DIPLOMOVÁ PRÁCE

Kryptoměny a možnosti jejich využití v praxi

Cryptocurrencies and their possible practical use

STUDIJNÍ PROGRAM

Projektové řízení inovací

VEDOUCÍ PRÁCE

doc. RNDr. Bohumír Štědroň, CSc.

BRADOVÁ

MARIE

2020

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

ZADÁNÍ DIPLOMOVÉ PRÁCE

I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení: Bradová Jméno: Marie Osobní číslo: 460758

Fakulta/ústav: Masarykův ústav vyšších studií (MÚVS)

Zadávající katedra/ústav: Oddělení ekonomických studií

Studijní program: Projektové řízení inovací

Studijní obor: -

II. ÚDAJE K DIPLOMOVÉ PRÁCI

Název diplomové práce:

Kryptoměny a možnosti jejich využití v praxi

Název diplomové práce anglicky:

Cryptocurrencies and their possible practical use

Pokyny pro vypracování:

CÍL PRÁCE: Cílem DP je zmapovat a vyhodnotit praktické možnosti využití kryptoměn ve vybraných kavárnách v Praze.
PŘÍNOS PRÁCE: Přínosem DP je rozšíření povědomí potenciálních zákazníků o možnostech využití kryptoměn při platbách a seznámení čtenáře s aktuálními trendy v dané problematice. Výstupem bude článek v odborném časopise s citací použité literatury.
OSNOVA: (1) Úvod; (2) Teoretická část - Historie kryptoměn, Definice základních pojmů, Představení vybraných kryptoměn; (3) Praktická část - Představení a analýza vybraných kaváren v Praze, nabízejících možnost platby kryptoměnou; (4) Závěr

Seznam doporučené literatury:

LÁNSKÝ, Jan. Kryptoměny. V Praze: C.H. Beck, 2018. ISBN 978-80-7400-722-4.
STROUKAL, Dominik a Jan SKALICKÝ. Bitcoin a jiné kryptopeníze budoucnosti. Grada Publishing, 2018. ISBN 9788027107421.
ŠTĚDROŇ, Bohumír a kol. Prognostika. V Praze: C.H. Beck, 2019. Beckova edice ekonomie. ISBN 978-80-7400-746-0.
VEBER, Jaromír a kol. Digitalizace ekonomiky a společnosti. Praha: Management Press, 2018. ISBN 978-80-7261-554-4.

Jméno a pracoviště vedoucí(ho) diplomové práce:

doc. RNDr. Bohumír Štědroň, CSc., ČVUT v Praze, Masarykův ústav vyšších studií

Jméno a pracoviště konzultanta(ky) diplomové práce:

Datum zadání diplomové práce: 20.11.2019 Termín odevzdání diplomové práce: 30.4.2020

Platnost zadání diplomové práce: 30.9.2021

Podpis vedoucí(ho) práce | Podpis vedoucí(ho) ústavu/katedry | Podpis děkana(ky)

III. PŘEVZETÍ ZADÁNÍ

7.4.2020

Datum převzetí zadání | Podpis studenta(ky)

BRADOVÁ, Marie. *Kryptoměny a možnosti jejich využití v praxi*. Praha: ČVUT 2020. Diplomová práce. České vysoké učení technické v Praze, Masarykův ústav vyšších studií.

MASARYKŮV ÚSTAV
VYŠŠÍCH STUDIÍ
ČVUT V PRAZE

Prohlášení

Prohlašuji, že jsem svou diplomovou práci vypracovala samostatně. Dále prohlašuji, že jsem všechny použité zdroje správně a úplně citovala a uvádím je v přiloženém seznamu použité literatury.
Nemám závažný důvod proti zpřístupňování této závěrečné práce v souladu se zákonem č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) v platném znění.

V Praze dne: 10. 05. 2020 Podpis:

Poděkování

Tímto bych chtěla poděkovat panu doc. RNDr. Bohumíru Štědroňovi, CSc. za cenný čas a důvěru při vedení mé diplomové práce. Rovněž děkuji mé rodině a přátelům za podporu během mého studia.

Abstrakt

Diplomová práce se zabývá aktuálním tématem decentralizovaných, čistě digitálních měn – kryptoměn. Teoretická část popisuje kryptoměny od jejich historie a vlastností, až po problematiku jejich využití v praxi. Praktická část je věnována kvalitativnímu šetření mezi uživateli kryptoměn a praktickému využití kryptoměn jako alternativního platidla.

Klíčová slova

Kryptoměny, Fiat peníze, Bitcoin, Litecoin, Platba kryptoměnou

Abstract

The diploma thesis is focused on booming topic of decentralized, purely digital currencies – cryptocurrencies. Theoretical part describes cryptocurrencies from its history and characteristics to the practical application issues. The practical part is devoted to qualitative survey with cryptocurrency users and cryptocurrency practical use as the alternative method of payment.

Key words

Cryptocurrencies, Fiat Money, Bitcoin, Litecoin, Cryptocurrency payment

Obsah

Úvod

Dnešní doba je rychlejší než kdy předtím a ve vyspělých zemích si lidé zvykají, že mohou být v kontaktu s kýmkoli na druhé straně zeměkoule během vteřiny. Tento styl života a zvyšující se nároky populace se bezesporu promítají také do oblasti ekonomie. V současné době u sebe velká část moderní populace již nenosí hotovost, ale je zvyklá platit pomocí karty či mobilního zařízení, které nám umožní přeposlat v podobě nul a jedniček naše peníze, které jsme ani nikdy předtím neviděli, někomu jinému. Dalším faktorem je, že ačkoliv se podoba peněž i názory na jejich ekonomickou povahu v průběhu času měnily, nemůžeme popřít, že vždy hrály a stále hrají v životě lidstva velmi podstatnou roli.

Tyto zmiňované faktory, tedy možnost komunikace na obrovské vzdálenosti takřka bez časové prodlevy a rozsáhlá digitalizace většiny oblastí našeho života, včetně toho ekonomického, daly prostor pro vznik nové formy peněz – kryptoměn. Zkoumání kryptoměn a možností jejich využití ve spotřebitelském životě, je hlavním cílem této diplomové práce.

Diplomová práce je rozdělena na dvě části, část teoretickou a část praktickou. V teoretické části je představena historie kryptoměn, jsou popsány jednotlivé vlastnosti kryptoměnových systémů (včetně těch technických) a přiblížena problematika praktického využití kryptoměn. V praktické části jsou s využitím poznatků z části teoretické zkoumány možnosti využití kryptoměn v praxi ve smyslu jejich využitelnosti jako náhrady tradičních peněz. Závěr práce poté patří návrhům a doporučením, jak s kryptoměnami ve formě platidla nakládat.

Diplomová práce by měla sloužit jako základní zdroj informací osobám, které se chtějí zabývat kryptoměnami a možnostmi jejich využití jako alternativního platidla.

TEORETICKÁ ČÁST

1 PENÍZE

Pro lepší pochopení problematiky kryptoměn a toho, jak mohou být alternací k fiat měnám, je důležité si nejprve představit peníze z ekonomického hlediska, rozdělit si je do jednotlivých kategorií – komoditní peníze, fiat peníze a kryptoměny a tyto kategorie definovat.

Touto problematikou je třeba se také zabývat, jelikož dle studie Světového ekonomického fóra (WEF) a poradenské společnosti Deloitte jsou právě finanční instituce tou oblastí, která projde nejradikálnějšími změnami v důsledku rozšiřování umělé inteligence. (Štědroň, 2019, s. 147)

1.1 Definice peněz

Máme-li definovat peníze co nejpřesněji, je nejprve nutné si vymezit definiční oblast, kterou se budeme zabývat v této diplomové práci, nebude-li stanoveno jinak. Na peníze bude pohlíženo z ekonomického hlediska, nikoliv toho právnického.

Do podoby, která je nám známa nyní, se peníze vyvíjely několik tisíc let. Jak uvádí White (1999, s. 2) idea peněz existovala již dávno předtím, než peníze samotné, ovšem nešlo o laboratorní výzkum či rozhodnutí jedné osoby nýbrž o společenskou dohodu, která danému statku dala onu hodnotu.

Pojem peníze definovala řada ekonomů, jejichž pohledy využijeme k co nejpřesnější interpretaci:

Dle Mankiwa (1999, s. 572) peníze jsou: „Soubor aktiv v ekonomice, jež lidé pravidelně používají k nákupu zboží a služeb od ostatních lidí."

Další definice peněz říká: „Peníze jsou jakékoli aktivum nebo ověřitelný záznam, který je všeobecně přijímán jako platba za zboží a služby nebo splácení dluhů v určité zemi nebo sociálně-ekonomickém kontextu." (Mishkin, 2015, s. 44)

1.1.1 Komoditní peníze

Komoditní peníze jsou první používanou formou peněz. Jednalo se o důsledek vylepšení obchodu a začátek jejich používání nebyl plánován dopředu. (White, 1999, s. 3)

Komoditní peníze jsou založeny na podstatě, že mají vnitřní hodnotu, což znamená, že mají samy o sobě cenu a kromě využití ve formě platidla, mohou sloužit také jako komodita. V pozdější fázi existovaly komoditní peníze i ve formě „bankovek", jejichž princip byl založen na vyplacení dané sumy zlata po předložení „bankovky" v bance. (Von Mises, 1980)

1.1.2 Fiat peníze

Fiat peníze jsou dalším vývojovým krokem v platebním systému, kdy „kousky papíru" zastávají funkci prostředku směny. Výhodou papírové měny je, že je mnohem lehčí, než drahé kovy. (Mishkin, 2015, s. 48)

V Evropě bylo poprvé zaznamenáno využívání fiat měny v 17. století ve Švédsku, kde první centrální banka měla za úkol tisknout peníze pro podporu expanzivní politiky královské rodiny. (Janáčková, 2015, s. 25 - 26)

Fiat měny jsou měny s nuceným oběhem, které jsou garantované a vydávané jednotlivými státy. (Lánský, 2018, s. VII) Národní měna, vezmeme-li její funkci jako prostředek směny, vyjadřuje určitou hodnotu, která byla původně vztažena ke zlatu, takzvaný zlatý standard. [1] Ten měl vést k dlouhodobé stabilitě a fixním směnným kurzům. (Veber a kol., 2018, s. 180 – 181)

Jednou ze zásadních věcí, v čem se liší fiat peníze od peněz komoditních, je, že jejich akceptace již není dobrovolná. Akceptace měny je dána zákonem. (Janáčková, 2015, s. 28 – 29) V České republice se jedná o zákon 136/2011 Sb.

[1] Původní klasický zlatý standard dolaru, který byl platný do roku 1914, znamenal, že jeden dolar byl rovný 1/20 unce zlata. V roce 1929 byl zaveden také zlatý standard koruny, od kterého bylo odstoupeno koncem 80. let.

Na přelomu 19. a 20. století začínají vznikat také bezhotovostní peníze. Oficiálních argumentů, které podporují rušení hotovosti je několik: boj s terorismem, podpora moderních technologií, válka proti šedé ekonomice, atd. V dnešní době tvoří bezhotovostní peníze více než 80% peněžní zásoby České republiky. (Lipovská, 2018, s. 62 – 64)

Pro potřeby centrálních bank vznikly takzvané měnové agregáty, pomocí nichž mohou banky peníze regulovat na základě jednotlivých skupin. (Hrbková, 2015, s. 82-83) Jednotlivé skupiny měnových agregátů uvádí Tabulka 1:

Pasiva	**M1**	**M2**	**M3**
Oběživo	X	X	X
Jednodenní vklady	X	X	X
Vklady s dohodnutou splatností do 2 let		X	X
Vklady s výpovědní lhůtou do 3 měsíců		X	X
Akcie			X
Podílové listy fondů peněžního trhu			X
Repo operace			X
Dluhové cenné papíry do 2 let			X

Tabulka 1: Měnové agregáty

Zdroj: Vlastní zpracování dle (Hrbková, 2015, s. 82-83)

1.1.3 Kryptoměny

Kryptoměny jsou alternativou k fiat měnám. Jsou decentralizované (nemají žádnou centrální autoritu), čistě digitální a využívají kryptografických principů pro potvrzování transakcí. Transakce prováděné pomocí kryptoměn jsou pseudoanonymní[2], nevratné a jejich výhodou je také, že obvykle bývají rychlé a levné. (Lánský, 2018, s. VII)

Před samotným vznikem kryptoměny její vynálezce či skupina, která se podílí na vzniku kryptoměny, vydává takzvaný White paper. Součástí White paper je plán, dle kterého se kryptoměna řídí, jedná

[2] Pojem pseudoanonymní znamená, že jednotlivé transakce jsou vystopovatelné, ovšem neváží se s nimi žádné osobní či citlivé údaje.

se tedy o technické parametry kryptoměny, tedy například co je hlavní doménou kryptoměny, kolik peněz kryptoměna vytvoří a jakou rychlostí se budou tvořit. (Alonso, Koe, 2018, online)

1.2 Funkce peněz

Ať jsou peníze v jakékoliv formě od drahého kamení a zlata po bankovky, mají vždy tři hlavní úlohy, kterými jsou: prostředek směny, zúčtovací jednotka (měřítko hodnoty) a uchovatel hodnoty. (Mishkin, 2015, s. 45)

1.2.1 Prostředek směny

Téměř pro všechny tržní transakce v naší ekonomice jsou peníze využívány jako prostředek směny. Využití peněz jako prostředku směny podporuje ekonomickou účinnost minimalizováním času stráveným výměnou zboží a služeb. (Mishkin, 2015, s. 45)

Fiat měny tuto funkci plní, jelikož zákony jednotlivých států obchodníky nutí platidlo akceptovat. U kryptoměn funguje akceptace na dobrovolné bázi, tudíž obchodníci nejsou povinni kryptoměny přijímat. Kamenných i internetových obchodů a restaurací, kde jsou kryptoměny přijímány nicméně stále přibývá. (Stroukal, Skalický, 2018, s. 63)

1.2.2 Zúčtovací jednotka

Druhou úlohou peněz je poskytování zúčtovací jednotky. To jinými slovy znamená, že jsou využívány k měření hodnoty v ekonomice. Měříme hodnotu zboží a služeb pomocí peněz, stejně jako je například hmotnost měřena v kilogramech. (Mishkin, 2015, s. 46) Kryptoměny tuto funkci prozatím nemají, jelikož trpí vysokou volatilitou cen. To znamená, že kdyby obchodníci stanovili kryptoměnu jako zúčtovací jednotku, museli by velmi často měnit cenu zboží a služeb nebo by hrozilo, že se dostanou do ztráty.

1.2.3 Uchovatel hodnoty

Peníze fungují také jako uchovatel hodnoty, což jinými slovy znamená, že po přijetí peněz nemusí dojít k jejich okamžité útratě. Tato funkce peněz je samozřejmě velmi užitečná. Peníze nejsou je-

diným uchovatelem hodnoty, jakékoli aktivum, ať to jsou právě peníze, zásoby, pozemky, dluhopisy, atd. mohou sloužit jako uchovatel hodnoty. Mnohá z těchto zmíněných aktiv jsou jako uchovatel hodnoty dokonce výhodnější než peníze. (Mishkin, 2015, s. 47)
Zatím není možné označit kryptoměny jako uchovatele hodnoty, je tomu tak z důvodu, že legislativa není zatím kryptoměnám přizpůsobena a ani názor členských zemí Evropské unie není jednotný.

1.3 Forma peněz

Existují dvě základní formy peněz, hotovostní a bezhotovostní, které mají mezi sebou velmi úzký vztah. Tento vztah souvisí se snadnou přeměnou jedné formy peněz na druhou.

1.3.1 Hotovostní forma peněz

Hotovostní formu peněz neboli oběživo tvoří mince a bankovky. V České republice tvoří dnes hotovost zhruba 13% všech peněz. Z důvodu nízké kupní síly docházelo v minulosti také ke stahování mincí z oběhu (naposledy tomu tak bylo s padesátníky, které byly staženy 31. srpna 2008). Naopak význam bankovek stále narůstá vzhledem k inflaci. (Lipovská, 2018, s. 45 - 47)

Mince může být popsána jako kus kovu, který je obvykle kruhovitého tvaru a má předepsanou ryzost a hmotnost daného kovu. Na zadní straně mince se nachází nominální hodnota dané mince a na její přední straně můžeme obvykle nalézt nějakou z charakteristických vlastností země, kde byla mince vyražena.

Bankovky jsou cenné papíry, které byly dříve emitovány jakoukoli komerční bankou. Dříve tedy tyto cenné papíry sloužily jako potvrzení o uložení například zlata či jiných cenných kovů. Až postupem času začaly bankovky plnit funkci peněz, ve smyslu v jakém ho známe dnes. Bankovky jsou tedy cenné papíry, na nichž je vyobrazena jejich nominální hodnota, a jsou vydávány emisní bankou. V případně České republiky se jedná o Českou národní banku. (Vencovský, 2003, s. 173 – 176)

1.3.2 Bezhotovostní forma peněz

Pod bezhotovostní formou peněz si představíme peníze zapsané na bankovních účtech. Jedná se tedy o elektronické neboli digitální

peníze a jeden z typů elektronických peněz představují i kryptoměny. (Lipovská, 2018, s. 45 – 46)

§ 4 zákona č. 370/2017 Sb., o platebním styku, říká že:
„Elektronickými penězi je peněžní hodnota, která

a) představuje pohledávku vůči tomu, kdo ji vybral,
b) je uchována elektronicky,
c) je vydávána proti přijetí peněžních prostředků za účelem provádění platebních transakcí a
d) je přijímaná jinou osobou než tím, kdo ji vydal.“ (Česko, 2017, online)

2 KRYPTOMĚNY

V této kapitole bude čtenář seznámen s historií krypto peněz a kryptoměn samotných. Součástí kapitoly je představení základních pojmů spojovaných s kryptoměnami, především pak Bitcoinem a popis tří kryptoměn, které jsou oblíbené mezi uživateli.

