímco druhá bude vyřazena. (Kaushik, 2017)

Příjemce, který nečeká na potvrzení této platby pak má 50% šanci, že dostane tuto dvakrát utracenou minci (a peníze nakonec neobdrží). V rámci Bitcoinu je všem prodejcům doporučeno, aby počkali na minimálně 1 potvrzení transakce, a optimálně na 6 před tím, než platbu přijmou. Jedno potvrzení v tomto případě znamená, že po vytvoření transakce byl do blockchainu přidán další blok zahrnující tuto transakci. Šest bloků je pak matematicky vytyčená minimální hranice, kdy s danými transakcemi nelze

zpětně manipulovat. Pokud příjemce obdrží minimální počet potvrzení, může si pak být jistý, že se jedná o legitimní transakci.

Obrázek 5 Race útok



(Coinsutra, 2019)

6.2.1.3 Finneyho útok

Pojmenován po Halu Finneym (prvnímu příjemci bitcoinové transakce), který tento útok v roce 2011 navrhl. Jedná se o variaci na race útok.

Útočník vytvoří dvě transakce – v jednom případě posílá bitcoin prodejci a v druhém sám sobě. Transakce ale zatím neodesílá do sítě, místo toho se snaží soukromě vytěžit blok, kde je zahrnuta druhá transakce. Pokud se mu tento blok podaří vytěžit, rychle uskuteční nákup pomocí první transakce a získá zboží nebo službu, za kterou zdánlivě zaplatil. Následně odešle svůj předtěžený blok síti, v důsledku čehož je první transakce zrušena (přestože byla odeslána zbytku sítě).

Tento způsob útoku je daleko složitější než obyčejný race útok, jelikož vyžaduje vytěžení konkrétního bloku (což je dnes náročné jak časově tak finančně). Na druhou stranu je to útok nezjistitelný a to až do doby jeho uskutečnění. Jediný způsob obrany proti takovému útoku je tak vyžadování alespoň jednoho potvrzení transakce.

6.2.1.4 Brute Force útok

Obecně, brute force útok či útok hrubou silou je takový útok, který na prolomení systému využívá metodu pokusu a omylu. Zahrnuje totiž vyzkoušení každé možné kombinace znaků či dat k nalezení správného klíče, pomocí které pak zprávu

dešifruje.V praxi se tedy jedná o systematické testování všech možných kombinací, za účelem nalezení příslušného klíče k napadenému účtu.

Pokud by se v rámci Bitcoinu jednalo o tento útok, lze si jej představit tak, že by se útočník snažil získat privátní klíč od Bitcoinové peněženky, který by mu umožňoval přístup k bitcoinům. Toho by se samozřejmě snažil docílit za pomoci softwaru, který by systematicky generoval vstupy. Aby bylo možné provést úspěšný brute force attack na privátní klíč, bylo by třeba vyřešit 2^256 operací (jelikož klíč je 256 bitů dlouhý). Pro představu je níže uvedeno toto číslo v celém rozsahu.

$$2^{256} = 115792089237316195423570985008687907853269984665640564039457584007913129639936$$

Pravděpodobnost nalezení kolize je tedy 1 ku 2^256 u každého vygenerovaného vstupu. Průměrný počet pokusů na uhodnutí jednoho klíče je 2^128. Současný nejvýkonnější superpočítač by byl za optimálních podmínek schopen vygenerovat zhruba 10,51x10^11 pokusů za sekundu. Při takovém výpočetním výkonu by průměrná doba na uhodnutí jednoho privátního klíče činila asi 1 miliardu let. Ačkoli tak tento způsob útoku není matematicky nemožný, z hlediska pravděpodobnosti by šlo o pokus absurdní. Také by šlo o útok neefektivní, jelikož člověk s dostatečným výkonem na úspěšný útok by si vydělal nepoměrně více, kdyby ho použil na jiné činnosti jako je třeba těžení bloků. Doba potřebná na uskutečnění úspěšného útoku se ale bude samozřejmě pořád snižovat, a to úměrně Moorovu zákonu, který říká že výpočetní výkon se každé dva roky zdvojnásobí. Pokud by tento zákon platil, průměrný počítač by dokázal (při současném zabezpečení Bitcoinu) provést úspěšný brute force attack, už asi za 50 let.

Tento způsob brute force však není v rámci Bitcoinu jedinou možnou variantou. Další útok nazvaný Brute force attack představuje pokročilejší stupeň Finneyho útoku. Princip útoku spočívá v tom, že útočník ovládá určitý počet uzlů v síti, které společně a tajně těží bloky s cílem dvojité útraty. Útočník dosahuje dvojité útraty mince podobně jako v předchozím případě, tedy útratou mince ve veřejném blockchainu. Ve stejnou dobu ale pracuje na prodloužení větve svého privátního blockchainu, kterou eventuálně zveřejní celé síti. Vezměme tedy v úvahu, že prodejce je zkušený a před přijetím transakce čeká na určitý počet potvrzení, které mu potvrdí že jde o legitimní transakci.

Jakmile obdrží daná potvrzení, odešle produkt klientovi s vědomím, že za něj dostal zaplaceno. V tuto chvíli útočník, který

má předtěžené bloky odešle svou privátní větev do sítě a vzhledem k tomu, že bude delší než větev veřejného blockchainu, bude uznán jako blockchain platný. Důsledkem čehož pak bude transakce zrušena a obchodník platbu neobdrží. (Franco, 2015)

Lze si všimnout, že tento způsob útoku kombinuje jak útok 51% tak Finneyho útok. Z Finneyho útoku přebírá způsob, jakým je docíleno dvojité útraty i přes potvrzení transakcí, zatímco z 51% útoku pak potřebu určitého výpočetního výkonu potřebného k předtěžení bloků.

Potenciální škoda, kterou může tento útok způsobit, je značná. Cílem útoku by pravděpodobně byli směnárny či burzy, jelikož menší subjekty by z hlediska výnosnosti nebyli efektivní. Náklady na takový útok jsou totiž obrovské. Aby mohl být Brute Force útok považován za efektivní, tak by se získaná částka musela pohybovat v rámci milionů dolarů Nicméně právě proto by byla prevence proti Brute Force útoku velmi složitá. Jako jediný způsob obrany je možné uvažovat vyčkání na potvrzení transakce 6 bloky, po kterých už nelze s transakcí zpětně manipulovat.

6.2.1.5 Vector 76

Dalším způsobem útoku, který používá dvojitou útratu je Vector76. Nazván po uživateli, který tento hypotetický útok vymyslel a zveřejnil na fóru zabývajícím se kryptografickými technologiemi. Jedná se o další způsob útoku dvojité útraty, který by měl fungovat i v případě potvrzení transakce. Konkrétně se jedná o variantu, kdy cílem není jiný uživatel či obchodník, ale Bitcoinová směnárna. (Kaushik, 2017)

Zvláštností tohoto útoku je skutečnost, že operuje s globální povahou sítě. Pomocí pozorování způsobu jakým jsou transakce v síti šířeny je totiž možné stanovit nejbližší uzly k napadenému cíli (tedy nějaké Bitcoinové směnárně). Samotný útok pak funguje na myšlence, že síti jsou ve stejný okamžik odeslány dva různé validní bloky, z nichž ale pouze jeden bude nakonec blokem uznaným.

Jako v předchozích případech je potřeba mít k úspěšnému útoku předtěžený blok. Tento blok v sobě zahrnuje transakci obsahující poměrně velikou sumu, a to ve prospěch

Bitcoinové směnárny. Tato transakce je ve všech ohledech platná, není však zatím zahrnutá v právě těženém bloku veřejného blockchainu. Nicméně je ale zahrnutá v útočníkově předtěženém bloku. Jakmile má útočník předtěžený blok, zahrnující tuto transakci, pak čeká než bude další (veřejný) blok vytěžen někým jiným. V momentě, kdy je veřejný blok vytěžen, je zároveň s ním odeslán i útočníkův blok, a to do uzlů nejbližších Bitcoinové směnárně. Pokud směnárna uvidí tento blok dříve než blok veřejný, transakci přijmou, a to zároveň s jedním potvrzením z útočníkova bloku. Blockchain se v tuto chvíli rozdělí na dvě větve, kdy některé uzly berou za platný útočníkův, a některé veřejný blok.