2.1 Historie krypto peněz a kryptoměn

Zřejmě nejznámějším jménem spojovaným s historií kryptoměn je Satoshi Nakamoto, ovšem již dlouho předtím vzniklo několik jiných projektů, které se snažily vyřešit otázku omezených možností kusů kovu a papíru, které ztrácejí hodnotu inflací, jsou pod neustálým dohledem úřadu nebo banky a složitě se přesouvají. (Kaliský, 2018, s. 8)

2.1.1 DigiCash

Jeden z prvních projektů představil v roce 1989 Američan David Chaun. Jednalo se o firmu DigiCash, která provozovala měnu eCash. Chaun se zabýval šifrováním s využitím soukromých a veřejných klíčů, což je dodnes jednou ze základních technologií, které kryptoměny využívají. (Kaliský, 2018, s. 8)

Chaun také definoval, jaké vlastnosti by tyto peníze měly mít:

a) Nemožnost třetích stran určit příjemce, čas nebo částku platby provedenou určitou osobou
b) Schopnost jednotlivce poskytnou důkaz o provedené platbě, nebo za výjimečných okolností identifikovat příjemce platby
c) Schopnost zastavit používání odcizených platebních médií (Chaun, 1982, online)

Společnost bohužel po pár letech zkrachovala, mimo jiné z důvodu Chaunova přehnaného důrazu na bezpečnost a několika špatným manažerským rozhodnutím. Nicméně firma DigiCash byla pro vývoj kryptoměn klíčová, jelikož v ní pracovali lidé, kteří i po krachu společnosti posunuli principy kryptoměn dál. (Kaliský, 2018, s. 8)

2.1.2 Hashcash

Dalším projektem, který se podepsal na vývoji kryptoměn byl systém Hashcash Adama Backa z roku 1998. Jeho princip sahá ovšem až do roku 1992, kdy ho vypracovali Cynthia Dwork a Moni Naor (který také spolupracoval na koceptu eCash). Systém Hashcash bojoval proti emailovému spamu pomocí ověřování vykonané práce neboli Proof of Work (pojem je vysvětlen v podkapitole 2.4.1 Blockchainový souhlasný mechanismus). Při zasílání emailu musel počítač odesílatele věnovat čas a výkon pro nalezení systémem určeného čísla. Pro nalezení správného čísla potřeboval počítat přibližně sekundu a tím dokázal potvrdit, že odesílatel posílá jen omezené množství emailu nikoliv reklamní spam. Pokud by tomu tak nebylo, systém by náročnost hledání správného čísla exponenciálně zvyšoval a počítač zahltil. (Kaliský, 2018, s. 8 - 9)

2.1.3 B-money

Dalším důležitým pokrokem pro dnešní kryptoměny byl koncept B-money, zveřejněný v roce 1998, za kterým stojí programátor Wei Dai. Návrh formuloval systém, při kterém proběhne anonymní transakce, aniž by bylo potřeba zapojit třetí stranu a je vyžadován vklad počítačového výkonu (tzv. Proof of Work). Výsledky poté ověří celá komunita zapojena do sítě a ve veřejném záznamu je uchováván zápis transakcí. Účastníci sítě dedikují výkon pro její potřeby a následně jsou za tuto práci odměněni. Verifikaci transakcí uchovaných ve veřejném účetním záznamu zajišťuje kryptografický hash (pojem je vysvětlen v podkapitole 2.4.3 Hash). Transakce poté měly platit po odeslání do sítě s digitálním podpisem. A také k Nickovi Szabovi, který v roce 1998 navrhl mechanismus „Bit gold" pro decentralizovanou měnu, kde účastníci řeší kryptografické úkoly a řešení následně zveřejňují na otevřeném záznamu. Důležité bylo, že proces byl rozdělen na dílčí úkoly, které byly označeny časovým údajem. Dnes tyto dílčí úkoly nalezneme v blockchainu v podobě bloků – databáze transakcí Bitcoinu. (Kaliský, 2018, s. 9)

2.1.4 E-gold

Společnost E-gold, která vznikla v roce 1996 (ještě před společností PayPal), nabízela mobilní a online platby pro obchody a jednotlivce pomocí vlastní měny. Tato měna byla krytá fyzickým zlatem, uloženým u společnosti. Systémy společnosti se bohužel staly

obětí prvních phishingových útoků[3] a doplatily na nedostatky tehdejších operačních systémů. Přestože tyto útoky společnost ještě přežila, její zánik nastal s teroristickými útoky z 11. září, kdy následně došlo ke zpřísnění legislativy proti financování terorismu a praní peněz (tzv. Patriot act). Přestože se společnost snažila vyhovět novým legislativním požadavkům, byla přinucena, kvůli opatření soudů, negativní publicitě a následné ztrátě důvěry klientů, ukončit svou činnost. Za 13 let svého působení na trhu dokázala společnost obsloužit 5 milionů účtů. (Kaliský, 2018, s. 11)

2.1.5 Liberty Dollar

Jako poslední velký předchůdce kryptoměn je označována měna Liberty Dollar z roku 1998, jejímž tvůrcem je Američan Bernard von NotHaus. (Chen, 2018, online)

Jednalo se o jakési stvrzenky za uskladnění stříbra a zlata, v podobě kovových mincí či papírových bankovek, případně byly v elektronické podobě. Měna byla spravována Národní organizací pro zrušení Federálního rezervního systému a Zákonu o vnitřních příjmech. Již samotný název organizace vyjadřuje její ideologický záměr – odpoutat se od Americké měny, která podléhala rozhodnutím FEDu. Zakladatel měny byl nakonec odsouzen za výrobu a distribuci mincí „podobných mincím Spojených států amerických" (Kaliský, 2018, s. 11)

2.1.6 Historie Bitcoinu

2008 – 2009

Historie Bitcoinu začíná v roce 2008, kdy její zakladatel Satoshi Nakamoto registroval doménu bitcoin.org, která funguje dodnes. Bitcoin jako takový vznikl v roce 2009, kdy Nakamoto zveřejnil program, který umožňuje zapojení do bitcoinové sítě, těžbu a provádění transakcí neboli bitcoinového klienta. Ve stejné době Nakamoto vytěžil prvních 50 Bitcoinů, které vznikly s prvním blokem blockchainu (blok genesis). Poté, co byl kód zveřejněn, se začali

[3] Phishing je podvodná technika, která je využívána k získání citlivých údajů z elektronické komunikace.

přidávat noví nadšenci, kteří novou technologii a měnu testovali a navrhovali úpravy. (Kaliský, 2018, s. 14)

2010

V roce 2010 Satoshi Nakamoto své přístupy k úložištím kódu a doménám Bitcoinu prodal jednomu z klíčových členů komunity, Gavinu Andersenovi, a poté přestal zasahovat do vývoje. (Kaliský, 2018, s. 14)

Je patrné, že Satoshi Nakamoto chtěl utajit svoji identitu a je dokonce možné, že se nejednalo o jednotlivce, nýbrž skupinu odborníků. Řada lidí se snažila tuto záhadu rozluštit, nikomu se to ovšem doposud nezdařilo. Podstatné je, že ačkoliv Satoshi Nakamoto měnu vytvořil, nemá nad ní žádnou moc. (Stroukal, Skalický, 2018, s. 24 – 26)

Kromě zmizení Nakamota se v roce 2010 udály čtyři důležité události:
V květnu proběhla první transakce za Bitcoiny, kdy Laszlo Hanyecz koupil dvě pizzy v hodnotě 41 USD za 10 000 Bitcoinů. Díky této události vznikl takzvaný „Bitcoin pizza index", pomocí kterého novináři přepočítávají, kolik milionů v roce 2010 Laszlo zaplatil za jednu pizzu při aktuální ceně Bitcoinu.

V červenci téhož roku byla přepracována, z původní burzy na obchodování s kartami hry Magic: The Gathering Online, první online burza Bitcoinu, která měla brzy obchodu s Bitcoiny vládnout.

Další událost se stala v srpnu, kdy se v kódu Bitcoinu našla chyba, díky níž někdo vytvořil 184 miliard Bitcoinů mimo pravidla jejich těžby. Uživatelé si chyby a transakcí všimli, chyba byla opravena a pomocí takzvaného forku (nová verze klienta), čili rozdělení blockchainu, byla síť navrácena do původního stavu, ve kterém byla dodržena veškerá pravidla emise.

Za čtvrtou událostí roku 2010 stojí Čech Marek Palatinus, který založit Slush Pool – první bitcoinový těžební pool (první svého druhu), což umožňovalo velké jednorázové odměny pro těžaře. Do té doby bylo možné těžit pouze sám za sebe. Slush pool umožňoval sdružit výpočetní výkon, což bylo nezbytné, jelikož s přibývajícím počtem těžařů se prodlužovala i doba úspěšného vytěžení nového bloku jednotlivcem. V této době také již přestávaly stačit pro

těžbu běžné počítače a přecházelo se na nákladnější zařízení. (Kaliský, 2018, s. 15 – 16)

2011

Popularita Bitcoinu roste. V únoru dosáhl Bitcoin parity s dolarem, což znamená, že se jeden Bitcoin obchodoval za jeden dolar. Do června roku 2011 vyrostla cena Bitcoinu na neuvěřitelných 31,91 USD/BTC, ovšem během čtyř dnů došlo k obrovskému propadu o 70 procent. Toto období začalo být nazýváno Velká bublina roku 2011 a jednalo se o první velkou cenovou bublinu Bitcoinu, kdy na návrat na původní cenovou hladinu 31,91 USD/BTC bylo nutno počkat až do 28. února 2013.

Velké popularity se Bitcoin dočkal také díky umožnění posílat dary serveru WikiLeaks, kteří využívají možnosti internetu k zachování anonymity svých zdrojů, ovšem peněžní toky bylo jednoduše možné zablokovat, k čemuž také došlo poté, co byl server označen Pentagonem jako hrozba národní bezpečnosti Spojených států. Bitcoin si díky umožnění zasílání darů serveru udělal velkou reklamu a v konečném důsledku tak začal skrze dokumenty a informace zveřejněné na tomto serveru reálně měnit i mezinárodní vztahy a diplomacii. (Skalický, Stroukal, 2018, s. 43 – 44)

V roce 2011 došlo také ke vzniku dalších dvou kryptoměn - Litecoinu a Namecoinu, přičemž obě mají stejný programový základ jako Bitcoin. (Kaliský, 2018, s. 16)

2012

Do roku 2012 Bitcoin vstupuje s cenou 5 USD/BTC. Začaly se množit případy krádeží především soukromých klíčů, proto začal být kladen větší důraz na jejich zabezpečení a v této souvislosti začíná vývoj první hardwarové peněženky Trezor.

V roce 2012 také nastal poprvé takzvaný „halving", tedy snížení odměny za těžbu Bitcoinu na polovinu. Systém byl Satoshi Nakamotem navržen tak, aby se Bitcoiny uvolňovaly postupně. První 4 roky byla odměna za nalezený blok 50 Bitcoinů. Dle výpočtů by měl „halving" skončit v roce 2140, kdy dojde k vytěžení posledních zlomků z celkové zásoby 21 000 000 Bitcoinů. Toto opatření způsobuje, že je Bitcoin na rozdíl od fiat peněz deflační, tedy jeho hodnota postupem času narůstá.

Rozšiřuje se počet obchodníků a míst, kde je možno využít Bitcoin k platbě, důležitá byla především platforma Wordpress. (Kaliský, 2018, s. 16 – 17) Bitcoin ovšem jako platidlo nebyl příliš uživatelsky přívětivý. S tímto problémem se povedlo vypořádat společnosti BitPay, která nabídla podnikům přijímat platby v BTC, přičemž došlo k okamžité směně za aktuální kurz dolaru, odečtení poplatku a odeslání prodejci. (BitPay, 2019, online)

2013

Rok 2013 přinesl dramatický nárůst ceny Bitcoinu. Zatímco na začátku roku byla jeho hodnota 87 USD/BTC, na konci roku dosáhl na cenu 1000 USD/BTC.
Významnou událostí pro další směřování Bitcoinu bylo zatčení provozovatele ilegálního online tržiště Silkroad, kde bylo možné za Bitcoiny nakoupit zboží regulované zákonem, především pak drogy a farmaceutické produkty. Spojení se Silkroadem přineslo Bitcoinu další vlnu popularity, ovšem za tu cenu, že je dodnes často v myslích lidí spojován s platbami za nelegální zboží a činnosti. Pravdou ovšem je, že pokud uživatelé využijí Bitcoiny ve spojení s nezákonnou činností, jsou často identifikováni, jelikož záznam transakcí Bitcoinu je veřejný a tudíž ve chvíli, kdy se uživatel například rozhodne obchodovat s Bitocinem na burze, je snadno vystopovatelný. (Kaliský, 2018, s. 17 – 18)

2014

V únoru 2014 došlo k jedné z největších událostí v historii Bitcoinu – zbankrotovala burza Mt.Gox, která ovládala téměř tři čtvrtiny všech obchodů s Bitcoiny. V souvislosti s krachem spadla cena Bitcoinu během roku 2014 strmě dolů až na 340 USD/BTC.

V témže roce ovšem došlo i k pozitivním pokrokům – britský úřad pro výběr daní a cel prohlásil Bitcoiny za soukromé aktivum, což znamená, že z něho není nutné platit daň z přidané hodnoty.

Bitcoinu se dobře vedlo také v České republice, kde v roce 2014 došlo ke dvěma důležitým událostem. První z nich bylo spuštění hardwarové peněženky TREZOR a druhou bylo otevření institutu kryptoanarchie Paralelní Polis v pražských Holešovicích. V budově se kromě prostoru pro přednášky nejen o kryptoměnách nachází také coworkingový prostor, bitcoinový bankomat, 3D tiskárna, ale přede-

vším kavárna, ve které se dá platit pouze Bitcoiny, čímž je jediná svého druhu v České republice.

Přestože během roku 2014 došlo k výraznému propadu ceny Bitcoinu, neznamená to pokles zájmu, což dokázal mimo jiné Microsoft, který se rozhodl jako další přijímat platby v Bitcoinech. (Stroukal, Skalický, 2018, s. 57 – 60)

2015

Rok 2015 byl pro Bitcoin rokem stabilizace a budování důležité infrastruktury kolem sebe. O Bitcoinu vědělo čím dál tím více lidí a začal se aktivně používat v řadách velkých společností, ale především také ve stovkách a tisících malých podnicích po celém světě. Objevila se také řada pokusů o nové využití kryptoměn, například v erotickém a porno průmyslu.

Dalším aktivním Čechem v oblasti kryptoměn byl Vít Jedlička, který na území mezi Chorvatskem a Srbskem založil v dubnu 2015 nový mikrostát nazvaný Liberland. Zpráva o jeho vzniku oblétla celý svět a o občanství měli zájem statisíce lidí. Používanou měnou v novém státě měl být samozřejmě Bitcoin případně jiná kryptoměna, čímž se vzbudil opět po delší době zájem médií o kryptoměny. Jednalo se také o jeden z důvodů nárůstu ceny Bitcoinu, ovšem ty zásadní, kromě rozšířeného přijímání kryptoměn, nastaly v září a říjnu.

V září 2015 spustila bitcoinová velmoc – Čína, rozsáhlé kapitálové kontroly. Investoři s penězi v řádech desítek miliard dolarů začali Čínu opouštět a vláda tudíž rozhodla zavést kontroly přeshraničního toku financí. Světová média začala spekulovat, zda a jakým způsobem se tato událost projeví na ceně Bitcoinu, a pravdu měli ti, kteří tipovali její růst.

K druhé zásadní události došlo v říjnu ve Švédsku, kde Evropský soudní dvůr rozhodl, že na směnu Bitcoinů se nevztahuje DPH. Švédsko se totiž snažilo Bitcoin považovat za zboží, ze kterého by samozřejmě firmy byly nucené odvádět daně. (Stroukal, Skalický, 2018, s. 60 – 62)

2016 - 2017

V roce 2016 se začalo ukazovat, že ti, kdo vytrvali a drželi své Bitcoiny, udělali dobře.

Kromě obchodů přijímajících Bitcoiny, kterých bylo čím dál tím více (v roce 2017 se například k nim přidal i největší český e-shop Alza), se začaly na stranu kryptoměn přiklánět i jednotlivé státy. Vláda Japonska Bitcoin a jemu podobné měny, již v březnu roku 2016 označila za aktivum podobné penězům a následně ho v roce 2017 plně zlegalizovala. Bitcoinové účty nabídla svým klientům také největší norská online banka a o možné spolupráci s kryptoměnami začala mluvit dokonce i vláda Ruska.

Ani v roce 2016 se ovšem Bitcoin neobešel bez problémů. Jedna z historicky největších burz Bitfinex přišla o 120 000 Bitcoinů. V této době to ovšem již nebyl takový problém, jako když došlo k pádu Mt.Gox, jelikož se ztráta naprosté většiny uživatelů vůbec nedotkla (burzy využívali pouze obchodníci s velkými objemy, jelikož již existovaly bankomaty a směnárny).

Začala se projevovat i síla Bitcoinu před znehodnocením měny – z Venezuely, která v roce 2017 byla na pokraji zhroucení, se díky Bitcoinu povedlo utéct řadě lidem, kteří by jinak v době hyperinflace nebyli nikdy schopni na tento radikální krok našetřit.