Poté nastává chvíle, kdy se útočník pokouší o dvojitou útratu. Ihned po odeslání bloku požádá útočník směnárnu o vrácení bitcoinů, které původně odeslal, a to na adresu jím kontrolovanou. V tuto chvíli mohou nastat dva případy. Útočníkův blok se stane platným blokem v blockchainu, jelikož dostatek těžařů ho vidělo jako první a vytěžilo následný blok. V tomto případě útočník neztratí ani nezíská nic, jelikož ve směnárně pouze provedl vklad a následný výběr bitcoinů. Pokud se ale platným blokem stane původní veřejný blok, tak původní transakce s vkladem je zneplatněna. Nicméně blok obsahující transakci vracející bitcoiny je stále platný a součástí blockchainu. Útočník tedy získává zpět všechny bitcoiny za vklad, který podle blockchainu nikdy neproběhl.

6.2.2 Útoky cílící na infrastrukturu spojenou s Bitcoinem

Tato část rozebírá útoky spojené s Bitcoinovou infrastrukturou. Nejde již tedy o útoky cílící na Proof-of-Work či transakce, ale jde o útoky spojené s burzami, směnárnami či dalšími platformami, kde je Bitcoin používaný jako měna.

6.2.2.1 DDoS

DoS - Denial od service (česky odepření služby) je způsob útoku na síť, jehož hlavním cílem je znemožnění přístupu ke službě ostatním uživatelům či dokonce kompletní přerušení služeb poskytovatele. Toho je obvykle dosaženo tak, že je na napadenou službu odesláno v krátkém časovém úseku obrovské množství požadavků, důsledkem čehož je systém přehlcen a server se tak pro normální uživatele stává nedostupným.

Vzhledem k distribuované povaze Bitcoinové sítě a konsensuálnímu protokolu by však pouhý DoS útok pro fungování systému nepředstavoval žádné větší ohrožení. Na to, aby bylo narušeno fungování takovéto sítě je třeba poměrně silného DDoS – Distributed Denial of Service - útoku. Fakt, že jde o distribuované odepření služby je zásadní, jelikož na rozdíl od DoS útoku, který je obvykle prováděn pomocí jednoho počítače a jednoho internetového připojení, DDoS útok využívá velké množství rozptýlených počítačů. Z těchto počítačů je pak serveru, službě či síti odesláno velké množství požadavků, které mají za cíl přehltit primární zdroje (jako CPU či RAM) anebo velké množství aplikačních dat, které zahlcují síťovou infrastrukturu. Obě tyto metody lze pak kombinovat ve snaze o efektivnější způsob útoku. Tyto útoky jsou často prováděny v globálním měřítku a je tak prakticky nemožné rozeznat útočníky od normálních uživatelů. DDoS útoky jsou zpravidla velmi účinné a jejich důsledky jsou pro danou službu extrémně rušivé. Zároveň je ale poměrně levné tyto útoky uskutečnit.

Nejčastějším způsobem jak současně zaútočit z velkého množství počítačů v globálním měřítku je prostřednictvím pronajatého botnetu. Botnet si lze představit jako síť zařízení, schopných vysílat požadavky (ať už jde o počítače či chytré spotřebiče), které má útočník pod kontrolou. Tato zařízení se obvykle dostávají pod útočníkovu kontrolu skrze škodlivý software jako je malware či virusy. Nicméně existují i případy, kdy lidé poskytují svůj počítač pro vykonání DDoS útoku i dobrovolně, a to například při bojkotu či demonstraci proti určitým službám.

Byly doby, kdy bylo možné pomocí DDoS útoku narušit fungování celého Bitcoinového systému, nicméně dnes je infrastruktura Bitcoinu na takové úrovni, že už to není možné. V rámci Bitcoinu jsou tak DDoS útoky nejčastěji používány proti směnárnám, burzám a mining poolům. Útočníci se zaměřují zejména na velké mining pooly a směnárny, jelikož potenciální zisk je daleko větší, než kdyby cílem byly individuální těžaři. K útokům na mining pooly dochází hlavně z důvodu odstranění konkurence. Často tak mining pool s větším výpočetním výkonem napadá svou konkurenci tak, že jí odesílá velké množství požadavků (nejčastěji falešných transakcí) a vyčerpává tak její zdroje. Konkurence je pak eventuálně nucena vyřazovat všechny transakce, jak falešné tak pravé, a v případě pokračujících útoků může dojít až k situaci, že se musí stáhnout ze scény.

V případě útoků na bitcoinové směnárny či burzy jde o poněkud odlišný případ. U těchto platforem dochází nejčastěji k tomu, že je skrze DDoS útok omezena dostupnost

zásadních služeb pro obchodování s měnou. K tomu dochází hlavně ze dvou důvodů. Prvním je vysoká konkurence mezi různými směnárnami a burzami. V případě, že jedna z nich (obvykle ta největší) je častým objektem těchto útoků, obchodníci budou v dalších případech nakloněni k využití jiné burzy. Druhým důvodem je pak manipulace s cenou. Někteří obchodníci, orientovaní pouze na zisk, by mohli využít DDoS za účelem vytvoření příznivých obchodních podmínek. K tomu by mohlo dojít jak při růstu, tak i při poklesu cen. Při růstu cen by DDoS mohl tento růst zpomalit a zabránit obchodníkům v dalším nákupu bitcoinů. Pro příklad, obchodník snažící se koupit bitcoin, by mohl dát příkaz k nákupu za nižší cenu v menší směnárně, zatímco by pomocí DDoS útoku blokoval přístup ke směnárně větší. Jeho nižší nabídka by pak měla větší šanci na přijetí od prodejců, kteří dočasně nemohou obchodovat na největší směnárně. V druhém případě by docházelo k poklesu ceny, zatímco obchodník drží bitcoin. Obchodník by tak mohl využít DDoS, aby zpomalil pokles, případně aby se mu podařilo prodat za co nejvyšší cenu. (Vasek, Thornton , Moore, 2014)

6.2.2.2 Krádeže peněženek

Dalším z útoků cílených ne přímo na Bitcoinový protokol, ale na infrastrukturu s ním spojenou, jsou krádeže peněženek. Přestože ukrást přístupové klíče k peněžence pouze z Bitcoinové technologie je prakticky nemožné, i tak jsou krádeže peněženek jedním z největších, dokonce možná největším způsobem narušení bezpečnosti v celém systému. Problém leží ve způsobu, jakým jsou přístupové klíče zabezpečeny. Zabezpečení klíčů totiž spadá do rukou uživatelů. V návaznosti na to jak jsou bitcoiny uloženy a jaká bezpečnostní opatření jsou použita pak vznikají rozličná pochybení, která mohou potenciální útočníci zneužít. Hlavními cíli útoků jsou tak koncoví uživatelé, potažmo podniky zabývající se službami spojenými s peněženkami.

Podle způsobu jakým jsou klíče zabezpečeny pak může docházet k různým útokům. Nejčastějšími a nejnebezpečnějšími jsou pak tyto:

1. *Uložení bitcoinů na platformě třetí strany* – spousta investorů neznalých fungování systému kryptoměn nakoupí bitcoiny pomocí směnárny či burzy a následně své bitcoiny na této platformě i uloží. V některých případech dokonce ukládají na server směnárny či burzy i klíče svých peněženek. Přestože mají tyto platformy zajištěná důkladná bezpečnostní opatření, nejsou vůči útokům immuní. Pro útočníky v tuto chvíli místo skoro nemožného brute force útoku

vyvstává problém nalezení bezpečnostních nedokonalostí na serverech bitcoinových směnáren. Přestože útok na server velkých směnáren je nesmírně složitý, je daleko pravděpodobnější, než že by útočník dokázal provést úspěšný brute force. O nebezpečí ukládání informací na platformě třetí strany svědčí i fakt, že 5 největších bitcoinových krádeží bylo provedeno právě tímto způsobem. Dohromady bylo skrze ukradené autorizační údaje ztraceno přes jeden milion bitconů.

2. *Boti* – další z možností, jak lze provést krádež peněženky, je pomocí stále více populárních slack botů. Jedná se o automatizovaný program, který uživatele notifikuje o tom, že při jejich transakci došlo k chybě, a je třeba se přihlásit a transakci zopakovat. Ve zprávě bývá uvedeno, že v případě, že tak neučiní, vyvstává riziko, že o své mince mohou přijít. Tito boti často působí jako že se jedná o oficiální program zprostředkovaný například službou bitcoinové směnárny. Důvěřiví uživatelé pak mohou ve strachu o ztrátu mincí opravdu přejít do přihlašovacího portálu, kam zadají přihlašovací údaje ke své peněžence. Samozřejmě pak o své peníze opravdu přicházejí.

3. *Neoficiální aplikace* – v nedávné minulosti byly poměrně populárním nástrojem krádeží klíčů neoficiální aplikace. Na trhu je totiž spousta různých poskytovatelů služeb spojených s Bitcoinem. Ty menší se snaží zákazníky přilákat různými způsoby, ať již nižšími poplatky, či zvýšenou paletou služeb. Tito menší poskytovatelé ale ne vždy mají zajištěnou takovou infrastrukturu jako jejich větší protějšky. Často tak může docházet k případům, že nedisponují vlastními oficiálními aplikacemi, ať už na operační systém Android nebo na iOS. V takovém případě může dojít k tomu, že podvodníci navrhnou falešnou aplikaci vydávající se právě za takovou službu. Jádrem takové aplikace je pak malware, který shromažďuje klíče zadané ve snaze o provedení transakce. Tyto aplikace jsou často rychle odhaleny a nezůstávají tak dlouho dostupné, nicméně i tak může být potenciální škoda poměrně značná. Uživatelé využívající méně známého poskytovatele by se tak měli vždy ujistit, že používají aplikaci oficiální.

Za správné zabezpečení si vždy zodpovídá majitel klíčů. Lze však doporučit metody, pomocí kterých jde zajistit vysoký stupeň ochrany proti krádežím. Jak již bylo zmíněno, nedoporučuje se ukládat bitcoiny či autorizační údaje na platformě třetí strany. Pokud se však uživatel rozhodne pro tuto možnost, měl by vždy mít zajištěné údaje pomocí dvoufaktorového ověření. To by mělo nejlépe zahrnovat ověření e-mailovou adresou a ověření pomocí aplikace (SMS ověření se totiž dá zachytit). Dalším způsobem, jak zajistit větší ochranu, je pomocí hardwarové peněženky. Při použití by se mělo vždy ověřit, zda se jedná o peněženku, která dříve nepřišla do kontaktu s neznámým softwarem. Jako poslední by bylo vhodné zmínit ochranu za použití PPSS - Password protected secret sharing. Zjednodušeně jde o metodu, při které jsou autorizační údaje rozděleny na části, které jsou pak uloženy na různých serverech.

6.2.2.3 Refund útoky

Refund útok – útok na vrácení peněz – je dalším z řady útoků cílených na infrastrukturu spojenou s Bitcoinem. Konkrétně se snaží o napadení platebního protokolu BIP70. BIP70 je dnes komunitou přijatý, standartně používaný platební protokol, pomocí kterého zákazníci a obchodníci při platbách komunikují, a který určuje, jak jsou platby konkrétně prováděny. V současnosti je využíván dvěma největšími směnárenskými platformami – Coinbase a BitPay – které tento protokol poskytují více než 100 000 různým obchodníkům po celém světě. Hlavní myšlenka pro použití tohoto protokolu je zjednodušení uživatelského rozhraní využívaného při platbách Bitcoinem. Uživatelé a obchodníci již nejsou reprezentováni 34bitovou adresou, ale personalizovaným uživatelským jménem, což ve výsledku dělá proces platby jednodušší a daleko přehlednější. Další důležitou vlastností je schopnost zabránit manipulaci platby prostředníkem.

Níže je popsán průběh platební transakce, používající BIP70 protokol :

- Obchodník odešle žádost o platbu, která obsahuje Bitcoinovou adresu, počet požadovaných bitcoinů a poznámku obsahující účel platby. Tato žádost je podepsána obchodníkovým soukromým klíčem.
- Zákazník obdrží informace o platbě a ověří pravost požadavku pomocí své peněženky. Pokud je platba schválena, následují dva úkony.

- Peněženka autorizuje transakci a pošle ji do Bitcoinové sítě. Dále odešle obchodníkovi zprávu o platbě, která obsahuje kopii transakce, počet zaplacených bitcoinů a refund adresu, pro případ že by nastaly komplikace a zákazník vyžadoval vrácení peněz.

V současném online obchodu je zákazníkovi standartně vracena platba na stejný účet, ze kterého platbu provedl. Nicméně u Bitcoinu není adresa, na kterou je zákazníkovi vracena platba, ta samá, ze které byla původní platba provedena. Tato adresa navíc nemá žádnou vazbu, která by ji mohla spojovat s adresou původní. Obchodník si pak musí být vždy jistý, že je platba skutečně odesílána na zákazníkovu adresu. Navíc v současnosti neexistuje jednotný protokol pro vracení peněz. Proto si směnárny a obchodníci musejí stanovovat vlastní politiku vracení peněz. Z této skutečnosti pak vychází princip pro možné refund útoky.

V práci "Refund Attacks on Bitcoin's Payment Protocol" jsou pak rozlišeny dva možné útoky :

1) Silkroad Trader – tento způsob útoku se opírá o chybu zabezpečení autentizace v platebním protokolu. Hlavní myšlenka spočívá v tom, že zákazník může ve zprávě o platbě uvést refund adresu, která je pod kontrolou třetí osoby. Tato třetí osoba pak může iniciovat vrácení peněz. Důležité je, že od původního zákazníka se při požadavku vrácení peněz nevyžaduje digitální podpis. Obchodník tedy přichází o peníze a zákazník zboží nevrací, jelikož podle stavu jeho peněženky k žádnému vrácení peněz nedošlo.
2) Marketplace Trader - Coinbase a Bitpay nabízejí zákazníkům i možnost poskytnutí refund adresy pomocí externí metody komunikace, jako například e-mailu. Při využití této možnosti je pak refund adresa zahrnutá ve zprávě o platbě ignorována. Tato odchylka od protokolu umožňuje další způsob útoku, který do určité míry využívá phishingu. Útočníkem je v tomto případě prostředník mezi zákazníkem a obchodníkem. Ten založí webovou stránku s atraktivními cenami, která má přilákat potenciální zákazníky.Když zákazník klikne na tuto webovou stránku, omylem odhalí svou adresu, což je dostatečné k tomu, aby prostředník provedl útok. V případě, že si zákazník zakoupí produkt, prostředník odešle transakci legitimnímu obchodníkovi. Zákazník je pak spojen s obchodníkem, nicméně údaje o zákazníkovi již byly odhaleny prostředníkovi prostřednictvím

externí e-mailové komunikace. Po transakci prostředník zažádá jménem zákazníka o vrácení peněz, které ale budou zaslány na adresu prostředníka. Zákazník o tomto podvodu sice nebude vědět, nicméně obchodník i tak přichází o bitcoiny.

6.2.2.4 Deanonymizace

Jak již bylo řečeno v teoretické části, Bitcoin v zásadě není měnou zcela anonymní. Jde o měnu pseudoanonymni, což znamená, že veškeré transakce jsou zaznamenány, nicméně nejsou přímo spojeny s konkrétními osobami. Dále je doporučeno pro každou transakci využívat jiné adresy, aby se stupeň ochrany ještě zvýšil. Nicméně i přes všechny tyto vlastnosti je do určité míry stále možné vysledovat identitu vlastníků peněženek. Existuje více možností, v této části se ale zaměřím na nejpopulárnější deanonymizační útok, a to tzv. dust attack.