V roce 2017 opět došlo k prudkému nárůstu hodnoty Bitcoinu, kdy se z hodnoty 1000 USD/BTC vyšplhal až téměř na 20 000 UDS/BTC. (Stroukal, Skalický, 2018, s. 63 – 64)

2018

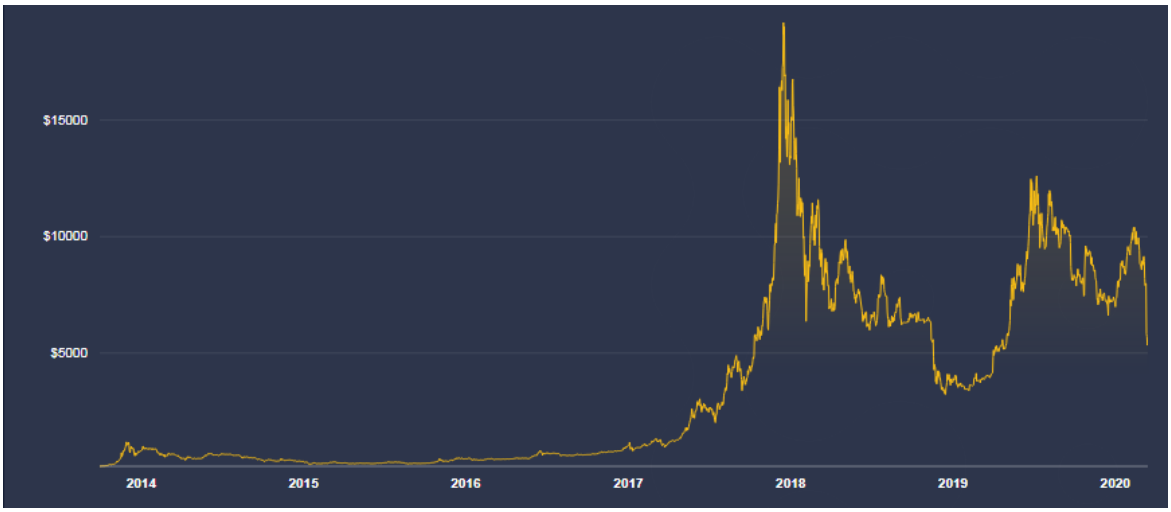
Na začátku roku 2018 se dostalo do oběhu 80% z celkového počtu (21 000 000 BTC) všech Bitcoinů, které budou kdy vytěženy.

Rok 2018 byl pro Bitcoin a jeho uživatele těžkým rokem. Mnoho uživatelů předpokládalo, že cena bude nadále stoupat, proto Bitcoiny drželi. Nastal ovšem přesný opak, když se na začátku února Bitcoin propadl o více než polovinu své hodnoty a tím pokles hodnoty zdaleka nekončil – na konci roku 2018 byla hodnota Bitcoinu méně než 4000 USD. Pokles na začátku roku odborníci přisuzují krokům vlády Jižní Korey (země, kde se uskutečňuje většina transakcí s Bitcoiny), která nařídila odhalení totožnosti obchodníků s Bitcoiny. (BitcoinWiki, online)

2019

V roce 2019 se Bitcoin opět vzpamatovává z prudkého poklesu a na počátku července došlo k extrémnímu vzrůstu ceny až na 12 500 USD. (BitcoinWiki, online)

2.1.7 Historický vývoj ceny Bitcoinu



Obrázek 1: Historický vývoj ceny Bitcoinu

Zdroj: Coindesk (online)

2.2 Kryptografie

Kryptografie je matematická disciplína zabývající se šifrováním, které můžeme vysvětlit jako převod zpráv z/do utajené podoby, jež můžeme přečíst pouze se znalostí šifrovacího klíče. V případě, že klíč k dešifrování zprávy je odlišný od klíče k jejímu zašifrování, mluvíme poté o asymetrické kryptografii. Kryptoměny využívají kryptografii ke svému bezpečnému fungování, zejména pak takzvané hashovaní funkce a digitální popis. (Stroukal, Skalický, 2018, s. 25)

2.3 Těžba

Těžba neboli mining je proces, při kterém je hledán další blok pro napojení do blockchainu pomocí strojově náročného výpočtu. Těžbu si tedy lze představit jako hledání řešení náročné matematické úlohy. Blok je nalezen, jestliže je splněna podmínka, že jeho hash je nižší než určitý cíl. Tento cíl je odvozen z momentální obtížnosti, k jejíž změně dochází každých 2016 bloků v závislosti na

rychlosti jejich nalezení, přičemž požadujeme, aby průměrná rychlost vygenerování jednoho bloku Bitcoinu činila 10 minut. Pokud tato podmínka na nízký hash není splněna, musí dojít k pozměnění serializace bloku a přepočítání hashe.

S náročností řešené úlohy samozřejmě souvisí počet například Bitcoinů v oběhu – čím vyšší množství Bitcoinů je v oběhu, tím menší odměnu těžař dostane a čím více těžařů se snaží přijít na řešení dané úlohy, tím je úloha náročnější.
V počátcích Bitcoinu tudíž byla těžba velmi jednoduchá a prováděla se na procesorech samostatných osobních počítačů. Dnes je již obtížnost řešené úlohy tak vysoká, že vezmeme-li 500 nejvýkonnějších počítačů na světě, výkon celé bitcoinové sítě je 20 000x vyšší.

Aby tedy bylo možné dosáhnout dostatečného těžebního výkonu, začali se těžaři sdružovat ve velkých skupinách, takzvaných poolech. Mezi největší pooly patří například BTC.com, AntPool, ViaBTC, český Shush pool, F2Pool, 58Coin nebo BTCC pool. V poolu tedy těžaři těží společně a vygenerované transakce včetně poplatků plynou poolu, který je následně přerozděluje. Jelikož je konkurence mezi pooly vysoká, mohou si těžaři vybírat podle podmínek, které mají jednotlivé pooly různé – na některých se platí poplatky, některé si ponechávají transakční poplatky, atd. Těžař samozřejmě může těžit i mimo pool, ale je to více rizikové. Pool zajišťuje těžařům sice menší výdělek, avšak v pravidelných intervalech.

Je tedy pravda, že těžit může kdokoliv, ovšem aby těžba byla výnosná, je třeba investovat velmi vysoké sumy do technického vybavení, mít přístup k levné elektřině a chlazení a počítat s velkými investicemi i do budoucna, jelikož vývoj jde dopředu radikální rychlostí. (Stroukal, Skalický, 2018, s. 82 – 87)

2.4 Blockchain

Blockchain neboli v překladu Řetěz bloků je spojový seznam (seznam, ve kterém je odkazováno na předky) bloků. Ke spojení dochází díky obsažení hashe (viz podkapitola 2.4.3 Hash) předchozího bloku v datech následujícího bloku. Kromě tzv. bloku genesis, tedy úplně prvního bloku, má každý blok jednoznačně určeného předka, nedochází tedy k zacyklení. Naopak vzniká strom bloků, kde navíc dochází k větvení velmi zřídka. Strom bloků tedy vypadá spíše jako jedna větev, přičemž se vždy pracuje pouze na té nejdelší, přesněji na té, jejíž bloky dalo nejvíce práce spočítat, a ta je nazývá-

na blockchain. Bloky, které jsou součástí nepokračujících větví, jsou ignorovány. Naopak bloky obsažené v blockchainu a transakce, které jsou v nich zahrnuté, se dají považovat za potvrzené.

Díky této koncepci je zaručena nepřepsatelnost historie, neboť k modifikaci bloku uprostřed blockchainu by bylo zapotřebí přepočítat veškeré následovníky. (Stroukal, Skalický, 2018, s. 28)

2.4.1 Blockchainový souhlasný mechanismus

Proof of Work (PoW) – Nejstarším využívaným matematickým algoritmem pro tvorbu bloků je algoritmus zvaný Proof of Work neboli důkaz prací. Při tvorbě bloku pomocí PoW se používá pojem těžba bloku (mining), přičemž těžaři hledají řešení složitého matematického problému, který má vést k nalezení části hash-bloku, který nese informace o bloku předchozím. Odměněn je následně těžař, který nalezne hash jako první.
Složitost náročnosti těžby daného bloku není stále stejná, ale v čase dochází ke změnám, což se vyvíjí od faktu, že počet těžařů a jejich výpočetní výkon také není stabilní. Tedy dochází-li k nárůstu počtu těžařů, dochází také ke zvyšování obtížnosti matematických výpočtů, což má zabránit rychlejší emisi kryptoměn, než byl původní plán jejich tvůrců. (Lánský, 2018, s. 23 – 24)

Proof of Stake (PoS) – neboli důkaz podílem je jedním z alternativních mechanismů k dosažení konsenzu na rozšíření kryptoměnového systému o další blok. Na rozdíl od důkazu prací se zde nepoužívá pro vytvoření nového bloku pojem těžba, nýbrž pojmy ražení bloku (minting) nebo slévání bloku (forging). (Lánský, 2018, s. 32)

Proof of Work and Proof of Stake (PoW + PoS) – hybridní model souhlasného mechanismu PoW + PoS je v posledních letech využíván stále častěji. Je tomu tak z důvodu nižší energetické náročnosti a systém je tím pádem spravedlivý i pro těžaře, kteří nedisponují tak vysokou výpočetní silou. Princip tohoto modelu je takový, že první část kryptoměn je vytěžena pomocí mechanismu Proof of Work a po určité době, kdy je na ověření bloku predikována vyšší náročnost, se přejde na mechanismus Proof of Stake. (HCash, online)

Proof of Importance (PoI) – neboli „Důkaz důležitosti" je nejméně rozšířeným souhlasným mechanismem. PoI funguje na principu hledání důležitého uživatele. Důležitost uživatele je hodnocena pomocí několika kritérií: kolik operací provedl uživatel v platební síti,

jak dlouho je v síti aktivní a jaké má množství peněz na účtu. (Asolo, 2018, online)

2.4.2 Double spending problem

Double spending problem neboli problém dvojité útraty je riziko, že bude digitální měnu možné utratit dvakrát (ačkoliv se jedná o termín spojovaný poslední dobou především s kryptoměnami, jedná se o problém všech digitálních měn). K tomuto problému dochází, pokusí-li se uživatel duplikovat kód transakce, což jinými slovy znamená, že pro dvě různé platby použije stejný kód. Požaduje-li ovšem uživatel potvrzení obou transakcí, nemůže k tomu dojít a validní bude pouze ta, která byla dříve zapsána do blockchainu. (Frankenfield, 2019, online)

2.4.3 Hash

Důležitou funkcí pro fungování blockchainu a tedy i systému kryptoměn je tzv. hashovací funkce. Tato funkce funguje na principu, kdy vstup, kterým je množina dat obecné délky, je převeden na výstup (hash) množiny dat omezené délky. Nejčastěji se jedná o 256 bitů, v případě použití nejaplikovanějšího algoritmu, SHA-256. (Stroukal, Skalický, 2018, s. 84)

SHA-256 – hashovací funkce SHA-265 je využívána mimo jiné nejrozšířenější kryptoměnou Bitcoinem (v případě Bitcoinu je funce aplikována dvakrát po sobě). Porovnáváme-li SHA-256 s hashovacím algoritmem Scrypt, má SHA-256 vyšší náročnost výpočetního výkonu. Tato charakteristická vlastnost tedy také ovlivňuje dobu těžby bloku, která je u Bitcoinu 10 minut, zatímco u Litecoinu to jsou pouze 2,5 minuty. (Lánský, 2018, s. 24)

SCRYPT – jak již bylo zmíněno hashovací funkce Scrypt je v porovnání s funkcí SHA-256 méně náročná na výpočetní výkon, je tomu tak ovšem proto, že spadá do třídy paměťově těžkých algoritmů neboli memory hard. Funkce spadající do této třídy vyžadují pro svůj výpočet maximální možnou paměť, jakou může tento algoritmus s danou časovou složitostí vyžadovat. Příkladem kryptoměny využívající hashovací fukci Scrypt je Litecoin. (Lánský, 2018, s. 26)

CryptoNote – k vytvoření hashovací funkce CryptoNote došlo, jelikož se její autoři snažili vylepšit nedostatky hashovací funkce

Bitcoinu. Mezi hlavní cíle patřilo zvýšení anonymity odesílatele platby, příjemce platby a také hodnoty transakce. Příkladem kryptoměny využívající hashovací funkci CryptoNote je Monero. (Saberhagen, online)

2.5 Výčet vybraných kryptoměn

Obsahem této kapitoly je popis tří uživatelsky oblíbených kryptoměn, které mají některé znaky společné, ovšem každá využívá jiné hashovací funkce.

2.5.1 Bitcoin

Bitcoin je vůbec první kryptoměnou, která kdy vznikla. Stalo se tak v roce 2008, kdy osoba či skupina osob vystupující pod jménem Satoshi Nakamoto zaregistrovala doménu bitcoin.org (více v podkapitole 2.1.6 Historie Bitcoinu). Bitcoin vznikl jako „open source" projekt, což jinými slovy znamená, že jeho zdrojový kód je veřejně dostupný, tudíž na jeho základě mohou vznikat nové kryptoměny.

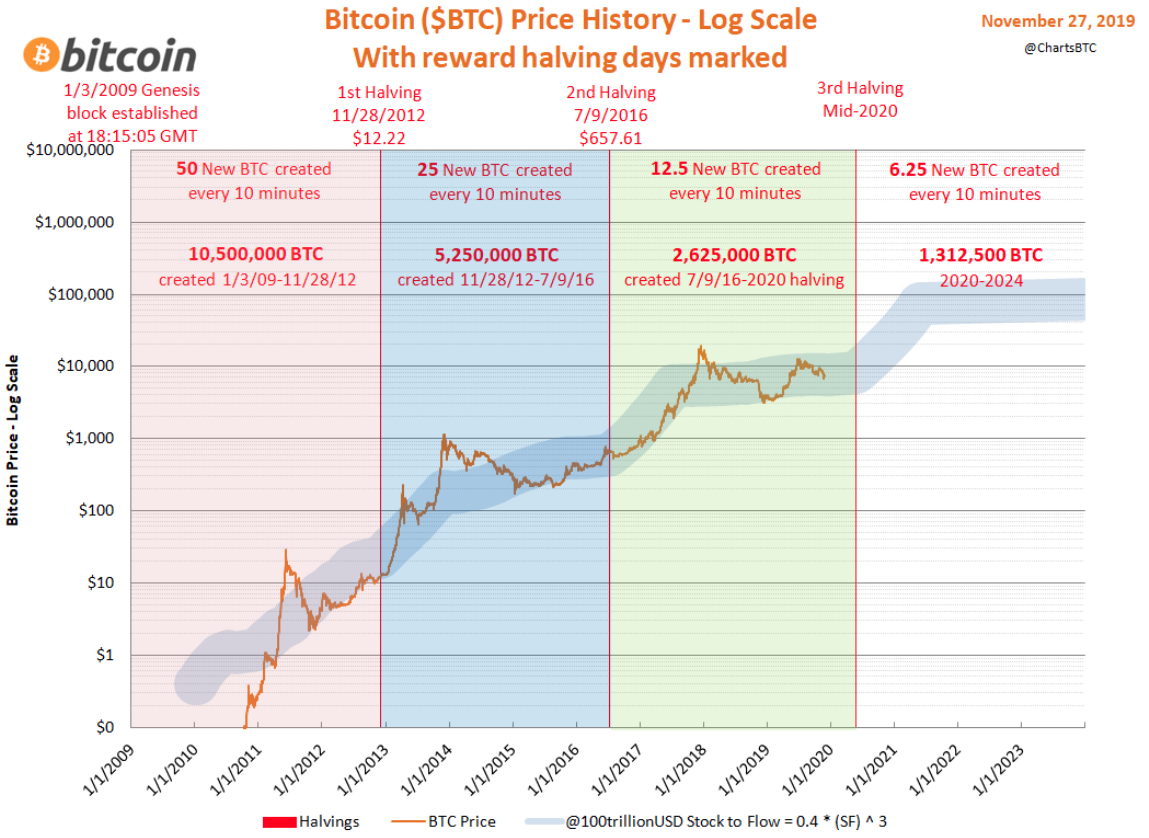
Jedná se o decentralizovanou peer-to-peer[4] digitální měnu, jenž je nejpopulárnějším příkladem užívajícím technologii blockchain. (Crosby a kol., 2015)

Bitcoin je kryptoměnou s nejvyšší tržní kapitalizací, která k dnešnímu dni 29. 3. 2020 činí téměř 114 miliard dolarů. Bitcoin má pevně danou rostoucí peněžní zásobu, (to znamená, že je daný maximální počet mincí, který bude kdy vypuštěn do oběhu), která činí 21 milionů BTC. Mince jsou, na základě matematického algoritmu, do oběhu uvolňovány postupně a k dnešnímu dni je jich již v oběhu 18 293 025 BTC. (Coinmarketcap.com, online)

Satoshi Nakamoto vytvořil emisní plán, který limituje generování nových Bitcoinů. Jak již bylo řečeno, maximální vydaný počet mincí do oběhu činí 21 milionů BTC, což uvádí právě emisní plán. Na počátku procesu těžby byla odměna za vytěžený blok 50 BTC, ale každé čtyři roky dochází k takzvanému půlení, kdy odměna klesá na polo-

[4] Pojem peer-to-peer (P2P) označuje typ počítačových sítí, kde všechny uzly jsou si rovny a klienti spolu komunikují přímo (bez existence centrálního uzlu). (Stroukal, Skalický, 2018, s. 24)

vinu, přičemž doba generování jednoho bloku je rovna deseti minutám. (Nakamoto, 2008, online)



Obrázek 2: Historie půlení BTC

Zdroj: Coinmama (online)

Jak můžeme vidět z Obrázku 2, k dalšímu půlení dojde v letošním roce, konkrétně by k němu mělo dojít v týdnu začínajícím 18. května 2020. (IG, online)

2.5.2 Litecoin

Za vznikem kryptoměny Litecoin (LTC) stojí Cherlie Lee, který její vznik oznámil 9. 10. 2011 a jejíž těžba započala o čtyři dny později (aby se zájemci mohli účastnit těžby již od jejího počátku). Litecoin byl založen, aby konkuroval Bitcoinu, což dokazuje i slavná fráze „Bitcoin je zlato, Litecoin je stříbro", která byla zveřejněna v příspěvku o vzniku Litecoinu.

Litecoin využívá jiného algoritmu než Bitcoin a tím je hashovací funkce Scrypt. Doba těžby jednoho bloku je 2,5 minuty (tedy 4x mé-

ně než u Bitcoinu) a stejně jako Bitcoin pracuje v síti P2P, tedy jeho zdrojový kód je veřejně dostupný. (Lánský, 2018, s. 26)

Tržní kapitalizace Litecoinu je k dnešnímu datu (29. 3. 2020) více než 2,48 miliardy dolarů. Jedná se tak v současné době o kryptoměnu se sedmou nejvyšší tržní kapitalizací na světě. Stejně jako Bitcoin, má i Litecoin pevně danou rostoucí peněžní zásobu, maximální počet LTC, které kdy budou vytěženy je 84 milionů a nyní je již v oběhu 64 390 668 LTC. (Coinmarketcap.com, online)

Také u Litecoinu dochází každé čtyři roky k půlení, v současné době je tedy odměna za těžbu rovna 12,5 LTC za vytěžený blok. (Lite Coin White Paper, online)

2.5.3 Monero

Kryptoměna Monero (XMR) vznikla 18. 4. 2014, kdy se oddělila od kryptoměny Bytecoin. Hlavním důvodem oddělení bylo velké množství vytěžené měny a malá transparentnost operací.

Na vzniku Monera se podílelo 7 vývojářů, z nichž dva odhalili svoji identitu. Jde o Davida Latapie a Riccarda Spagni, zbytek skupiny se rozhodl zůstat anonymní a vystupují pod pseudonymy. (Alonso, Koe, 2018, online)

Monero je kryptoměna založená na protokolu CryptoNote, rozšiřuje ho ještě dále o anonymizační schopnosti, kdy není vidět placená částka, ani odesílatel a příjemce platby. Anonymita je u kryptoměny Monero, na rozdíl od jiných kryptoměn, povinná. Pro Monero je typické využívání čtyř klíčů (například u Bitcoinu jsou to dva – soukromý a veřejný) – veřejný platební klíč, veřejný prohlížecí klíč, soukromý platební klíč a soukromý prohlížecí klíč. Každý z klíčů má svoji funkci a je využíván k typickému úkonu. Veřejné klíče jsou využívány k anonymizaci transakce, kdy na základě náhodného čísla a právě těchto dvou klíčů jsou generovány tzv. stealth address, což je adresa, ze které jsou jednotlivé transakce odesílány. Právě k provádění plateb slouží soukromý platební klíč a soukromý prohlížecí klíč prokazuje vlastnost kryptoměny. (Alonso, Koe, 2018, online)

Dalším cílem kryptoměny Monero je nezávislost těžby na speciálních ASIC strojích, tedy chce zachovat možnost těžby na klasických grafických kartách a procesorech. Hlavním důvodem, vedoucím k tomuto

rozhodnutí, je nemožnost získat nadpoloviční většinu v síti. Srovnáme-li to s Bitcoinem, ten naopak možnosti těžby nijak nereguluje a i z tohoto důvodu se pro jeho těžbu využívají speciální ASIC stroje pro těžbu. Dochází tedy ke sdružování do poolů v zemích s levnou elektrickou energií a jednoho dne se tedy může klidně stát, že v této zemi vznikne takové množství poolů, které bude vlastnit více než 51% v síti a dojde tak k možnosti ovlivnit Bitcoin. Monero se tedy naopak snaží cílit na jednotlivce, kteří těží na grafických kartách a procesorech, a pravděpodobnost ovládnutí více než 51% v síti je tak minimální. (Wilmoth, 2018, online)

V souvislosti s kryptoměnou Monero je také důležité si vysvětlit pojem „Hardfork". Hardfork je změna protokolu, o které můžeme říci, že bloky a transakce vytvořené podle pravidel nových nejsou validní podle pravidel starých. (Stroukal, Skalický, 2018, s. 127) V případě kryptoměny Monero se jedná o změnu protokolu, která by měla zamezit přechodu na těžbu na ASIC strojích. Konkrétně při hardforku dojde k rozdělení kryptoměny na krytpoměny dvě, čímž dojde ke snížení hashovací rychlosti. (Alonso, Koe, 2018, online) K poslednímu hardforku u Monera došlo 30. listopadu loňského roku. (Batabyal, 2019, online)

Dle tržní kapitalizace obsazuje Monero v současné chvíli (29. 3. 2020) dvanáctou příčku s hodnotou téměř 819 milionů USD. (Coinmarketcap.com, online) Princip nastavení peněžní zásoby je opět částečně odlišný od Bitcoinu i Litecoinu. Stejně jako u výše zmíněných kryptoměn je také u Monera postupně snižována odměna za těžbu, až dojde k vytěžení celkového počtu 18,4 milionu mincí XMR. K tomu by však mělo dojít již v roce 2022 a uživatelé by tak z důvodu narůstajících transakčních poplatků mohli být odrazeni Monero dále používat. Proto se skupina vývojářů stojící právě za touto kryptoměnou rozhodla, že i po vytěžení 18,4 milionů mincí bude docházet k nárůstu jeho peněžní zásoby a to tempem 0,3 XMR za minutu. (Alonso, Koe, 2018, online)

2.6 Uživatelské pohledy na kryptoměny

Obsahem této kapitoly je představení hlavních výhod a nevýhod uživatele kryptoměny.

2.6.1 Plátce platby

Jednou z výhod pro plátce, tedy pro osobu užívající kryptoměnu k platbě za určitou komoditu, je časová nenáročnost ke schválení transakce. Zásadně zde ovšem závisí na kryptoměně, která je pro platbu zvolena. Pro potřeby této diplomové práce bude v této kapitole pracováno s jedním zástupcem decentralizované kryptoměny – Bitcoinem a jedním zástupcem centralizované kryptoměny – Ripple (XRP). U Bitcoinu je doba mezi zadáním transakce a jejím potvrzením přibližně jedna hodina. U centralizované kryptoměny je tato doba značně kratší, prodleva je téměř nulová.

Další výhodou pro plátce jednoznačně je, že transakce není závislá na geografické poloze. K uskutečnění transakce je nezbytné pouze zařízení s přístupem k internetovému připojení. Mimo jiné to také znamená, že za platby prováděné ze zahraničí (v našem případě mimo Českou republiku) neplatíme žádné poplatky navíc, jako to může být u některých bank.

Nespornou výhodou je také anonymita, která plátci zůstává u veškerých proběhlých transakcí. V dnešní době si většina uživatelů ani neuvědomuje, kolik soukromých dat je z jejich pohybu ve virtuálním světě sbíráno a prodáváno třetím stranám. V případě platby kryptoměnou o plátci nezůstávají žádné informace, kromě hash kódu jeho peněženky. (Horčička, 2019, online)

2.6.2 Příjemce platby

Jednou z největších výhod pro příjemce platby je jednoznačně časová nenáročnost pro akceptaci platby. Rozhodne-li se obchodník přijímat ve svém podniku platby například v Bitcoinech, musí pro to udělat pouze několik jednoduchých kroků. Nejprve si musí založit bitcoinový účet a zvolit si správce poskytovatele plateb. Dále je nutné už jenom vyplnit pár nezbytných údajů, jakými jsou například bankovní účet (příjemce tímto krokem ztrácí anonymitu, ale získává tím možnost přijímat transakce vyšší než 1000 USD měsíčně) a měnu, ve které budou Bitcoiny směňovány. (Vpnmentor.com, 2020, online)

Využít výhody, kdy jsou transakce odeslány bez zpoždění, mohou především online obchody, které odesílají zboží až po obdržení platby. U kryptoměn je možné tento čas významně snížit, navýšením částky za zprostředkování transakce. Tyto částky jsou uváděny v jednotkách Satoshi, přičemž 0,00000001 BTC je rovno jedné jed-

notce Satoshi, což odpovídá jednomu bytu transakce. Abychom docílili toho, že transakce proběhne bez zpoždění, bylo by nutné mít nastaven poplatek 29 Satoshi na byte a více. S transakcemi souvisí také již u plátce zmíněná nezávislost na geografické poloze, kdy pro obchodníka to má tu výhodu, že může získat více zákazníků ze zahraničí.

Další výhodou, které mohou využít především větší obchodníci, kteří se rozhodnou přijímat kryptoměnu, je stále poměrně velký zájem médií o kryptoměny. Společnost si tak může udělat PR téměř zadarmo, jako toho například využila v roce 2017 společnost Alza. (Fillner, 2017, online)

Pro příjemce plateb je také velice výhodné, že kryptoměny fungují jako open source projekt, což znamená, že mohou být zdokonalovány téměř kýmkoliv. Kryptoměny tedy reagují na potřeby svých uživatelů například zvýšením anonymity, urychlením transakcí, atd.

Ačkoliv se zdá, že přijímání kryptoměn přináší obchodníkům pouze výhody, samozřejmě tomu tak není. Systém kryptoměn má i řadu nevýhod, které jsou uvedeny ve zbylé části této kapitoly.

První nevýhodou je jednoznačně vysoká volatilita kryptoměn, to jinými slovy znamená, že se neustále mění jejich cena v čase. Dochází k velkým nárůstům, ale i propadům cen, čehož někteří uživatelé využívají a v obdobích, o kterých se domnívají, že je to pro ně výhodné, směňují kryptoměny zpět na fiat měny. To může zapříčiňovat i pád tržní ceny, což může mít mimo jiné za důsledek i vzdalování se okamžiku, kdy budou kryptoměny uznány jako platidlo. V současné chvíli se jedná spíše stále pouze o instrument vhodný k investicím či spekulacím.

Transparentnost respektive její nedostatek může být také považován za jednu z nevýhod kryptoměn. Jak již bylo zmiňováno, identita tvůrců kryptoměn je většinou neznámá. Uživatelé stejně tak mohou postrádat dostatečné informace o budoucím směřování kryptoměny a obecně jejím fungování.

Problémy s likviditou – k tomuto problému dochází z důvodu, který může potkat každou měnu, která nebyla doposud uznána jako oficiální platidlo a tím je pokles zájmu od běžných uživatelů. Obchodníci přijímají kryptoměny především ze zájmu o moderní technologie a je to pouze projev jejich dobré vůle, budou-li ovšem kryptoměny ztrá-

cet na hodnotě, obchodníci je nebudou chtít přijímat a bude hrozit pokles likvidity kryptoměn.

Anonymita – v jedné z předchozích kapitol byl zmiňován blockchain, kde jak víme, je možné dohledat jakoukoli uskutečněnou transakci, konkrétně výši platby a adresu, z které byl příkaz k platbě zadán. Víme-li, komu tato adresa patří, již transakce není anonymní, ale hovoříme o takzvané „pseudoanonymitě". Ke komplikacím s anonymitou může dojít v případě, kdy v decentralizované síti udělá uživatel chybu a odešle transakci někomu jinému. V takovém případě nejen, že není možnost zjistit, o koho se jedná, ale ani není možné vyžadovat navrácení peněz, jelikož v decentralizované síti neexistuje nadřazená osoba, která by to mohla vyžadovat. S rostoucí hodnotou kryptoměn jsou spojené také hackerské útoky, kdy v případě decentralizované sítě opět bohužel neexistuje cesta, jak své prostředky získat zpět. Uživatel může snadno o své prostředky přijít také ztrátou kryptografického klíče.

Další nevýhodou je závislost na moderních technologiích, jakými jsou mobilní zařízení (např. mobilní telefon, tablet, notebook), internetové připojení a elektrická energie. Je tomu tak, jelikož kryptoměny a blockchain neexistují v hmatatelné podobě. To samozřejmě také zapříčiňuje největší rozvoj kryptoměn v oblastech, kde je vybudována kvalitní telekomunikační infrastruktura.

Přestože ve většině zemí nejsou kryptoměny legislativně omezovány, existuje pár výjimek, kde zákony o kryptoměnách již vyšly v platnost. Jedním příkladem je Kanada, kde byl v roce 2014 vydán zákon, řadící kryptoměny mezi cenné papíry. (Millan, 2014, online) Přísnější regulační politiku zastává Čínská lidová republika, kde byl obchod s kryptoměnami zakázán, z důvodu velkého odlivu kapitálu mimo stát právě pomocí kryptoměn. (Akolkar, 2018, online)

2.7 Užívání kryptoměn v praxi

Se všeobecně rostoucím zájmem o kryptoměny a rostoucím počtem obchodníků, kteří nabízí možnost platby kryptoměnou ve svých kamenných i internetových obchodech, roste také počet osob, které chtějí kryptoměny k platbám používat.
V této kapitole bude teoreticky představeno, jak probíhá užívání kryptoměn v praxi.

2.7.1 Pořízení peněženky

Prvním krokem, který musí osoba, která má zájem o používání kryptoměn udělat, je pořízení peněženky. Peněženka, stejně jako tomu je u tradičních peněz, slouží k ukládání peněz a existuje několik možností jak to udělat. Kryptoměnu si můžeme představit jako unikátní kód, který musí být někde uložen. Může být uložen na počítači, na paměťové kartě či externím disku, uživatel ho může zaslat do zašifrovaného úložiště na internetu, případně je i možné si ho napsat na papír a ten dobře uložit. Uživatelé, kteří mají v plánu investovat do kryptoměn větší částky, si mohou také pořídit speciální bezpečnostní hardware.

Software oficiálního bitcoinového klienta

Prvním způsobem pořízení peněženky je stažení si softwaru oficiálního bitcoinového klienta z webových stránek bitcoin.org. To ovšem není příliš uživatelsky přívětivé, především pro začátečníky, jelikož software v sobě ukládá celý blockchain a tedy například u Bitcoinu dosáhla velikost databáze již na konci roku 150 GB. Blockchainy ostatních kryptoměn zatím mají řádově menší velikosti.

Softwarová peněženka

Druhou, velikostí mnohem úspornější volbou je softwarová peněženka. Tou pravděpodobně nejpopulárnější je program Electrum, který si uživatel snadno nainstaluje do počítače. V programu je snadné si vytvořit novou peněženku a tu uložit do libovolného úložiště. Soubor je také možné snadno zálohovat. I u softwarové peněženky je zásadní bezpečné uložení hesla. V programu je také snadné zjistit adresu vytvořené peněženky a pomocí této adresy je již možné přijímat kryptoměny. Pokud již máte v peněžence nějaké kryptoměny nahrané, je možné je někomu zaslat, stačí znát jeho adresu. Při posílání kryptoměn je důležité myslet na poplatek za transakci.

Webová peněženka

Třetím způsobem, jakým je možné si pořídit peněženku, je její online verze. Webové peněženky jsou velice uživatelsky přívětivé a jednou z nejpopulárnějších je coinbase.com případně blockchain.info. Webová peněženka má tu nevýhodu, že uživatel nad ní nemá plnou kontrolu, jelikož svěřuje své kryptoměny třetí straně. V případě, že uživatel plánuje v peněžence uchovávat vyšší sumy kryptoměn, nejsou ty webové příliš bezpečnou volbou. Webové peně-

ženky fungují podobně jako softwarové peněženky a pro jejich založení stačí na dané stránce vyplnit email a heslo. Ve většině peněženek je také možné při posílání platby zadat namísto adresy pouze email nebo telefonní číslo adresáta, kterému poté přijde upozornění na vyzvednutí platby, při registraci pod přiloženým odkazem.

Mobilní aplikace

Posledním, a v dnešní době nejspíše uživatelsky nejpřívětivějším způsobem, jak si kryptoměnu pořídit a držet ji, je stažení mobilní aplikace do chytrého telefonu. V závislosti na operačním systému může uživatel volit z řady aplikací, které fungují podobně jako softwarová peněženka Electrum, s tím rozdílem, že máte své kryptoměny vždy po ruce. Mezi nejoblíbenější patří opět aplikace Coinomi, kterou si mohou stáhnout jak uživatelé Androidu, tak iOS. Při instalaci vyzve peněženka uživatele k opsání takzvaného seedu, jedná se o již zmiňované heslo, které je tím nejdůležitějším pro přístup k účtu s kryptoměnami. Doporučuje se opsat slova na papír a ten pečlivě uschovat, namísto zapsání do mobilního telefonu či počítače, který může být snadno odcizen.

Užívání mobilní peněženky je opět velice intuitivní a uživateli stačí tři hlavní záložky, kterými jsou: „Send", „Balance" a „Recieve". V záložce „Send" stačí vyplnit adresu příjemce a částku, kterou chceme odeslat, případně využít čtečky QR kódu, která po přečtení obrázku předvyplní adresu i obnos a stačí pouze potvrdit odeslání. Druhá záložka „Balance" ukazuje uživateli zůstatek a umožňuje také zobrazení transakční historie. V záložce „Recieve" je možné pouze vyplněním částky vygenerovat QR kód pro přijetí platby.

Výhodou aplikace Coinomi je také integrovaná P2P směnárna, kde lze snadno vyměnit jednu kryptoměnu za druhou, například Bitcoin za Litecoin. (Stroukal, Skalický, 2018, s. 68 – 74)

2.7.2 Nákup kryptoměn

V případě, že má již uživatel peněženku, bude ji chtít pravděpodobně naplnit určitým obnosem kryptoměny, který získá výměnou za tradiční měnu.

První otázkou, nad kterou je dobré se zamyslet je, zda je taková činnost legální. V České republice, dle vyjádření České národní

banky a Ministerstva financí, se jedná o legální činnost a nikdo nebyl zatím stíhán, nicméně nemusí to tak být navždy a legislativa může být v budoucnu upravena. Další otázkou, kterou by si mohl položit nejeden člověk, který se začíná zajímat o kryptoměny v dnešní době je, proč by si je měl nakupovat, když se dají těžit? Ano dají, ovšem dnes je již těžba pomocí standardní výpočetní techniky nemožná. Disponuje-li ovšem daný zájemce o těžbu dostatečným kapitálem a ideálně i přístupem k levné elektřině, začít těžit je možné i dnes (viz kapitola 2.3 Těžba).

Bitcoinmaty

Nejsnadnějším způsobem, jak nakoupit první „mince", jsou bitcoinové bankomaty, tzv. Bitcoinmaty. V nich lze snadno směnit tradiční peníze za kryptoměny. Stačí mít vytištěný QR kód peněženky či nainstalovanou mobilní aplikaci. Bankomat po přiložení QR kódu (ať již vytištěného či z mobilního zařízení) pomocí čtečky rozezná, kam má kryptoměnu zaslat. Do Bitcoinmatu pak už jen stačí vložit bankovky a ten je dle kurzu a s marží přepočítá na vybranou kryptoměnu. Pro malé částky však nemusí být bankomaty v době vysokých poplatků ideální volbou. Bitcoinmaty slouží stejně jako klasické bankomaty obousměrně, stačí tedy zadat sumu, vyfotit QR kód a Bitcoinmat vydá majiteli účtu papírové peníze.