Dust attack – prašný útok – je způsob, jakým je možné díky vztahu mezi adresami identifikovat vlastníka peněženek. Dust, neboli prach, je v Bitcoinu termín užívaný pro extrémně malou část bitcoinu, někdy také nazývanou jako satoshi. Jde o jednotku tak malou, že při jejím odesílání transakční poplatky převyšují její hodnotu. V této skutečnosti také spočívá princip útoku. Pro uživatele, kteří tento dust obdrží je nevýhodné ho dál odesílat v původním stavu, ale je lepší ho připojit v rámci nějaké větší transakce. (Medium, 2019)

Útok konkrétně probíhá tak, že útočník do sítě rozešle obrovské množství jednotek dustu. Tento dust se připojí do velkého množství adres, a to ve formě tzv. Unspent Transaction Outputu (v podstatě nevyužitých prostředků). Tyto malé částky si však zachovávají důležitou vlastnost, a to dohledatelnost v blockchainu. Útočník má tak o každé této částce přehled a může sledovat její další pohyb v rámci transakcí. Pro tento útok je důležitý fakt, že zůstatek na bitcoinových peněženkách je prezentován sumou vstupů a nevyužitých prostředků (výstupů). Pro příklad tak zůstatek 1 bitcoinu na peněžence může představovat sumu několika nevyužitých vstupů jako např. 0,3 + 0,2+ 0,5 BTC. Také samozřejmě může být tvořen daleko větším počtem výstupů o různé hodnotě, zahrnujících i dust. Samozřejmě lze kontrolovat, které prostředky jsou využity na zaplacení transakcí, nicméně běžný uživatel bude nejčastěji využívat služby svého poskytovatele. V takovém případě bude využita služba poskytovatele, která automaticky sbírá prostředky z nejvhodnějších adres nacházejících se v peněžence. Pak již uživatel

nemá kontrolu nad tím z jakých adres je transakce placena a je pravděpodobné, že v těchto transakcích bude zahrnutý i dust.

Princip odhalení identity pomocí dust útoku spočívá ve způsobu, jakým v Bitcoinu funguje placení. Dejme tomu, že si chci koupit zboží v hodnotě 1BTC. Nicméně žádná z mých adres sama o sobě nemá dostatečné prostředky k zaplacení. Pokud ale využiji prostředků z více mých adres, mohu si zboží bez problému koupit. Takto pak v praxi fungují platby. Pokud na žádné adrese není dostatečná suma k zaplacení dané transakce, automaticky se zkombinují prostředky z kontrolovaných adres tak, aby odpovídaly požadované částce. A právě v této chvíli přichází do hry dust. Pokud se dust nachází na všech adresách, ze kterých je transakce placena a je v nich zahrnut, pak může útočník pomocí blockchainu odhalit, že jeden uživatel kontroluje právě tyto adresy.

Kromě útoků zaměřujících se na odkrytí identity uživatelů, existují samozřejmě i způsoby, jakými se uživatelé prozrazují sami.

1) *Zveřejnění jména spolu s Bitcoinovou adresou na internetu*

Kdo zná identitu : Bitcoinová směnárna

Jde asi o nejběžnější způsob, jakým je odhaleno vlastnictví Bitcoinové adresy. Spousta lidí na internetu nechává veřejně přístupnou svou Bitcoinovou adresu spolu s jejich jménem, v naději, že pak obdrží platbu. Často se může jednat o tvůrce obsahu, kteří své dílo volně a zdarma zpřístupňují, a kteří u tohoto díla nechávají několik způsobů jak jim mohou lidé přispět. Může se jednat právě o Bitcoinovou adresu, bankovní účet či například PayPal.

Nicméně jakmile je adresa na internetu zveřejněna, kdokoliv s internetovým připojením má možnost identitu zjistit. Pomocí blockchainu je pak také možné vysledovat, jaké transakce pomocí dané adresy proběhly.

2) *Obchodování s Bitcoiny pomocí směnáren*

Kdo zná identitu : Bitcoinová směnárna

Téměř každá směnárna, která operuje s národními měnami, podléhá předpisům o praní špinavých peněz. Tudíž je vyžadováno, aby zákazníci, kteří chtějí s kryptoměnami obchodovat, prokazovali směnárně svou totožnost, ať už pomocí občanských průkazů,

bankovních výpisů či účtenek. Pokud tedy zákazníci nepoužijí zfalšované dokumenty, směnárny pak mají záznamy o identitě všech zákazníků. Tyto záznamy si pak mohou zachovat a to na dobu neurčitou. Samozřejmě že záznamy nejsou veřejně přístupné, nicméně samotná jejich existence nepřímo zamezuje platby spojené s nelegálními aktivitami. Uživatelé totiž mohou být spojeni se všemi příchozími a odchozími transakcemi na účtu směnárny. Tyto transakce pak mohou zpětně odhalit, kdo je skutečným vlastníkem adres spojenými se zmíněnými transakcemi.

3) Nákup zboží pomocí Bitcoinu

Kdo zná identitu: Obchodník nebo platební protokol

Odhalení identity při nákupu zboží pomocí Bitcoinu se nedá lehce vyhnout. Příjemce Bitcoinové platby totiž může vždy identifikovat identitu pomocí odesílací adresy zákazníka. Pokud zákazník nekupuje zboží v digitální podobě, ve většině případů totiž poskytuje obchodníkovi svoje jméno společně s dodací adresou.

V případě, že obchodník používá platební protokol jako Coinbase nebo Bitpay, fyzická adresa ani identita z pravidla nebývá odhalena. Nicméně i tak bude záznam o transakci spolu s detaily uložen na platformě platebního protokolu.

6.2.3 Návrhy na vylepšení úrovně anonymity

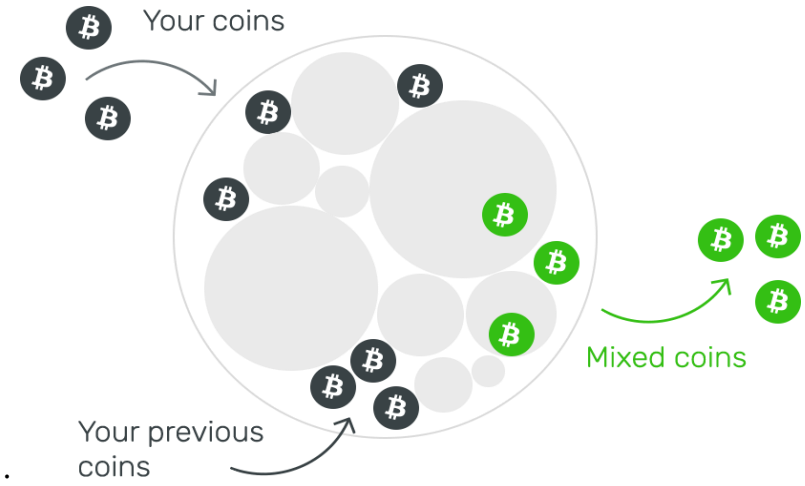
Je důležité si uvědomit, že anonymita není Bitcoinovému systému vlastností inherentní. Nicméně i tak jde o vlastnost, která se s Bitcoinem velice často spojuje. Skutečnost, že blockchain je veřejně přístupný a bitcoiny jsou jedinečné a zpětně dohledatelné, má v budoucnosti velký potenciál narušit anonymitu uživatelů. Proto zde uvádím dva návrhy jak uživatelé mohou zvýšit stupeň anonymity při používání Bitcoinu.

1) Použití mixing protokolu

Mixování bitcoinů je jedna z možností, jak lze zvýšit stupeň anonymity. Nejčastěji bývá poskytovaná skrze osoby známé jako mixeři. To jsou poskytovatelé služeb, kteří používají mixing protokoly tak, aby zaměňovaly trasy transakcí. V procesu mixování dochází k tomu, že klientovy prostředky jsou rozděleny do několika menších částí. Tyto části jsou pak náhodně namixovány s podobnými částmi jiných klientů. Po dokončení mixováni klient obdrží stejnou částku, která je ale tvořena částmi od ostatních klientů.

Klient tak operuje v podstatě s úplně novými prostředky. Tato skutečnost pomáhá přerušit jakýkoli vztah, které by mohl být mezi klientem a použitými mincemi nalezen

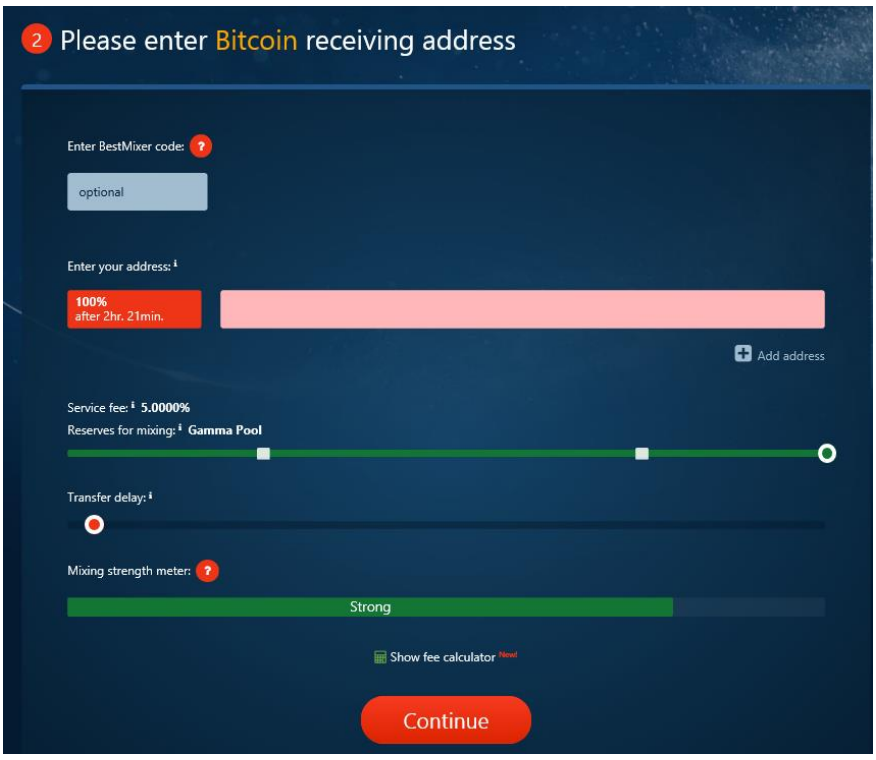
Obrázek 6 Mixování Bitcoinů



(Medium, 2019)

V rámci mixingu lze využít dvou forem, a to: Peer-to-peer mixingu a distribuovaného mixingu. V rámci P2P mixingu je asi nejvíce využívaným protokolem *Coinjohn*, zatímco u distribuovaného je to pak *MixCoin* či *Tumbler*. Poskytovatelů mixovacích služeb je dnes několik, zde bych uvedl např *BESTCOINMIXER.IO,* jehož uživatelské prostředí si lze prohlédnout na obrázku č. 7.

Obrázek 7 Uživatelské prostředí bestcoinmixer.io (Bestcoinmixer, 2019)



Pokud si chce Bitcoin zachovat anonymitu jako jednu z jeho předních vlastností, bylo by vhodné, aby podobný protokol integroval do svého systému.

2) Použití VPN

Další z možností jak může být narušena anonymita v rámci Bitcoinu je od poskytovatele internetu. Bitcoin totiž nemá žádné šifrování co se týče odesílání transakcí do P2P sítě. Když klient odesílá transakce do sítě, projdou přes servery poskytovatele ve formátu prostého textu. Poskytovatel internetu pak může tuto zprávu zachytit a určit, že daná transakce patří k příslušné IP adrese. Odeslané transakce se v síti nejprve zobrazí pomocí IP adresy, čímž se odliší od transakcí, které už přijaly jiné uzly. Tato IP adresa pak může být poskytovatelem internetu použita k dohledání osobní identity. Tomuto problému se dá zabránit při použití VPN, která zamaskuje klientovu skutečnou IP adresu.

VPN je virtuální privátní síť - systém propojení počítačů do zabezpečené soukromé sítě, a to i v případě, že jsou na různých místech v internetu. Mezi počítači se vytvoří šifrovaný tunel, kterým proudí veškerá komunikace mezi počítači ve virtuální síti. Pro Bitcoin to hlavně znamená, že VPN neuchovává historii aktivit na svých serverech. Některé VPN také používají sdílenou IP adresu pro více uživatelů, aby bylo obtížnější nalézt identitu osoby.

Použití VPN k připojení do Bitcoinového klienta je tedy dalším způsobem, jak lze zvýšit bezpečnost a anonymitu transakcí. Nicméně v tomto případě je také důležité věřit poskytovateli VPN, že nemonitoruje aktivity uživatelů. Pro příklad uvádím několik populárních poskytovatelů VPN doporučovaných pro Bitcoinové platby: ExpressVPN, NordVPN, CyberGhost, Windscribe.

Tabulka 1 Útoky cílící na Bitcoinový systém

Útok	Cíle útoku	Způsob	Zasažené subjekty	Efekty útoku	Možná obrana
Útok 51%	Bitcoinový systém, Pow protokol	Útočník kontroluje více než 50% hashratu sítě, pomocí soukromého těžení dochází k větvení blockchainu	Bitcoinová síť, Bitcoinové směnárny, těžaři, uživatelé	Oslabení konsensuálního protokolu, oslabení důvěry v měnu,umožnění DDoS útoků, demotivace menších těžařů	Důkladné sledování sítě, komunikace a varování o úspěšných double-spend útocích, demotivace těžení ve velkých uskupeních
Race útok	Pow protokol	Jeden Bitcoin je zároveň použit pro dvě transakce, s vědomím, že pouze jedna se stane platnou	Obchodníci	Obchodníci přicházejí o produkty či služby, klesá důvěra v systém, větví se blockchain	Dočasné přerušení přijímání transakcí , důkladné sledování sítě, komunikace a varování o úspěšných double-spend útocích
Finneyho útok	Pow protokol	Využívá principu Race útoku, pomocí předtěženého bloku dokáže provést útok i v případě jendoho potvrzení transakce	Obchodníci	Ulehčuje útoky dvojité útraty + stejné efekty jako race útok	Vyčkání na určitý počet potvrzení transakce
Brute Force	Bitcoinový systém, Pow protokol	Pokročilejší stupeň Finneyho útoku, útok je prováden pomocí řady předtěžených bloků	Obchodníci, uživatelé	Ulehčuje útoky dvojité útraty, vytváří se dlouhé větve blockchainu	Sledování sítě, komunikace a varování o double-spend útocích
Vector 76	Pow protokol	Kombinace Race útoku a Finneyho útoku, princip útoku je stejný jako v případě Race útoku, využívá ale předtěženého bloku	Bitcoinové směnárny	Usnadňuje dvojitou útratu velkého počtu bitcoinů	Vyčkání na určitý počet potvrzení transakce

Tabulka 1 Útoky cílící na Bitcoinový systém

Útok	Cíle útoku	Způsob	Zasažené subjekty	Efekty útoku	Možná obrana
DDoS	Bitcoinová infrastruktura	Koordinovaný útok na služby, s cílem vyčerpat síťové zdroje a způsobit nedostupnost služeb	Bitcoinová síť, směnárny, těžaři, uživatelé	Přerušení služeb pro uživatele a těžaře, demotivace těžařů, manipulace s cenou, usnadnění potenciálního útoku 51%	Ověřování na základě digitálního podpisu
Krádeže peněženek	Bitcoinová infrastruktura, servery směnáren	Útočníci ukradnou nebo zničí soukromé klíče uživatelů	Uživatelé, Bitcoinové směnárny	Ztráta bitcoinů v peněženkách, zvyšování nedůvěry v měnu, zpomalení růstu	Dvou-faktorové zabezpečení, využití hardwarových peněženek, PPSS
Refund útoky	Platební protokol	Zneužití současné politiky vracení peněž platebních protokolů	Obchodníci, uživatelé	Obchodníci přicházejí o peníze či produkty, zákazníci se mohou dostat na černou listinu	Používání veřejně ověřitelné adresy, změna politiky vracení peněz, úprava platebního protokolu
Deanonymizace	Peněženky a adresy	Nalezení identity osoby kontrolující Bitcoinové peněženky	Uživatelé	Uživatelé přicházejí o soukromí, může docházet k útokům na osobu	Využití metod pro zajištění větší anonymity

Zdroj: Vlastní zpracování

6.2.4 Zhodnocení

Pokud zvážíme útoky cílící na Bitcoinový systém, všechny zmíněné útoky se snaží o dosažení dvojité útraty. Z hlediska potenciálních ztrát se jeví jako nejnebezpečnější většinový útok. V tomto případě je ale nutné vzít v úvahu jeho finanční náročnost. V současnosti si totiž nelze představit většinový útok, který by byl z ekonomického hlediska efektivní. Náklady by byly vždy alespoň několikanásobně vyšší než jeho potenciální zisky. Zároveň pokud by takovýto útok opravdu proběhl, hodnota napadené kryptoměny by s nejvyšší pravděpodobností okamžitě poklesla, což by ve výsledku ještě snížilo jeho efektivitu.