Prodejci kryptoměn

Dalším způsobem, jak získat první Bitcoin (či spíše jeho část) nebo jinou kryptoměnu, jsou prodejci. Prodejce lze nalézt například na serveru localbitcoins.com, kde dle zadaného města vyskočí veškeré nabídky seřazené podle ceny. U jednotlivých prodejců je samozřejmě možné si přečíst reference z již proběhlých transakcí a také zkontrolovat účty, jimiž daný prodejce disponuje. Pokud je prodejce důvěryhodný a kupujícímu vyhovuje cena, mohou si snadno přes server domluvit podmínky zaslání platby a zaslání kryptoměn do peněženky kupujícího.

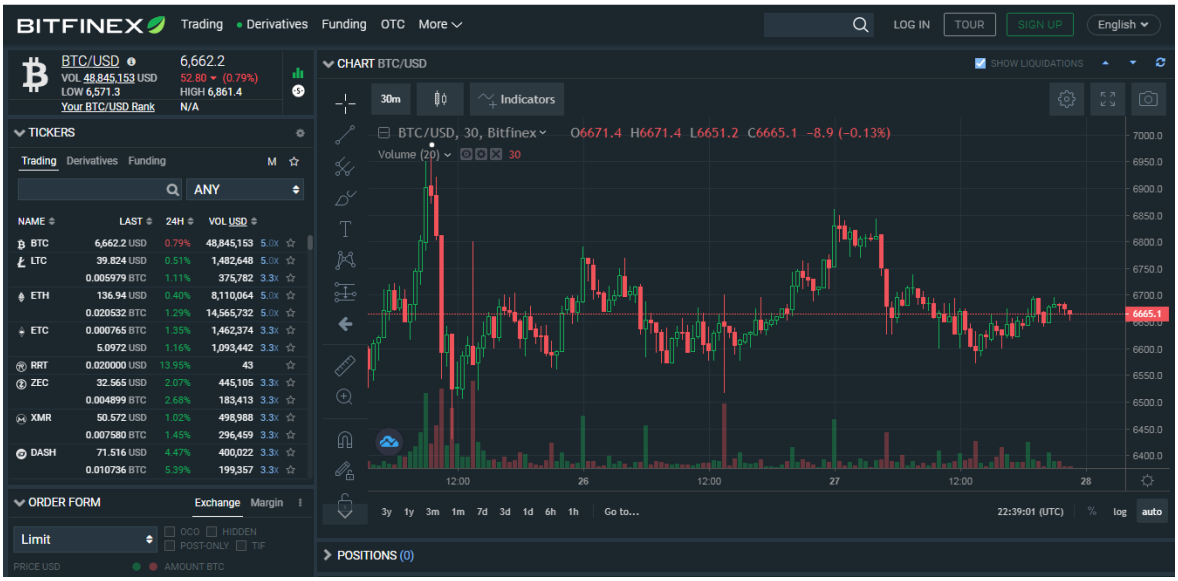
Směnárny a burzy

Specializované směnárny jsou na českém trhu dobrým a rychlým způsobem, jak získat kryptoměny. Jednou z takových směnáren je například simplecoin.cz, kde stačí jednoduše zadat adresu peněženky, email a množství Bitcoinů či jiné kryptoměny. Pokud kupující má účet u některé z bank preferovaných směnárnou, kryptoměna bude

připsána do peněženky prakticky ihned po zadání bankovního převodu. Jak již bylo řečeno, směnárna je velmi rychlý způsob k získání/prodeji kryptoměny a také je její výhodou, že celou transakci lze provést bez jakékoli registrace, nevýhodou ovšem je vyšší kurz pro kupující a naopak nižší pro prodávající. Je to logické, neboť právě na tomto rozdílu směnárna vydělává.

Další, již více odbornou možností, je obchodování na specializované burze. Jedná se o nástroj především pro nákup pravidelných objemů za vyšší sumy. Mezi největší bitcoinové burzy patří v současné době bitstamp.net, kraken.com, bitfinex.com, poloniex.com a další. V případě zájmu o investování vysokých částek je zodpovědné poradit se s odborníky, jelikož burz existuje velké množství a ne všechny jsou bezpečné. Burzy nabízí ve srovnání s bankomaty na Local Bitcoins některé možnosti navíc, není to však zadarmo. Při zakládání účtu na burze je vyžadováno zaslat provozovatelům osobní údaje, konkrétně doklad o bydlišti a osobní identifikaci v podobě naskenovaného průkazu totožnosti, řidičského průkazu či cestovního pasu. Pro českého uživatele je další nevýhodou, že chce-li na burzu zaslat peníze, musí tak učinit v eurech či dolarech, jelikož burza, kde se obchoduje v korunách, v současnosti neexistuje.[5] Další postup je již jednoduchý. Má-li zájemce o nákup či prodej na burze dolary, eura či jinou obchodovatelnou měnu, stačí v záložce „trade" (případně „buy/sell") kliknout na daný příkaz pro nákup či prodej, omezit příkaz maximální/minimální cenou (případně obchodovat s okamžitou tržní cenou burzy). Opět je důležité zopakovat, že třetím stranám nelze nikdy věřit a v případě pádu burzy (jako se to stalo s burzou Mt.Gox) mohou všichni uživatelé o své kryptoměny přijít. (Stroukal, Skalický, 2018, s. 75 – 80)

[5] V lednu 2019 skončila česká kryptoměnová burza NakamotoX.



Obrázek 3: Demonstrace bitcoinové burzy

Zdroj: Bitfinex (online)

2.7.3 Jak kryptoměny ochránit

Ochrana kryptoměn funguje obdobně jako ochrana tradičních peněz. Pokročilí uživatelé doporučují kombinovat různé druhy úschovy a ochrany. V peněžence na mobilním zařízení by měla být uschována pouze menší část peněz a větší část peněz by měla být uschována ideálně na více než jednom zařízení pod fyzickým zámkem. Jak již bylo zmiňováno, důvěra ve třetí strany se nemusí vždy vyplácet a fyzické zamykání kryptoměn zase není velmi uživatelky přívětivé. Mnoho vývojářů se proto snaží přijít s možnostmi, jak zajistit uživatelům co nejlepší ochranu jejich kryptoměn.

TREZOR

Zásadní posun v této problematice přinesl český startup Satoshi-Labs s jejich hardwarovou peněženkou TREZOR One. Jedná se o USB zařízení, velikostí podobné klíči od auta, v němž nalezneme jedno-účelový počítač. SatoshiLabs nabízí několik modelů, včetně těch s barevným dotykovým displejem.

Obrázek 4: Hardwarová peněženka TREZOR One

Zdroj: Pihl (online)

TREZORy fungují na dvou principech, prvním je izolace klíčů a druhým je nutnost fyzické přítomnosti uživatele. Pokud chce uživatel přijmout či odeslat transakci, musí tak vždy být potvrzeno přímo na samotném zařízení. To znamená, že soukromé klíče jsou vždy uložené v TREZORu a nikdy nejsou odeslány do mobilního zařízení či počítače. Připojený přístroj tedy komunikuje s peněženkou, ve které jsou stále zadávány veškeré údaje o transakci a v TREZORu zabezpečeném dalším PINem dochází pouze k potvrzení transakce. V případě obavy z krádeže či ztráty TREZORu je možné si vytvořit takzvaný recovery seed, tedy náhodně vygenerovaná anglická slova, pomocí nichž je možné zpětné obnovení peněženky. TREZOR je tedy ideální volbou při držení větších částek.

Papírové peněženky

Další možností jak může uživatel chránit své kryptoměny jsou tzv. papírové peněženky. Jejich nespornou výhodou je zejména odproštění od jakýchkoli hackerských útoků, nemohou zkolabovat a není třeba se spoléhat na zabezpečení třetí strany. Mají ovšem i slabé stránky obdobné jako papírové peníze. Mohou být tedy snadno fyzicky odcizeny, zničeny nebo ztraceny.

V případě zájmu o papírovou peněženku je třeba nejprve najít jejího poskytovatele, jímž je například web bitaddress.org. Po vygenerování adresy a volby možnosti „paper wallet" je možné si peněženku v podobě bankovky fyzicky vytisknout.

Obrázek 5: Papírová peněženka

Zdroj: Besticoforyou (online)

Na papírové peněžence nalezneme soukromý a veřejný klíč, které přísluší každé bitcoinové adrese. V levé části „bankovky" (Obrázek 5) se nachází adresa, na kterou lze zaslat libovolné množství peněz. Je také možné adresu nahrát do aplikace, kde je možné sledovat a přijímat transakce, ovšem jelikož tam není uložen klíč soukromý, kryptoměny není možné utrácet. Ten se nachází pod QR kódem v pravé části „bankovky". Papírovou peněženku je důležité mít dobře uschovanou, právě z důvodu, že se na ní nachází i soukromý klíč. (Stroukal, Skalický, 2018, s. 88 – 93)

3 Virtuální měny a sport

Virtuální měny mají využití v mnoha různých odvětvích a nejedná se pouze o nástroj investorů či spekulantů. Z důvodu rozšíření povědomí čtenáře o další sektor, kde k využití kryptoměn dochází, je zařazena na závěr teoretické části diplomové práce tato kapitola.

3.1 Jak blockchain a jeho aplikace může pomoci růstu sportovního průmyslu

Transformace spotřebitelských návyků a všudypřítomnost digitálních technologií umožnily vznik řadě inovací. Tyto inovace jsou zdrojem růstu také pro sportovní průmysl. Blockchain se dostal do povědomí populace především díky Bitcoinu, ovšem tato základní technologie umožňuje využití v mnoha dalších oblastech.

Ve sportovním průmyslu může být blockchain použit k:

- usnadnění hromadné koordinace mezi zúčastněnými stranami prostřednictvím decentralizace;
- snížení nákladů odstraněním třetích stran;
- budování důvěry mezi zúčastněnými stranami;
- zabezpečení dat a učinění je transparentními. (A PwC France initiative, 2019, online)

3.1.1 Jak může blockchain a jeho aplikace pomoci udržovat vztahy mezi kluby a jejich členy

Sportovní asociace neustále hledají nové způsoby komunikace a navyšování peněz v odvětví, které se stalo vysoce konkurenceschopné. Sportovní kluby se snaží přicházet na nové způsoby jak navýšit členskou základnu a především budovat loajalitu. Inovace a konkrétněji blockchain, mohou naplnit očekávání klubů, federace, fanoušků a zároveň členů.

Co blockchain klubům nabízí je virtuální měna s ním spojená a použitelná prostřednictvím decentralizované aplikace.

Řešení této povahy by kupujícím, tedy fanouškům, dobrovolníkům, sponzorům a partnerům, umožnilo:

- hlasování o strategických a finančních rozhodnutí klubu;

- pronájem prostor a organizování akcí v klubu;
- získání speciálních cen za tréninky a výjezdy, dále pak za reklamní předměty klubu a ostatní doplňkové služby (jako například sportovní fyzioterapii);
- propagaci mimo klubových aktivit a služeb.

Využívání kryptoměny by klubům umožnilo například:

- odměňovat práci dobrovolníků;
- financovat některé projekty propagované členy klubu;
- pomoci získat peníze na individuální projekty členů klubu usnadněním iniciativy crowdfundingu[6]. (A PwC France initiative, 2019, online)

3.1.2 Využívání kryptoměn sportovními týmy

Přesunu mnoha odvětví do online prostoru se snaží přizpůsobit i sportovní týmy a organizace, které začínají využívat kryptoměny, aby umožnily jejich fanouškům přístup k exluzivnímu obsahu díky kryptoměnám. Tento posun k akceptaci kryptoměn se stále vyvíjí, ale v některých klubech se tak již děje poměrně dlouhou dobu. Například jeden z týmů NBA Sacramento Kings přijímá Bitcoiny již od roku 2014, jako způsob platby za vstupenky a zboží. Jednalo se pravděpodobně o průkopníka v této oblasti a od té doby se řada sportovních týmů a organizací začala zabývat využitím kryptoměn jako moderním nástrojem, který může usnadnit jejich fanouškům a zákazníkům elektronické obchodování.

Fotbal skóruje s kryptoměnami

Fotbal je jedním z nejpopulárnějších sportů na světě a slavné kluby mají obrovské fanouškovské základny po celém světě. Řada největších evropských týmů přijala řešení založená právě na blockchainu.

Slavné kluby jako například Juventus nebo Paris Saint Germaine se zapojily do fanouškovské platformy Socios, která je založená na blockchainu. Platforma umožňuje zapojeným týmům spustit své vlast-

[6] Crowdfunding neboli skupinové financování je způsob financování, kdy pro získání cílové částky na realizaci předmětu financování, přispívá menším obnosem větší počet jednotlivců. (Wikipedia, online)

ní fanouškovské tokeny[7], které mohou pak fanoušci na platformě použít. Fanoušci pak mohou pomocí svých tokenů hlasovat o věcech, jako jsou například změny dresu klubu a zároveň mít přístup k exluzivnímu obsahu. Na platformě Socios existují dva typy volebních mechanismů – závazný a nezávazný. Závazné hlasování znamená, že klub musí přijmout jakýkoli výsledek hlasování. Pokud tedy fanoušci hlasují pro změnu barvy dresu, klub bude muset splnit svůj slib. Vzhledem k tomu, že hlasy jsou prováděny na platformě blockchain, nelze s nimi manipulovat ani je vymazat. Jedná se o zajímavé využití blockchainu a skutečnost, že se takto slavné kluby rozhodly zapojit, je pro toto odvětví velkou podporou.

Dalším příkladem z fotbalového prostředí je portugalský klub Benfica, který začal v červnu 2019 přijímat kryptoměnové platby za zboží a lístky prostřednictvím platformy Utrust. Tento krok byl způsoben především splněním požadavků více než sedmi milionů fanoušků na sociálních sítích.

Zajímavostí je, že kryptoměny a projekty založené na blockchainu mají podporu mimo jiné od barcelonské hvězdy Lionela Messiho. (Jenkinson, 2019, online)

3.1.3 „Krypto - reklamy" ve sportu

Sport a sázky mají dlouhou společnou historii a kryptoměny mají zase vlastnosti, které hazardní hry a sázení usnadňují. Sázkové společnosti zaznamenávají úspěch a stávají se hlavními sponzory mnoha sportovních klubů. V tomto ohledu se v posledních letech dostávají do popředí také sázkové společnosti založené na kryproměnách.

Sázkové společnosti vytvářejí dokonce své vlastní kryptoměny, jako tomu bylo například u kalifornské společnosti CashBet, která přišla na trh s jejich kryptoměnou CashBet Coin. Spolupráci s touto společností uzavřel Arsenal a inzerci této kryptoměny mohlo být vidět na Premier League v roce 2019.

[7] Kryptoměnový token je digitální aktivum, které je možné použít v rámci nějakého projektu. Tokeny na rozdíl od kryptoměn potřebují cizí blockchain, přes který mohou fungovat. Jedním druhem je utility token, který je vytvořen pro využití v rámci decentralizované aplikace. Obecně ovšem mohou být tokeny také využívány pro platby. (Tradearena, online)

Další klub Premier League, Wolverhampton Wanderers, má zase uzavřenou reklamní dohodu se směnárnou kryptoměn CoinDeal. Jejich logo se objevilo na dresu týmu během sezóny 2018 – 2019 a spolupráce bude nadále pokračovat.

V roce 2018 byl také zaznamenán rozruch kolem reklamní spolupráce společnosti eToro, uzavřené se sedmi kluby Premier League, která byla plně placena Bitcoiny. Součástí kampaně bylo také spuštění programu eToro FC, který poskytoval členům komunity vzdělávací materiály, návody a zprávy o trhu.

V roce 2019 byly zaznamenány „krypto – reklamy" také v NBA, když se například na dresech Cleveland Cavaliers objevilo logo kryptoměnové burzy UnitedCoin. (Jenkinson, 2019, online)

3.1.4 Průnik kryptoměn do sportu

Vliv a dosah, který má sport po celém světě, mu nelze upřít. Nejoblíbenější sporty mají stovky milionů sledujících po celém světě a průnik kryptoměn a technologie blockchainu do tohoto odvětví je impozantní (i vzhledem k tomu, že existují pouze něco málo přes deset let) a může být velice zásadním. Partnerství s největšími týmy evropského fotbalu stejně jako proniknutí do amerického publika skrze basketbal a americký fotbal nelze podceňovat a je pravděpodobné, že samotná reklama v tomto odvětví přivede do světa kryptoměn a blockchainu řadu nových uživatelů. (Jenkinson, 2019, online)

PRAKTICKÁ ČÁST

4 METODIKA A DATA

Druhá část diplomové práce se zabývá využitím kryptoměn v praxi, se zaměřením na kavárny v Praze, z pohledu běžného uživatele. V první části budou popsány poznatky z vlastního pozorování, od pořízení peněženky, přes nákup kryptoměny a platbu.

Pro získání více informací a obohacení diplomové práce bylo provedeno také kvalitativní šetření ve formě dotazníku mezi osobami, které se kryptoměnami aktivně zabývají.

V závěru praktické části se nachází návrhy a doporučení, které jsou zaměřeny především na čtenáře, kteří nemají s předchozím využitím kryptoměn žádnou nebo minimální osobní zkušenost a chtěli by se začít zajímat o možnosti využití kryptoměn ve formě alternativního platidla.