Jako neproveditelnější způsob útoku se jeví Race útok, spolu s jeho variacemi Finneyho útokem a Vecor76. Z hlediska ekonomické efektivity nasává u Finneyho u Vector76 problém. Oba dva totiž pracují s principem předtěženého bloku, na který je třeba vynaložit značné náklady společně s časem. U všech tří útoků je ale problém jeho možná prevence. Způsob prevence je v tomto případě velmi snadný a stačí pouze počkat na potvrzení transakce dostatečným počtem bloků. Pokud jsou tedy obchodníci a uživatelé srozuměni s možností těchto útoků, a způsobem jakým Bitcoin funguje, pak by měla být možnost těchto útoků prakticky eliminována.

Celkově se žádný z útoků cílících na dvojitou útratu nejeví jako bezprostřední ohrožení systému. Buď se jedná o útoky neefektivní a časově náročně nebo útoky, kterým je možné předejít znalostí principů fungování systému. Nicméně fakt, že tyto útoky jsou teoreticky možné je ale zásadní. Ukazují totiž, že systém není bezchybný a existují možnosti jak ho zneužít. Ačkoli tak v současnosti nejsou tyto útoky pravděpodobné, v budoucnu by se mohli ukázat jako silné nedostatky systému.

Co se týče útoků cílících na infrastrukturu spojenou s Bitcoinem, je situace poněkud odlišná. DDoS útoky jsou v praxi proveditelné, z dlouhodobého hlediska ale nebudou mít pro Bitcoin velké následky. Pravděpodobně půjde o rychlou změnu ceny, která bude rychle vyrovnána korekcí. V případě deanonymizace je provedení útoku vcelku pravděpodobné, vyvstává ale otázka čeho útočník dosáhne, odhalí-li identitu vlastníka peněženek. Pokud se nebude jednat o vlastníka ovládající jednu z největších peněženek, hodnotu Bitcoinu to neovlivní.

Jako potenciálně největší nebezpečí se jeví krádeže peněženek. Uživatelé používající Bitcoin totiž nejsou kryptografové, a velká část z nich pravděpodobně systému do hloubky nerozumí. Mohou tak místo zvýšeného zabezpečení upřednostnit pohodlí při používání. Pokud používají webové peněženky a jejich klíče jsou uloženy na platformě třetí strany, může tak nastat problém. V případě, že tuto službu využívá velký počet uživatelů a bezpečnost serverů je prolomena, pro Bitcoin to může znamenat silné důsledky.

6.3 Příklady konkrétních útoků na Bitcoin

V této části jsem vybral několik skutečně provedených útoků na Bitcoin. Zvolil jsem útoky, které byly, co se objemu ukradených bitcoinů týče poměrně velké a měly tak silný dopad. Na těchto příkladech chci demonstrovat, jaké útoky jsou používány v praxi a kde se v systému historicky nacházela nejslabší místa. Také chci ukázat, jaké cenové dopady mohou takovéto útoky přinášet.

6.3.1 Útok na burzu Mt. Gox

Dodnes největším úspěšným útokem v historii Bitcoinu byl útok na burzu Mt. Gox. Mezi lety 2013 a 2014 to byla největší kryptoměnová burza na světě se sídlem v Japonsku, která zpracovávala 70% všech Bitcoinových transakcí.

Ačkoli dodnes není jisté, jakým konkrétním způsobem byl útok proveden, předpokládá se, že většina bitcoinů byla ukradena z „hot "online peněženek. Hot peněženka, je Bitcoinová peněženka, která je vždy připojena k internetu a může komunikovat s externími zdroji. Podle dostupných zpráv byl privátní klíč Mt. Gox po určitou dobu v roce 2011 nezašifrovaný. Tento klíč byl někdy v září 2011 ukraden, což mělo za následek, že se zkopírovaný soubor wallet.dat dostal do rukou hackerů.

Poté, co útočníci prolomili tento soubor, získali přístup k šifrování a všem bitcoinům na burze, a to bez vědomí Mt. Gox. Pomocí zkopírovaného souboru měli útočníci přístup ke všem klíčům, což vedlo ke krádežím prostředků z peněženek pomocí opětovného použití adres. To si ale systémy Mt. Gox interpretovaly tak, že jsou prostředky

přesouvány na bezpečnější adresy. Vždy když tedy byly z peněženky odčerpány prostředky, systém připsal dalších 40 000 bitconů na adresy postižených účtů.

Útok tak probíhal od roku 2011 až do roku 2014, kdy burza vyhlásila bankrot. Už ale v polovině roku 2013 v podstatě přišla o veškeré bitcoiny. V rámci útoku bylo ukradeno 744 408 bitcoinů, které měly v té době hodnotu přibližně 450 milionů dolarů. Co je ale důležitější, jednalo se o krádež 6% ze všech bitcoinů, které byly v roce 2014 v oběhu. Ze všech ukradených bitcoinů bylo uživatelům vráceno pouze asi 200 000, zbytek byl navždy ztracen.

Na obrázku č. lze vidět jak se cena Bitcoinu vyvíjela v měsících po vyhlášení bankrotu burzy Mt. Gox.

Graf 4 Dopady útoku na burzu Mt. Gox (Coindesk, 2019)

6.3.2 Útok na směnárnu Bitfinex

Bitfinex je kryptoměnová směnárna a burza založená a sídlící od roku 2012 v Hongkongu. Dnes je druhou největší kryptoměnovou směnárnou.

V roce 2016 se stala obětí druhého největšího Bitcoinového útoku v historii. Zdrojem prolomení byl pravděpodobně způsob, jakým byly strukturovány uživatelské účty spolu s využitím poskytovatele peněženek BitGo jako dodatečného zabezpečení. V roce 2015 totiž Bitfinex a BitGo vytvořily systém vícepodpisových peněženek. V tomto systému byly klíče ke každé peněžence rozděleny mezi více vlastníků, s cílem snížení rizika neoprávněné manipulace. Ve výsledku tak každý uživatel měl tři klíče, dva z nich uložené na platformě Birfinexu (jeden online a jeden offline) a poslední na BitGo, sloužící k podepisování transakcí. BitgGo klíč měl sloužit jako další vrstva zabezpečení, jehož hlavním účelem bylo ověření a schválení transakce iniciované pomocí Bitfinexu. Aby mohl uživatel manipulovat s prostředky na účtě, musel získat autorizaci alespoň dvou ze tří klíčů.

Oficiální zprávu o útoku Bitfinex nikdy nevydal, nicméně je známo, že útočníkům se nějakým způsobem podařilo získat kontrolu nad určitým počtem klíčů uložených na Bitfinexu, nejpravděpodobněji uložených v hot online peněženkách. Pomocí Bitfinex klíče pak byly iniciovány transakce. Místo aby tyto transakce byly zastaveny, Bitgo automaticky podepsal všechny transakce a poskytl tak útočníkům autorizaci jejich klíče. K tomu pravděpodobně došlo kvůli nesprávné implementaci systému. S dvěma autorizovanými klíči pak byli hackeři schopni přesunout bitcoiny z Bitfinexu.