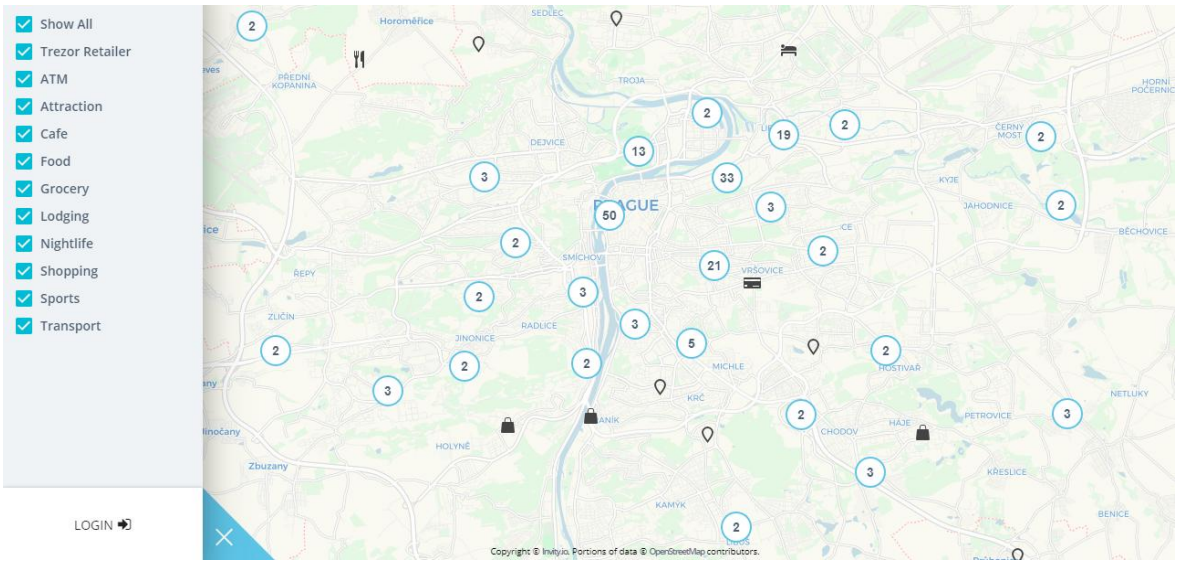
5 VLASTNÍ POZOROVÁNÍ

Obsahem této kapitoly je provedení čtenáře úkony, které je třeba provést, chce-li začít využívat kryptoměny k platbám v kavárnách (případně jiných podnicích a kamenných obchodech).

5.1 Kde je možné kryptoměnou zaplatit

Pro jednoduchý a rychlý přehled míst, kde lze kryptoměny využít k platbě, kde se nachází bankomaty pro výměnu kryptoměn a kde lze zakoupit hardwarovou peněženku Trezor, existuje portál coinmap.org. Na tomto portálu lze zobrazit tato místa kdekoliv na světě a je možné si tak udělat i dobrý přehled, v jaké četnosti jsou kryptoměny využívány v jednotlivých zemích. Na zobrazené mapě lze pomocí filtru provést výběr konkrétních odvětví, což je velice uživatelsky přívětivé.

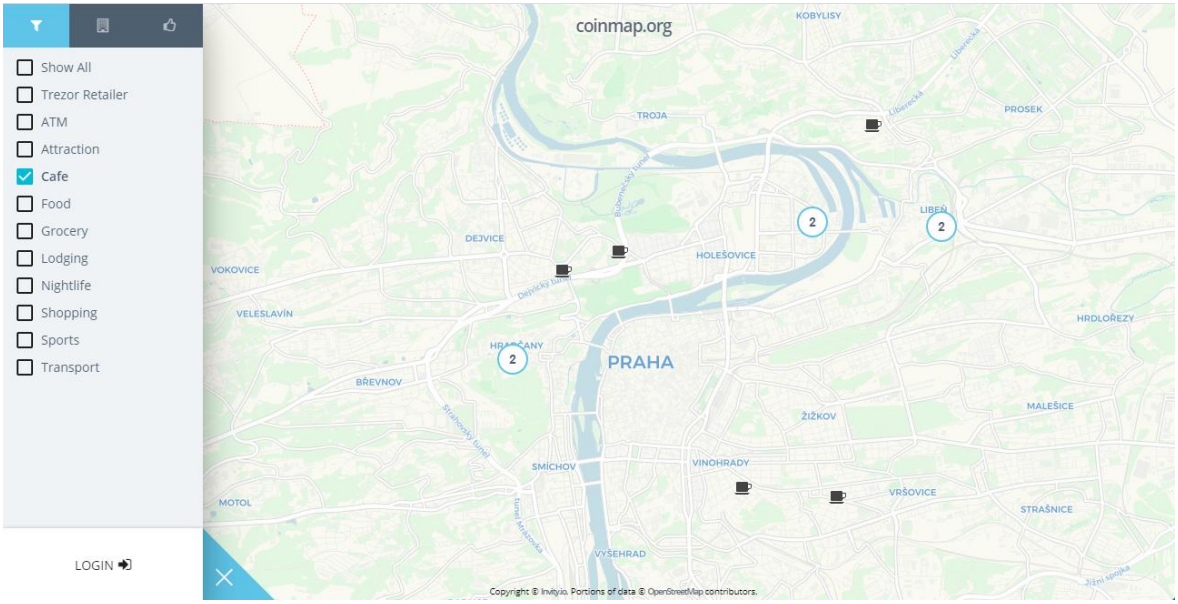
Jak můžeme vidět z Obrázku 6, v Praze a jejím nejbližším okolí se nachází v současnosti téměř 200 míst, kde je možné provést platbu kryptoměnou, případně si kryptoměnu nakoupit či zakoupit hardwarovou peněženku Trezor.



Obrázek 6: Přehled míst pro možnost využití kryptoměny v Praze

Zdroj: Coinmap (online)

Na Obrázku 7 je možné vidět kavárny v Praze, kde lze platit kryptoměnou. Dle portálu coinmap.org se jedná celkem o jedenáct kaváren, kde lze uplatnit kryptoměny.



Obrázek 7: Přehled kaváren s možností platby kryptoměnou v Praze

Zdroj: Coinmap (online)

5.1.1 Paralelní Polis

Paralelní Polis je nezisková organizace sídlící od roku 2014 v pražských Holešovicích. Jedná se o jedno z hlavních kryptoměnových center v České republice, kde se fanoušci a majitelé kryptoměn schází. V prostorech Paralelní Polis jsou pravidelně pořádány přednášky a workshopy (nejen) o kryptoměnách z cyklu Bitcoin Meetup.
Nachází se zde také dva z pražských Bitcoinmatů. Jeden z nich je chytře umístěn přímo v prostoru kavárny Bitcoin Coffee. Bitcoin Coffee je jedinou kavárnou v České republice, kde lze zaplatit pouze kryptoměnou. V kavárně jsou přijímány kryptoměny Bitcoin, Litecoin, Dash a Monero.

5.1.2 Ostatní kavárny přijímací kryptoměny

Jak již bylo zmíněno výše, v Praze v současné době funguje jedenáct kaváren, kde lze uplatnit kryptoměny (viz Obrázek 7). Všechny

zařízení kromě Paralelní Polis přijímají kryptoměny pouze jako alternativu k tradiční měně.

Na portálu coinmap.org lze u jednotlivých podniků vidět také datum, odkdy kryptoměny přijímají. Z tohoto hlediska je určitě důležité zmínit podnik Alchymista sídlící na Letné, kde jsou přijímány kryptoměny již od 10. 1. 2014.

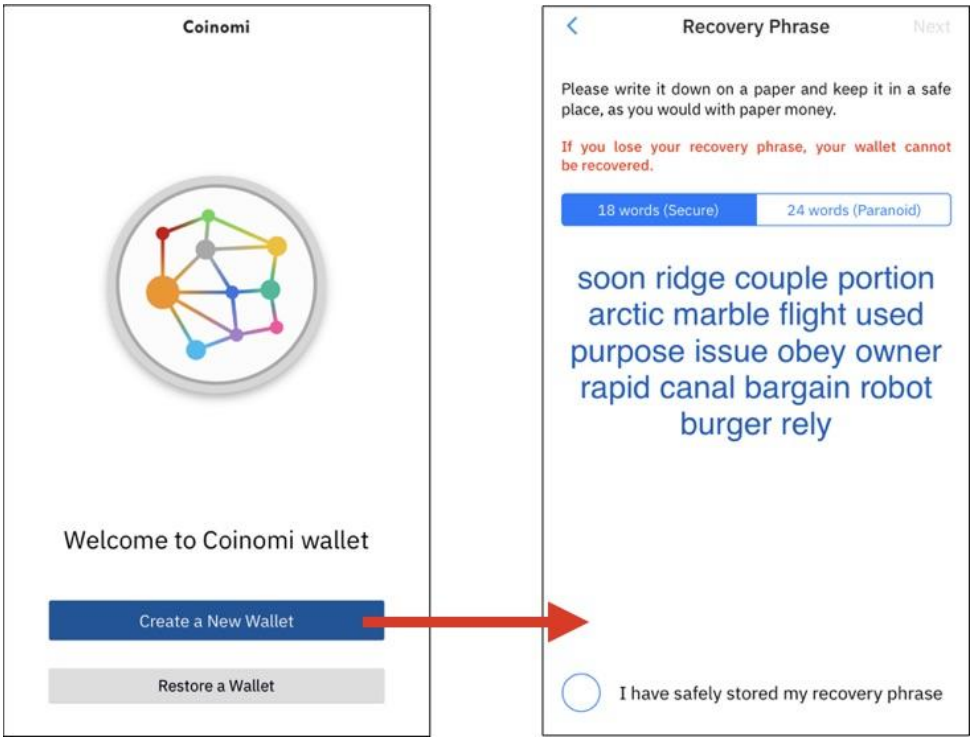
Z dat uvedených na portálu coinmap.org je vidět, že kavárny se k přijímání kryptoměn přidávají postupně. Je tedy možné předpokládat, že s narůstající popularitou právě kavárenského odvětví a zároveň s rostoucím zájmem o kryptoměny bude počet podniků přijímajících tento alternativní způsob platby do budoucna narůstat.

5.2 Pořízení mobilní peněženky

V dnešní době, kdy u sebe většina lidí neustále nosí chytrý telefon, je uživatelsky nejpřívětivější formou uložení kryptoměn mobilní peněženka.

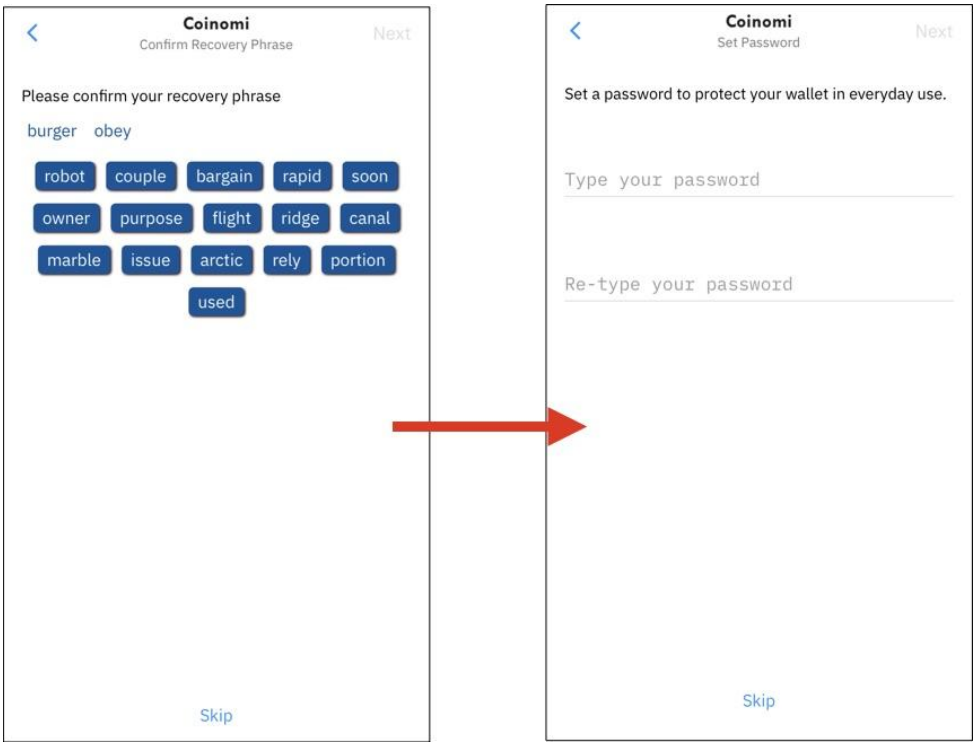
V rámci této diplomové práce bude představena mobilní aplikace Coinomi, která je uživatelsky velmi oblíbenou, jak mezi uživateli Androidu, tak uživateli iOS. Většina mobilních peněženek ovšem funguje na velmi podobném principu a všechny jsou, co se týká složitosti ovládání, uživatelsky přívětivé.

Založení mobilní peněženky je velmi jednoduché a rychlé.
Po nainstalování aplikace do mobilního zařízení je uživatel vyzván k opsání takzvané bezpečnostní fráze. Bezpečnostní fráze je 18 (případně 24) anglických, náhodně řazených slov, které nedávají dohromady žádný význam (viz Obrázek 8). Aplikace doporučuje uživateli opsat bezpečnostní frázi na papír a tento papír poté dobře uschovat na bezpečném místě. Je doporučeno tuto frázi s nikým nesdílet a nikdy ji nezadávat na jakékoli webové stránce nebo službě. Po odsouhlasení bezpečného uložení bezpečnostní fráze vyžaduje aplikace frázi zopakovat (viz Obrázek 9). Při zakládání mobilní peněženky samozřejmě nejsou vyžadovány žádné osobní údaje. Jediné, co peněženka vyžaduje je vytvoření minimálně desetimístného hesla, které slouží k šifrování peněženky (viz Obrázek 9). Poté, co je heslo vytvořeno a potvrzeno opakovaným zadáním, je peněženka připravena k použití.



Obrázek 8: Coinomi – mobilní peněženka

Zdroj: Infocryptoland (online)



Obrázek 9: Coinomi – mobilní peněženka

Zdroj: Infocryptoland (online)

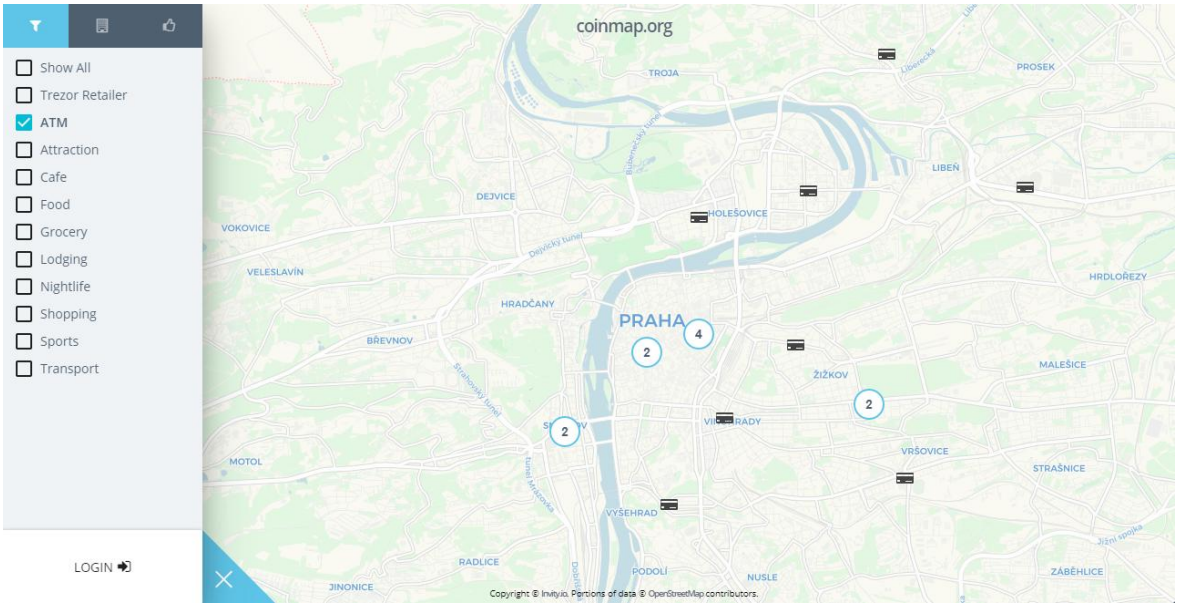
Jak je možné vidět z Obrázku 9, kroky ověřování bezpečnostní fráze a zadání osobního hesla k zašifrování peněženky je možné přeskočit, nicméně je vysoce doporučeno těmito kroky projít.

Aplikace je dostupná také v českém jazyce, ovšem prostředí není přeloženo kompletně a některé názvy či úkony jsou uvedeny stále v jazyce anglickém.

5.3 Nákup kryptoměn

Veškeré nově vytvořené peněženky mají nulový zůstatek a je tedy na ně potřeba kryptoměnu dobít.

Jednou z nejjednodušších cest, jak kryptoměnu nahrát do své peněženky je pomocí bankomatu, tzv. Bitcoinmatu. Na Obrázku 10 můžeme vidět Bitcoinmatovou síť Prahy. Bankomaty fungují obousměrně, což znamená, že v nich lze kryptoměnu nakoupit i prodat. Zároveň je možné z něho i vybrat hotovost. Při nákupu v bankomatu není ani nezbytně nutné mít naistalovanou mobilní peněženku, jelikož automat umí vytisknout papírovou peněženku ve formě účtenky s QR kódem, pod kterým se skrývá adresa s nakoupenou kryptoměnou.



Obrázek 10: Rozmístění Bitcoinmatů v Praze

Zdroj: Coinmap (online)

Nahrát peníze do peněženky pomocí bankomatu lze snadno v několika krocích:

1) Volba jazyka - v bankomatech v Praze je možné volit mezi češtinou a angličtinou
2) Volba měny – v ČR lze rozměňovat české koruny a eura
3) Volba kryptoměny, kterou chce uživatel zakoupit
4) Načtení QR kódu s adresou z mobilní aplikace případně papírové peněženky[8]
5) Vložení papírové hotovosti (bankomaty nerozměňují, tzn., že v případě vložení například 500 Kč si bankomat vezme celou částku a nelze nahrát například pouze 300 Kč)
6) Potvrzení nákupu

Peněženku lze také naplnit jednoduše z papírové peněženky, naskenováním QR kódu, případně přijetím transakce od jiného vlastníka kryptoměn.

Další možností je zakoupení kryptoměny kreditní či debetní kartou skrze poskytovatele Simplex, do jehož platební brány je uživatel přesměrován přímo z mobilní aplikace.

Při nákupu kryptoměn je důležité myslet na poplatky s tím spojené, tudíž například výměna pouze malého obnosu v Bitcoinmatu se může poměrně prodražit. Dalším důležitým faktorem, na který je třeba při nákupu myslet, je časová prodleva, se kterou je kryptoměna do peněženky nahrána – u Bitcoinu se může jednat až o desítky minut, dle výše priority transakce.

Více pokročilé možnosti nákupu kryptoměn jsou popsány v kapitole 2.7.2 Nákup kryptoměn, ovšem ty nebyly v rámci praktické části této diplomové práce testovány.

5.4 Platba kryptoměnou

Platba kryptoměnou je poměrně snadnou a rychlou záležitostí.

Před provedením platby je potřeba obsluze říci, ve které kryptoměně bude platba uskutečněna.

[8] Tento bod je možné vynechat (v případě, že nemá zájemce o kryptoměnu vlastní mobilní či papírovou peněženku) a zvolit možnost vytisknutí účtenky s QR kódem

V případě použití mobilní aplikace otevře zákazník v jejím rozhraní čtečku QR kódu a načte QR kód, s adresou příjemce platby, poskytnutý obsluhou. Poté si zákazník zkontroluje uvedenou částku, zadá své osobní heslo (heslo vytvořené při zakládání peněženky, které slouží k jejímu šifrování) a platbu potvrdí.

V případě použití papírové peněženky proběhne platba obdobným způsobem, s tím rozdílem, že obsluha si naskenuje QR kód peněženky svým zařízením a zákazník na něm následně platbu potvrdí.

6 VÝSLEDKY KVALITATIVNÍHO ŠETŘENÍ

V rámci kvalitativního šetření bylo dotazováno 15 osob, které se aktivně zabývají kryptoměnami. Cílem tohoto dotazníkového šetření bylo zjištění motivace těchto osob, které se kryptoměnami zabývají především ve svém volném čase, k užívání kryptoměn.

Otázky položené v dotazníku lze nalézt na konci diplomové práce v Příloze 1. Většina položených otázek byla otevřeného charakteru pro ponechání respondentům většího prostoru vyjádření se k danému tématu vlastními slovy.

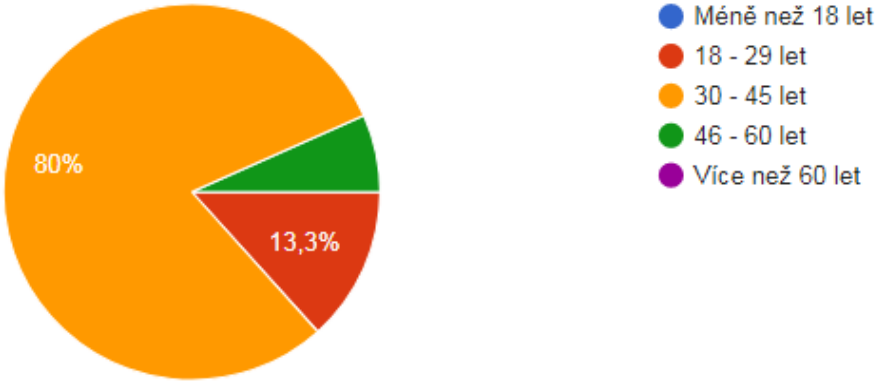
První tři otázky se týkají pohlaví, věku a nejvyššího dosaženého vzdělání, což poskytne možnost utvoření si základní představy o složení respondentů, a zároveň to tak může poskytnout základní informaci o profilu uživatele kryptoměn.

Pohlaví respondentů

Respondenti tohoto dotazníkového šetření byli pouze muži. Z tohoto výsledku nelze udělat závěr, že ženy se kryptoměnami nezabývají, jelikož počet respondentů je příliš nízký. Ovšem lze předpokládat, že se touto problematikou zabývají především muži, jelikož se jedná o obor technického charakteru. Podíváme-li se na složení studentů na školách s technickým zaměřením, stále značně převažují muži.

Věk respondentů

Jak je možné vidět z Grafu 1, 80% respondentů (12 osob) se nachází ve věkové kategorii 30 – 45 let, 2 respondenti spadají do věkové kategorie 18 – 29 let a jeden respondent spadá do věkové kategorie 46 – 60 let. Z těchto výsledků je možné odvodit, že kryptoměnami se zabývají především osoby mladší až střední generace, které jsou samostatně výdělečně činné.

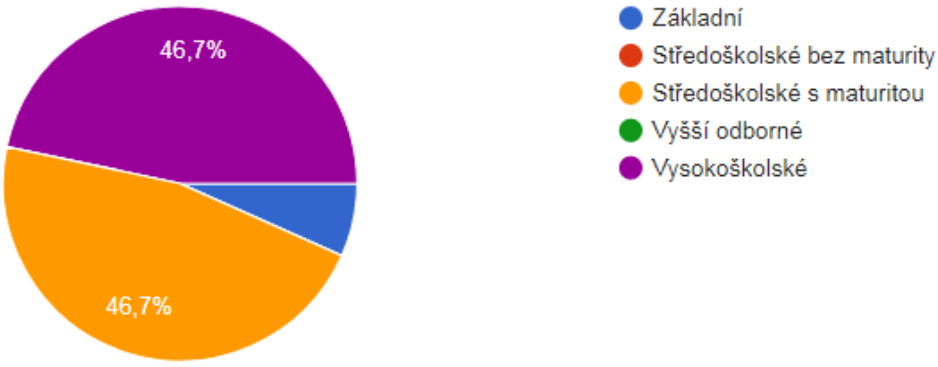


Graf 1: Otázka č. 3 – Věk respondentů

Zdroj: Vlastní zpracování

Nejvyšší dosažené vzdělání respondentů

Z Grafu 2 je možné vidět, že s výjimkou jednoho respondenta se základním vzděláním, má polovina respondentů středoškolské vzdělání s maturitou a druhá polovina vzdělání vysokoškolské. Vzhledem k tomu, že v ČR žije přibližně 20% obyvatel s vysokoškolským titulem (Český statistický úřad, online), lze předpokládat, že problematikou kryptoměn se zabývají především osoby s nadprůměrným vzděláním.



Graf 2: Otázka č. 4 – Nejvyšší dosažené vzdělání respondentů

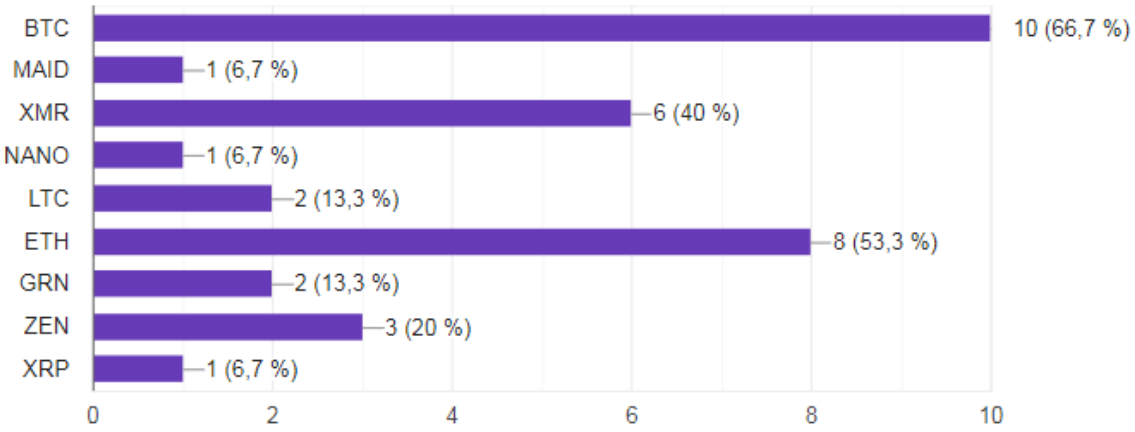
Zdroj: Vlastní zpracování

Doba užívání kryptoměn

Všichni respondenti se zabývají problematikou kryptoměn minimálně dva roky. Třetina respondentů se věnuje kryptoměnám tři roky a 6 z 15 respondentů se tímto tématem zabývá 5 let a více. Je otázkou, zda kryptoměny jsou stále atraktivní i pro nově příchozí na trh. Lze předpokládat, že se stále narůstajícím počtem nově vzniklých kryptoměn, se na trhu objeví také noví uživatelé, kteří se kryptoměnami dříve nezabývali.

Druhy používaných kryptoměn

V Grafu 3 je možné vidět, které kryptoměny používají respondenti dotazníkového šetření. Zajímavostí je, že třetina dotazovaných vůbec nepoužívá nejznámější a nejrozšířenější kryptoměnu Bitcoin. Druhou a třetí nejrozšířenější kryptoměnou mezi respondenty jsou Ethereum a Monero. Mezi méně známé kryptoměny, které se objevily v odpovědích, patří například MaidSafeCoin nebo GreenPower.
Jeden z respondentů také uvedl, že se zajímá pouze o Bitcoin, jelikož ostatní druhy kryptoměn jsou pouze kopiemi a nepřináší žádné inovace.



Graf 3: Otázka č. 6 – Druhy používaných kryptoměn

Zdroj: Vlastní zpracování

Zájem o fungování kryptoměn

Před analýzou odpovědí je vhodné zde uvést celé znění otázky: „Zajímáte se o fungování kryptoměn více? Pokud ano, co Vás k tomu vede? Nebo jste pouze uživatelem (kryptoměny využíváte pouze k nákupu/prodeji zboží)?“

Všichni respondenti se zajímají o fungování kryptoměň více a nejedná se pro ně pouze o nástroj k nákupu/prodeji zboží. Většinu respondentů zajímají kryptoměny z technického hlediska, dále pak vlastnost decentralizace (nemožnost ovládání měny centrální autoritou) a nové možnosti kryptoměn jako alternativního platidla.

Za citaci stojí odpověď pana Ing. Aleše Maškovského, který se kryptoměnami aktivně zajímá jak z pracovního hlediska, ale především pak ve svém volném čase:

„Ekonomika je postavena na "chtění" a toto "chtění", způsobuje často jednání v zájmu vlastním, místo v zájmu cizím. Centrální správa měny by měla být prováděna v režimu zájmu o cizí hodnotu - protože je navázána na práci ostatních. Je přesto často provozována v režimu "vlastní, nebo politický zájem". Centrální správa fiat měny tedy má "moc", se kterou podle toho nakládá. Kryptoměny toto řeší tím, že jsou decentralizované, tedy odebírají "moc" konkrétní autoritě. Jsou devalvovány dle programu, nikoliv podle "úsudku" centrálních bank a bank, které pomocí úvěrů, zvětšují množství oběživa, (kryptoměny tedy také vyřazují lidský faktor, dobré nebo špatné chování vůči správě cizího majetku prostřednictvím měny). Tj. kryptoměny mají "vzácnost - hodnoty i povahy". Tato vzácnost hodnoty je dána množstvím kryptoměny v oběhu, i když jsou paradoxně navázány na fiat měny. Protože člověk potřebuje pro pochopení "hodnoty" srovnání - bez toho nelze pochopit, zda je něčeho málo, či hodně, zda je něco hezké, či ošklivé, byly kryptoměny kurzem nešťastně svázány právě s fiat měnou, kterou každý zná. Hodnota kryptoměny pak je dána "nabídkou a poptávkou", která nezohledňuje "vzácnost" kryptoměn. Pak se děje paradoxně například to, že hodnota ve fiat měně elektrické energie roste (ona je ve skutečnosti stejná, protože se těží uhlí a vyrábí elektřina stále stejným úsilím například, ale ředí se fiat měna, proto to vypadá, že cena energie roste, ale vlastně klesá hodnota měny) a současně může klesat hodnota kryptoměny, která je v ten moment například pod tlakem výprodejů. (Výsledek by měl být, že kryptoměna by měla hodnotu vůči ceně energie přibližně stejnou, zatímco by "vzácnost" fiat měny měla stále klesat.) Způsob, jakým média, vlády, korporáty a různá uskupení prezentují kryptoměny způsobuje, že je kryptoměna "devalvována" v očích uživatelů dle aktuální nálady, ne její skutečné povahy a hodnoty. Kryptoměna má další zásadní vlastnost, tou je jí likvidita a dostupnost tím tedy také neztrácí vzácnost. Je to určitá forma stability. (Je to jako mít stále svůj notebook, který potřebuji ke svojí práci a vím, že o něj nepřijdu. Banky umí

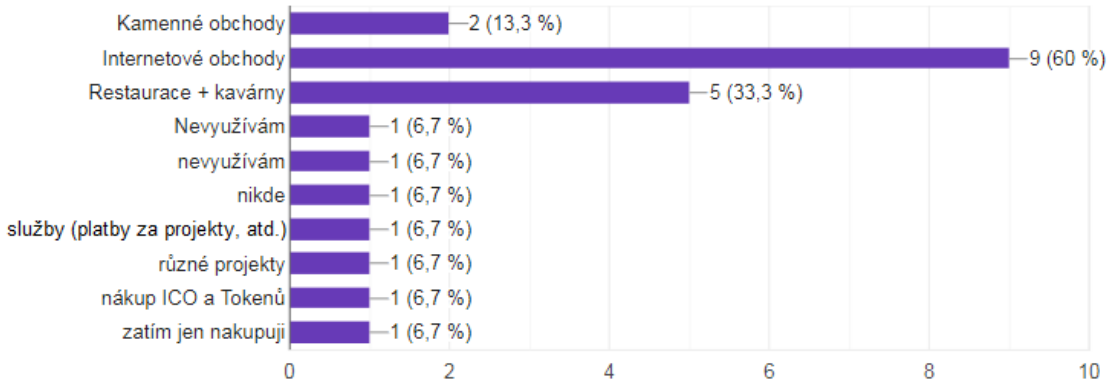
své bankomaty zcela uzavřít.) Zatímco fiat měna, jejím nekonečným ředěním, je stále více a více méně vzácná a nemusí být ani dostupná! Tím, že je méně vzácná a korporáty (Tesco například) si to uvědomují, zvedají ceny zboží (nebo devalvují hodnotu - nekvalitní výrobky např.). To způsobí, že běžní lidé musí mít buď vyšší plat, nebo musí přibrat další práci. Protože dynamika zvyšování mezd je menší, než dynamika zvyšování cen (a komplexně to nikdo moc neřeší - na úrovni tvůrců měny, zda zaměstnanec zaplatí nájem, energii, jídlo atd.), vzniká situace, že prodáváme svoji práci - kterou nemůžeme neustále zvyšovat, za "něco", co má stále menší hodnotu. Kryptoměna vznikla v tomto bodě, jako nesouhlas s výše uvedeným modelem, který je postaven na principu chtění a principu "špatné správy cizího majetku prostřednictvím měny". Ona je i otázka, zda cizí majetek (lidská práce, cena zboží a služeb vs. množství měny) při vší dobré vůli lze spravovat dobře. Moc ne. Jádrem celého problému je právě lidská chtivost, která je kořenem a jádrem celé ekonomiky a současně i problémem ekonomiky. Bez této chtivosti, by se vše zastavilo. Tato chtivost funguje jako vysavač peněz. Dám to na příkladu, kdy vysavač vysává peníze z oběhu - ten kdo má určité výhody (samočinné stroje, počítače co pracují s penězi, exkluzivní znalosti zavedené do programů, moc, eshopy, nebo aplikace - jako třeba systémy automatických reklam a další) umí vysávat z oběhu peníze rychleji, než jsou schopni zaměstnanci vytvořit v hodnotě svojí práce a vyměnit za peníze a následně si koupit. Začíná pak kolo dvě - nákup na dluh. Dnes v době koronaviru, se nabízí bezúročné půjčky a neřeší se otázka, jak se splatí. Jde jen o to, aby se kolotoč znovu točil. Jiný příklad je pískoviště kde písek představuje peníze a ten se dopravníkem dostává na tatru. Na tatře je málo lidí (bohatí) a ten dopravník se zrychluje. Lidé pracují stále usilovněji, aby písek naházeli na dopravník, lidí je stále více, ale pracují se stále menším množstvím písku. Za určitý čas, nebudou mít žádný písek, začnou si tedy půjčovat písek z tatry, aby jej mohli znovu házet, protože "za házení", si mohou trochu písku nechat pro svoji potřebu. Měna se tedy dostane do situace, kdy stéle větší množství lidí bude mít horší přístup k určitému množství měny, která bude mít stále menší hodnotu. Oproti nákupu klasické měny se tedy kryptoměna chová i jako investice - která hodnotu neztrácí. Byť její hodnocení v očích uživatelů a tím jak je nám vše prezentováno, to tak nevypadá. Aby společnost mohla fungovat, bylo by potřeba, aby se jednou za čas, vysypala tatra na pískoviště, aby lidé mohli znovu prodávat svoji práci házením písku na dopravník. Tomu, ale brání model "chtění", protože by byl potřeba přesně opačný model jednání. A tím je soucítění s těmi,

kteří ačkoliv pracovali, nemají "co" házet. A protože by tím byla poražena základní myšlenka "chtění" a modelu ekonomiky, dojde pravděpodobně k tomu, že se vše zastaví a nastane transformace. Až lidé pochopí, že fiat měna ztrácí svojí "vzácnost" a také "užitečnost" až nastane situace, že nebudou mít možnost házet písek, protože žádný nebude a navíc k němu budou mít horší přístup, k tomu co zbyde, pak se můžou obrátit na kryptoměny, které zatím mají "vzácnost", ale chybí jim "užitečnost" (díky neznalostem lidí jak s nimi pracovat, díky strachu, regulacím a dalším komplikacím, které dnes kryptoměny provází). Může tedy přijít doba, kdy určitá část lidí bude mít kryptoměny a určitá část lidí bude pracovat s fiat měnami, za které si nic nekoupí, nebo málo.
Za sebe, věřím kryptoměnám, jako alternativě k současnému ekonomickému systému a dost se o to zajímám. Používám je jako investice, kupuji kryptoměny. Tam kde s nimi lze platit, platím s nimi, většinou v oblasti služeb. Dále se připravuji na smart kontrakty (nad ETH), které vyřazují soudy a právníky a zjednodušují uzavírání smluv. To mne v poslední době zajímá velmi.
V budoucnu budou mít lidé tohle, nebo něco nového. To určí pravděpodobně ten, kdo převezme moc. Protože kryptoměny nemají "vůdce", který by je spravoval, tak kdyby stát ztratil moc nad energií (každý bude mít vlastní solární elektrárny) a ztratil moc nad měnou (přešlo by se kompletně na kryptoměny), vznikne situace, kdy možná nebude nikdo, kdo řeší silnice, nemocné, sociálně slabé, důchodce atd. Tj. kryptoměny v plném rozsahu můžou přijít až v době, kdy lidské soucítění bude na takové úrovni, že vzájemná pomoc bude samozřejmostí a policie a soudy nebudou potřeba (model Ubuntu například). Tj. až nebude hlavním proudem lidské chtění, ale vzájemná pomoc, péče o druhé s vazbou na "vědomé myšlení". Tj. vím, co způsobí důsledky mých činů. Pokud by kryptoměny zlomily fiat měnu dříve, bude to zřejmě průšvih.
Poslední moje úvaha je o důvěře. Pokud se ekonomika dostane do stagnace (recese) a lidé už nemají písek. Pak je koronavirus požehnáním pro vládce. Protože nejhorší, co se může vládám stát, je ztráta důvěry. Pokud koronavirus vláda potlačí a lidé uvěří v "systém, model", dají se ekonomické ztráty a důvod špatné situace svést na koronavirus a límečky zůstanou čisté. Dokonce z toho ještě vyjdou s medailí. Úmrtnost 3% není totiž nic zásadního a ve srovnání s morem ve středověku nebo jinými epidemiemi, je koronavirus vlastně normální chřipka s rychlejším nakažením.“

Pan inženýr Maškovský zajímavě shrnul základní vlastnosti kryptoměn, a také jeho osobní pohled na problematiku a motivaci, proč se kryptoměnami zabývá.