Počet ukradených bitcoinů se nakonec ustálil na čísle 119 756, což v té době odpovídalo asi 72 milionům dolarů. Všechny ukradené bitcoiny pocházely z peněženek uživatelů. Okamžitě po útoku zastavil Bitfinex veškeré výběry a transakce v systému. Jako reakce na útok spadla cena Bitcoinu o celých 20% . Konkrétní cenové důsledky si lze prohlédnout na níže přiloženém grafu.

Graf 5 Dopady útoku na směnárnu Bitfinex(Coindesk, 2019)

6.3.3 Útok na směnárnu Coinrail

Posledním, zde zmíněným útokem, je útok na Coinrail z roku 2018. Coinrail je korejská kryptoměnová směnárna, obchodující s širokým spektrem měn od Bitcoinu až po kryptoměny nedosahující hodnoty ani jednoho dolaru. V porovnání s konkurencí jde o směnárnu vcelku malou. Právě proto je zajímavé podívat se na to, jaké důsledky vyplynuly z útoku na takovouto menší směnárnu.

Útok proběhl 5. června 2018 a přestože oficiální zprávy o provedení nejsou dostupné, základní princip útoku byl stejný jako v předchozích případech. Útočníci nějakým způsobem prolomili ochranu serverů a zmocnili se klíčů nacházejících se v hot peněženkách. Konečné škody pak byly vyčísleny zhruba na 37 milionů dolarů. Zajímavé ale je, že převážná většina ukradených mincí nebyla Bitcoin. Ukradeny byly především měny zvané jako altcoiny – kryptoměny mimo Bitcoin a Ethereum. Přestože byl tedy Bitcoin zasažen jen nepatrně, i tak byla reakce silná a okamžitá. Za jeden den

ztratil Bitcoin skoro 1000 dolarů, což bylo asi 15% z celkové hodnoty. Lze si tedy všimnout i jakési provázanosti mezi kryptoměnami.

Graf 6 Dopady útoku na směnárnu Coinrail (Coindesk, 2019)

6.3.4 Zhodnocení

Z těchto tří příkladů je patrné, že otázka bezpečnosti má pro kryptoměny kritický význam. Ve všech třech případech začala hodnota Bitcoinu bezprostředně po útoku silně klesat. V nejhorším případě dosáhl pokles až 30%, průměrně pak byl pokles na úrovni 20% její původní hodnoty. Dalším důležitým faktem je, že ztráta hodnoty přišla prakticky okamžitě. Svého maxima dosáhl pokles hodnoty prakticky vždy již 24 hodin od narušení bezpečnosti a zároveň nastolil klesající trend, trvající až několik měsíců.

Na základě těchto poklesů hodnoty je pak možné zpochybnit funkci Bitcoinu jako peněz. Obecně jednou z hlavních funkcí peněz totiž je, že uchovává hodnotu. Jak lze ale z těchto příkladů vidět, hodnota Bitcoinu je silně volatilní a často je podmíněna externími faktory. Hodnota Bitcoina také z velké části vychází z důvěry lidí. Pokud lidé důvěřují Bitcoinu jako obecné přijímanému platidlu a zároveň roste jeho užitečnost, pak

i jeho hodnota v očích veřejnosti roste. Pokud je ale předmětem útoků a lidé kvůli nim přicházejí o finanční prostředky, pak jeho hodnota klesá.

Ve všech třech případech byl také útok prováděn podobným způsobem. Vždy totiž cílil na uživatelské peněženky uložené na platformě burzy či směnárny. Vzhledem k tomu, že poslední zmíněný útok byl proveden v roce 2018, lze usuzovat, že podobné útoky jsou z hlediska výnosnosti pro útočníky stále nejefektivnější. Ačkoli jsou tedy útoky dvojité útraty teoreticky možné, v praxi jsou pro kryptoměnu nejničivější útoky cílené na infrastrukturu spojenou s jeho obchodováním. Na základě těchto tří příkladů se pak konkrétně jedná o krádeže peněženek, kterých je docíleno tak, že se útočníci zmocní klíčů uložených na platformách provozovatelů služeb.

Třetí příklad pak ukazuje poměrně zvláštní vlastnost Bitcoinu a to, že jeho hodnota reaguje na události týkající se i ostatních kryptoměn. To je zejména dáno tím, že lze Bitcoin považovat za vlajkovou loď kryptoměn. Pokud se řekne kryptoměna, nejčastější asociace je právě Bitcoin. Hodnota Bitcoinu tedy také z části závisí na vývoji a bezpečnosti ostatních kryptoměn.

Z těchto důvodů je pak možné usoudit, že nejslabší místo, co se bezpečnosti týče, je pak ve způsobu zabezpečení klíčů. To však neproudí z toho, že by systém Bitcoinu byl nezabezpečený, ale z toho, že s klíči mohou jejich vlastníci zacházet jak se jim zachce. Často je pak jejich zabezpečení podceněno, v důsledku čehož může docházet k úspěšným útokům, které pak způsobují vysokou volatilitu.

7 Závěr

Teoretická část práce seznámila čtenáře s pojmem Bitcoin. Bylo rozebráno jakými specifiky se kryptoměny vyznačují, co konkrétně Bitcoin představuje a jaký byl jeho vývoj. Dále následovaly kapitoly seznamující čtenáře s tím, jakým způsobem lze Bitcoin získat, a jak v rámci systému probíhají transakce. Na závěr byly rozebrány výhody a nevýhody celého systému.

Cílem praktické části práce pak bylo určit jakou roli pro Bitcoinový systém hraje bezpečnost a anonymita. První částí bylo dotazníkové šetření, načež následovala analýza potenciálních útoků na systém a příklady konkrétních úspěšně provedených útoků. Dotazníkové šetření mělo přinést informace o tom, jaké je v současnosti povědomí o Bitcoinu a jaký má význam bezpečnost pro jeho využívání. Analýza potenciálních útoků pak měla odhalit možnosti narušení bezpečnosti jak z hlediska Bitcoinového systému, tak z hlediska infrastruktury s ním spojené. Na příkladech uskutečněných historických útoků jsem pak zjišťoval, jaké konkrétní útoky jsou v praxi využívány a jaké ekonomické důsledky z nich vyplývají.

Dotazníkové šetření ukázalo, že ačkoli většina respondentů měla určité znalosti o Bitcoinu, pouze malá část z nich ho někdy vlastnila či použila. Jako největší překážka pro jeho použití se ukázala vysoká volatilita, následovaná pochybnostmi o bezpečnosti systému.

V rámci analýzy potenciálních útoků bylo rozebráno několik útoků z hlediska jejich technického provedení, potenciální škody a možnosti jejich prevence. Analýza útoků cílících na Bitcoinový systém ukázala, že ačkoli Bitcoinový systém není proti potenciálním útokům zcela immuní, v současnosti neexistuje žádný útok, který by byl efektivní. Jejich problémy zejména leží buď v jejich vysoké technické, finanční a časové náročnosti nebo jednoduchosti jejich prevence. V rámci útoků cílící na infrastrukturu se jeví jako největší nebezpečí krádeže peněženek, a to zejména proto, že zabezpečení klíčů může být uživateli podceňováno. Pokud pak nastane případ, kdy jsou klíče napadeny ve velkém měřítku, mají tyto útoky pak dopad na celý systém.

Na příkladech provedených útoků pak bylo ukázáno, jakými způsoby jsou útoky prováděné v praxi a jaké jsou jejich cenové dopady. Ve všech případech byla cílem útoku Bitcoinová směnárna či burza. Předmětem útoků byla krádež klíčů z online peněženek, využívající různé chyby v zabezpečení serverů. Důsledkem těchto útoků pak

byl prudký pokles hodnoty Bitcoinu, kdy v nejhorším případě nastal až třetinový propad ceny.

I. Summary

This bachelor thesis deals with Bitcoin. It provides an overview how this cryptocurrency works and what are its main security drawbacks.

Theoretical part provides a brief introduction into the world of cryptocurrencies. It explains what is Bitcoin, how it works, its predecessors and goes through its ten year development. Then it explains the specifics of the system such as blockchain and how the system deals with transactions and ownership. Then it also explains advantages and disadvantages of the system. Practical part is split into three parts. The first is a questionnaire that deals with questions regarding the most important drawbacks of the system and how important is the question of security to its users or public. The second part analyzes potential attacks on the system from different standpoints such as their execution or defense against them. Last part deals with actual succesfull attacks and their impacts on the currency.

The goal is to identify what potential attacks are the most dangerous to the system and if they are realized, in what manner they affect the cryptocurrency .

Keywords: Bitcoin, blockchain,, security, anonymity, attacks, transactions

II. Seznam použitých zdrojů

Literární zdroje:

Antonopoulos, A. M. (2015). *Mastering Bitcoin:*. Sevastopol: OReilly.

Narayanan, A. (2016). *Bitcoin and cryptocurrency technologies: A comprehensive introduction*. Princeton, NJ: Princeton University Press.

Reid, Fergal, & Harrigan, Martin. (2012). *An Analysis of Anonymity in the Bitcoin System*. Cornell University Library [online]. USA: Cornell University Library, [cit. 2018-03-22]. Dostupné z: https://arxiv.org/abs/1107.4524

Swan, M. (2015). *Blockchain: Blueprint for a new economy*. Sebastopol: Oreilly.

Heilman, E., Baldimtsi, F., Goldberg, S. (2016). *Blindly signed contracts: Anonymous on-blockchain and off-blockchain bitcoin transactions. In Financial Cryptography and Data Security* – FC 2016 International Workshops, BITCOIN, VOTING, and WAHC. Christ Church, Barbados. [online]. Dostupné z: https://doi.org/10.1007/978-3-662-53357-4_4

Back, A. (2002). *Hashcash - A Denial of Service Counter-Measure.* Dostupné z: http://www.hashcash.org/hashcash.pdf

Franco, P. (2015). *Understanding Bitcoin*. Chichester, West Sussex: Wiley.

Guttmann, B. (2013). *The Bitcoin Bible Gold Edition*. Books On Demand.

Katz, J. and Lindell, Y. (2008). *Introduction to Modern Cryptography*. New York: CRC Press.

Kaushik A., Choudhary A., Ektare C., Thomas D., Akram S. (2017). *"Blockchain — Literature survey"* . Bangalore

McCorry, Patrick & Shahandashti, Siamak & Hao, Feng. (2017). *Refund Attacks on Bitcoin's Payment Protocol*. 581-599. 10.1007/978-3-662-54970-4_34.

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System.* Dostupné z: https://bitcoin.org/bitcoin.pdf

Vasek M., Thornton M., Moore T. (2014). *Empirical Analysis of Denial-of-Service Attacks in the Bitcoin Ecosystem* . DOI: 10.1007/978-3-662-44774-1_5

Vigna, P. and Casey, M. (2016). *The age of cryptocurrency*. New York: Picador USA.

Vijayakumaran, S. (2018) *The Security of the Bitcoin Protocol*. Dostupné z: https://drive.google.com/viewerng/viewer?url=https://www.zebpay.com/pdf/Bitcoin-Security-White-Paper.pdf

Internetové zdroje:

Acheson, N. *(2018) What is Bitcoin?*. Dostupné z: https://www.coindesk.com/information/what-is-bitcoin

Bajpai, P. (2019) *How to Buy Bitcoin.* Dostupné z:https://www.investopedia.com/tech/how-to-buy-bitcoin/

Bestcoinmixer. (2019). Dostupné z: https://bestmixer.io/en

Bitcoin Price History Chart (Since 2009). (2019). Dostupné z: https://www.buybitcoinworldwide.com/price/

Bitcoinclock.com (2019). *Bitcoin Clock: 2020 Bitcoin Halving Countdown*. [online] Bitcoinclock.com. Available at: https://www.bitcoinclock.com/ [Accessed 5 Apr. 2019].

Bitcoinman.cz (2019) *Co je Bitcoin a jak funguje.* Dostupné z: http://bitcoinman.cz/

CoinCube (2019). *Get a Bitcoin Wallet.* Dostupné z: http://coincube.com/get-a-bitcoin-wallet/

Coindesk (2019). *Bitcoin Price Index Real-time Bitcoin Price Charts.*Dostupné z: https://www.coindesk.com/price/bitcoin

Coinsutra (2019). *What is Double Spending & How Does Bitcoin Handle It?*. Dostupné z: https://coinsutra.com/bitcoin-double-spending/

Commons (2019). *Centralised, decentralised, distributed*. Dostupné z: https://commons.wikimedia.org/wiki/File:Centralised-decentralised-distributed.png

Franco, P. (2015). *Understanding Bitcoin.* Chichester, West Sussex: Wiley.

Frankenfield, J. (2018) *Proof of Work.* Dostupné z: https://www.investopedia.com/terms/p/proof-of-work.asp

Grigg, I. (2014) *A Quick History of Cryptocurrencies BBTC — Before Bitcoin.* Dostupné z: https://bitcoinmagazine.com/articles/quick-history-cryptocurrencies-bbtc-bitcoin-1397682630/

Hardyn.cz (2018) *Kryptoměna.* Dostupné z: https://www.hardyn.cz/kryptomena/

Ihodl (2019). *Chart of the Day: Bitcoin Reward Halving and Price History*. Dostupné z: https://ihodl.com/infographics/2018-04-09/chart-day-bitcoin-reward-halving-and-price-history/

Khatwani, S. (2018) *Bitcoin Private Keys* Dostupné z: https://coinsutra.com/bitcoin-private-key/

Khatwani, S. (2018) *Proof of Work vs Proof of Stake.* Dostupné z: https://coinsutra.com/proof-of-work-vs-proof-of-stake-pow-vs-pos/

Kment, V. (2005) *Hašovací funkce: Jak se odolává hackerům*. Dostupné z: https://www.lupa.cz/clanky/hasovaci-funkce-jak-se-odolava-hackerum/

Lielacher, A. (2018) *The History of Bitcoin - What is Hashcash?*. Dostupné z: https://btcmanager.com/the-history-of-bitcoin-part-1-what-is-hashcash/

Mahler, T. (2018) *Public Key Cryptography.* Dostupné z: https://medium.com/blockwhat/public-key-cryptography-a-comprehensive-guide-1e8489e08104

Medium (2019). *Bitcoin Mixing Services.* Dostupné z: https://medium.com/@btcblend/advantages-of-bitcoin-mixing-services-633e4fc07485

Medium. (2019). *Bitcoin's Attack Vectors: Dust Attacks*. Dostupné z: https://medium.com/chainrift-research/bitcoins-attack-vectors-dust-attacks-9040edee2986

Miksa, M. (2018). *Jak koupit bitcoin: 5 způsobů pro investory a spekulanty.* Dostupné z: https://www.zive.cz/clanky/jak-koupit-bitcoin/sc-3-a-191806/default.aspx#part=2

Reiff, N. (2018) *Were there cryptocurrencies before Bitcoin?*. Dostupné z: https://www.investopedia.com/tech/were-there-cryptocurrencies-bitcoin/

Seth, S. (2018) *Are Bitcoin Payment Services Similar to Credit Cards?*. Dostupné z: https://www.investopedia.com/tech/bitcoin-payment-services-introduction/

Swahilpages (2019). *How does the 51% attack occur?*. Dostupné z: https://swahilipages.blogspot.com/2019/01/ethereum-classic-attacked-how-does-51.html

Thompsonreuters (2019). *Are you ready for blockchain?*. Dostupné z: https://www.thomsonreuters.com/en/reports/blockchain.html

Tuwiner, J. (2019) *Bitcoin & Cryptocurrency Wallets.* Dostupné z: https://www.buybitcoinworldwide.com/wallets/

III. Seznam obrázků, tabulek a grafů

Seznam obrázků

Seznam tabulek

Seznam grafů