Místa využití kryptoměn k platbě

Jak je možné vidět z Grafu 4, 60% respondentů využívá kryptoměny k platně v internetových obchodech. Jedna třetina respondentů platí s kryptoměnami v restauracích a kavárnách a dva z patnácti respondentů využívají kryptoměny při platbách v kamenných obchodech. Celkově čtyři respondenti odpověděli, že kryptoměny k platbám nevyužívají. Z těchto výsledků je možné usoudit, že platby kryptoměnou na internetu jsou více rozšířené. Nižší využívání plateb v kamenných obchodech a kavárnách a restauracích může být dáno (jak také vyplyne z následujících otázek) malým množstvím obchodníků přijímacích kryproměny.

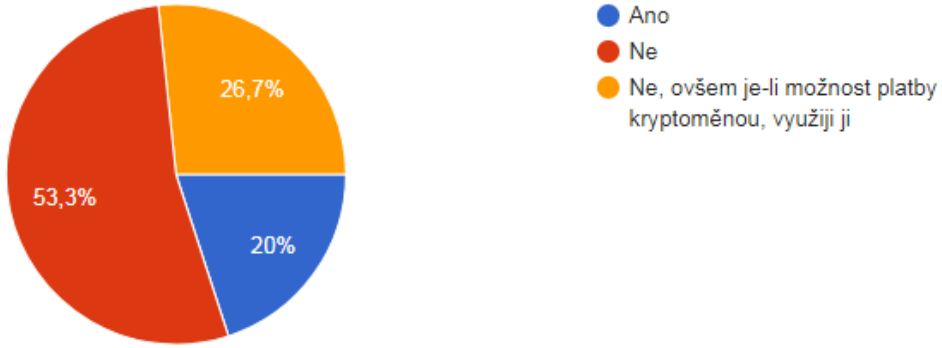


Graf 4: Otázka č. 8 – Místa využití kryptoměn k platbě

Zdroj: Vlastní zpracování

Záměrné vyhledávání míst s možností platby kryptoměnou

Z Grafu 5 vyplývá, že na otázku „Vyhledáváte cíleně místa/obchody, které umožňují platbu kryptoměnou?" odpověděla nadpoloviční většina (8 osob) respondentů záporně. Čtyři z celkového počtu respondentů odpověděli, že záměrně tato místa nevyhledávají, ovšem je-li ta možnost, tak platbu kryptoměnou využijí. Tři respondenti odpověděli, že taková místa záměrně vyhledávají.



Graf 5: Otázka č. 9 – Záměrné vyhledávání míst s možností platby kryptoměnou

Zdroj: Vlastní zpracování

Pravidelné návštěvy restaurace/kavárny s využitím platby kryptoměnou

Dvě třetiny respondentů odpověděli na otázku, zda pravidelně navštěvují nějakou restauraci či kavárnu, kde využívají platbu kryptoměnou, negativně. Zbylá třetina respondentů uvedla Paralelní Polis v Holešovicích, kde se nachází kavárna Bitcoin Coffee přijímající platby pouze v kryptoměnách.
Odpovědi v této otázce mohou být mírně zkreslené, neboť většina respondentů nepochází z Prahy a v menších městech v České republice je možnost platby kryptoměnou více omezená.

Hlavní výhody související s užíváním kryptoměn

Pro většinu respondentů je hlavní výhodou spojenou s užíváním kryptoměn anonymita a skutečnost, že jsou kryptoměny decentralizované. Dalšími zmiňovanými výhodami jsou rychlost, kontrola vlastních financí, jednoduchost užívání kryptoměn, jejich vzácnost či užitečnost v případě „havárie" fiat měny.

Hlavní nevýhody související s užíváním kryptoměn

Nejčastěji zmiňovanou nevýhodou je malá rozšířenost mezi obchodníky a s tím související menší užitná hodnota, a možnost hackerských útoků. Další vícekrát zmíněnou nevýhodou je technologická složitost kryptoměn a s ní spojená horší dostupnost pro starší a méně technicky zdatné osoby. Respondenti mezi nevýhodami zmiňovali také

vysokou volatilitu kryptoměn a velký vliv neznámých faktorů na jejich kurz.
Jeden z respondentů uvedl, že nevidí žádné nevýhody související s užíváním kryptoměn.

Akceptace kryptoměn v českém prostředí

K této otázce nezaujali tři respondenti žádný postoj nebo nevěděli, jak na ni odpovědět. Ostatní respondenti vesměs cítí v českém prostředí progres, ale velmi pomalý. Jeden z respondentů uvedl, že ČR se nachází ve srovnání s ostatními zeměmi nad průměrem - obzvláště pak Praha.
Zmíněn byl také postoj zákonodárců, kteří dle odpovědi respondenta neumí problematiku uchopit, jelikož se jedná o technologicky příliš novou věc a zároveň je omezena možnost řízení, regulace a kontroly.

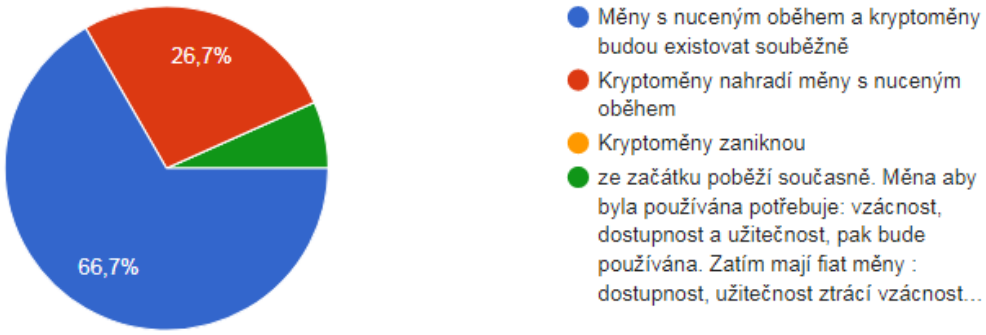
Profil uživatele kryptoměn

Třetina respondentů uvedla, že není schopna definovat profil uživatele kryptoměn, v jednom případě bylo upřesněno, že je tomu tak z důvodu příliš vysokých odlišností v profilech uživatelů.
Ostatní respondenti uváděli především technologickou zdatnost uživatelů a blízkost k IT oboru či oboru financí. Dále pak bylo uváděno, že uživatel kryptoměn je povětšinou osoba hledající nové možnosti a osoba s vizemi, která se nespokojila se současným ekonomickým modelem a má touhu po svobodě. Uživatelé kryptoměn byli také respondenty zařazeni do skupiny spekulantů.

Budoucnost kryptoměn

Jak je možné vidět v Grafu 6, dvě třetiny respondentů se domnívají, že v budoucnu budou kryptoměny a měny s nuceným oběhem existovat souběžně. Čtyři z patnácti respondentů věří ve vývoj kryptoměn na takové úrovni, kdy nahradí fiat měny. Jeden z respondentů zvolil vlastní odpověď, kdy se domnívá, že kryptoměny a fiat měny ze začátku poběží současně. Svoji odpověď odůvodnil argumenty, které zní: „Měna aby byla používána, potřebuje: vzácnost, dostupnost a užitečnost, pak bude používána. Zatím mají fiat měny: dostupnost, užitečnost ztrácí vzácnost. Kryptoměny mají vzácnost, chybí jim však užitečnost. Ta nastane, až ztratí užitečnost fiat měny. Pak

dojde k zániku měn s nuceným oběhem a budou používány kryptoměny, nebo budou oba druhy měn používány současně.“



Graf 6: Otázka č. 15 – Budoucnost kryptoměn

Zdroj: Vlastní zpracování

Volná poznámka k tématu

Možností přispění volnou poznámkou k tématu využili tři respondenti.
První z nich uvedl, že se kryptoměnami zabýval jako příležitostí k obohacení, ovšem zatím v tomto směru nevidí výsledky.
Druhý respondent uvedl, že se domnívá, že z kryptoměn má velkou budoucnost pouze Bitcoin. Tento názor zastává, jelikož se domnívá, že všechny ostatní coiny jsou závislé na někoho rozhodnutí a jen Bitcoin funguje zcela nezávisle.
Poslední z respondentů, který využil volné poznámky k tématu, uvedl: „Kryptoměny jsou tu proto, že nastává transformace myšlení. Pokud se lidstvo rozhodne, jít některým ze směrů změny myšlení, může dojít ke změnám nevídaných rozměrů a to jak v dobrém tak ve špatném modelu.“

6.1 Shrnutí výsledků kvalitativního šetření

Tato kapitola slouží k shrnutí nejdůležitějších výsledků provedeného dotazníkového šetření.

V rámci kvalitativního šetření bylo pomocí dotazníků zpovídáno 15 osob, které se tématem kryptoměn dlouhodobě zabývají. Jednalo se pouze o muže především mladší až střední věkové kategorie s převážně středoškolským a vysokoškolským vzděláním.

Respondenti se zajímají především o kryptoměny Bitcoin, Ethereum a Monero. Místem využití kryptoměn k platbě jsou pro respondenty především internetové obchody.

Motivací k zájmu o kryptoměny je pro respondenty především vlastnost decentralizace a anonymita s jejich používáním spojená. Dále je to pak využití kryptoměn jako alternativního platidla, ovšem respondenti místa, kde kryptoměny přijímají, spíše nevyhledávají.

Jako hlavní nevýhodu spojenou s užíváním kryptoměn respondenti vidí malou využitelnost v současné době, protože kryptoměny přijímá stále pouze zlomek obchodníků. S tím souvisí i předpokládaný výhled do budoucna, kdy se dvě třetiny respondentů domnívají, že kryptoměny a měny s nuceným oběhem budou existovat souběžně.

7 NÁVRHY A DOPORUČENÍ

Cílem této kapitoly je na základě vlastního pozorování a provedeného kvalitativního šetření shrnout čtenáři návrhy a doporučení, jak v současné době nakládat s kryptoměnami jako alternativním platidlem.

Rozšířenost kryptoměn a jejich popularita stále narůstá, ovšem jejich využitelnost u obchodníků je v současné době ještě pořád poměrně malá, především pak mimo Prahu. V Praze lze již nalézt několik desítek míst, kde jsou kryptoměny akceptovány, zájemce o tyto platby se o to musí ovšem sám aktivněji zajímat. Podrobný a dobře zpracovaný přehled, kde lze kryptoměny uplatnit je možné nalézt například na portálu coinmap.org.

Kryptoměny slouží na dobrovolné bázi ze strany obchodníků jako prostředek směny, ovšem nelze je považovat za zúčtovací jednotku z důvodu vysoké volatility cen, ani je nelze označit za uchovatele hodnoty, jelikož nejsou legislativně jednoznačně definovány. Z těchto důvodů by dle mého názoru mělo být do kryptoměn investováno pouze tolik, o kolik je investor ochoten v nejhorším možném scénáři přijít.

Dnešní doba internetu nahrává všem zájemcům o toto aktuální téma, proto bych všem, kteří by chtěli kryptoměny využívat k platbám doporučila nastudovat si alespoň základy této problematiky. Existuje dostatek informačních portálů v českém i anglickém jazyce, kde lze nalézt ověřené informace od osob, které se kryptoměnami dlouhodobě zabývají. Příkladem takových portálů jsou btctip.cz, kryptomagazin.cz, cryptosvet.cz, kryptoportal.cz, bitcoinmagazin.com, coindesk.com, atd.

Platby kryptoměnou se vyplatí uživatelům, kteří již nějaké kryptoměny vlastní, případně je sami těží, jelikož je s těmito platbami spojeno několik výhod, jako jsou anonymita, rychlost plateb, poměrně jednoduché uživatelsky přívětivé provádění plateb s mobilní aplikací, atd.

Pro uživatele, kteří se ovšem hlouběji o kryptoměny nezajímají a chtějí je využívat pouze jako alternativní platidlo v kavárnách či jiných podnicích, nemusí být využívání kryptoměn až tak výhodné. Rozměňuje-li si uživatel fiat měnu za kryptoměnu v bankomatu, platí stále poměrně vysoké poplatky a navíc musí počítat s určitou

časovou prodlevou, než jsou kryptoměny do peněženky připsány (prodleva u Bitcoinu může být až několik desítek minut). Samotný začátek používání kryptoměn, od pořízení peněženky, nákupu kryptoměny, přes platbu, je ovšem velmi jednoduchý a stačí k tomu základní zdatnost ovládání moderních technologií. Z tohoto důvodu jsou pravděpodobně kryptoměny využívány především mladší a střední generací, ovšem ani starší generace občanů, která se o nové technologie alespoň základním způsobem zajímá, nemusí mít z využívání kryptoměn strach.

Zájemcům o problematiku kryptoměn, ať již z řad začátečníků či pokročilých uživatelů, bych doporučila návštěvu Paralelní Polis v Holešovicích. Tam si lze nejen vyzkoušet nákup kryptoměn v bankomatu a platbu kryptoměnou v jediné kavárně v České republice přijímající platby výhradně v kryptoměnách, ale také se lze zúčastnit některé ze zajímavých přednášek či workshopů o kryptoměnách a tématech s nimi spojených.

S ohledem na výše uvedené poznatky a informace nabité v odborné literatuře bych čtenářům doporučila se problematikou kryptoměn zabývat. Je totiž velmi pravděpodobné, že budou mít v budoucnosti (vzhledem k rychlosti vývoje jejich i ostatních moderních technologií) značné využití.

Závěr

Diplomová práce je zaměřena na téma „Kryptoměny a možnosti jejich využití v praxi". Cílem této diplomové práce bylo zmapování a vyhodnocení praktických možností využití kryptoměn ve vybraných kavárnách v Praze.

Teoretická část diplomové práce je opřena o poznatky z odborné literatury a odborných internetových zdrojů. První část se zabývá vymezením pojmu peněz a kryptoměn z ekonomického (nikoliv právnického) hlediska, aby bylo možné jejich srovnání při snaze hledat možnosti využití kryptoměn jako alternativního platidla. V další části jsou podrobněji představeny samotné kryptoměny od jejich historie, základních definičních znaků a principů a uživatelských pohledů na kryptoměny. Zároveň jsou podrobněji představeny tři uživatelsky více rozšířené kryptoměny a teoreticky popsány kroky, které předchází užívání kryptoměn v praxi. Poslední kapitola teoretické části je věnována využití kryptoměn ve sportu. Tato kapitola byla zařazena, aby čtenářům bylo přiblíženo další odvětví, kde k využití kryptoměn a jejich základních principů dochází. Jelikož jsou kryptoměny rozsáhlé a neustále se vyvíjející téma, může tato diplomová práce sloužit pouze jako zdroj základních informací.

Praktická část diplomové práce měla za cíl analyzovat možnosti využití kryptoměn jako alternativního platidla, konkrétně se zaměřením na kavárny v Praze. Nejprve byly představeny poznatky o užívání kryptoměn v praxi na základě vlastního pozorování. Následně bylo provedeno kvalitativní šetření ve formě dotazníků pro získání více informací a pohledů na kryptoměny mezi osobami, které se touto problematikou aktivně zabývají.

Závěrečná kapitola diplomové práce je věnována návrhům a doporučením pro čtenáře, kteří by se chtěli zabývat kryptoměnami a možnostmi jejich využití jako alternativním způsobem platby. Návrhy a doporučení byly zpracovány na základě šetření v praktické části diplomové práce, s přihlédnutím k informacím a poznatkům nabitým z odborných zdrojů.

Seznam použité literatury

1. HRBKOVÁ, Jana. Společenské vědy pro techniky: ekonomie, právo, politologie. Praha: Grada Publishing, 2015. Expert (Grada). ISBN 978-80-247-5588-5.
2. JANÁČKOVÁ, Stanislava. Lesk a bída měnové politiky: peníze tajemství zbavené?. Praha: Institut Václava Klause, 2015. Publikace. ISBN 978-80-87806-99-9.
3. KALISKÝ, Boris. Bitcoin a ti druzí: nepostradatelný průvodce světem kryptoměn. Praha: IFP Publishing, 2018. ISBN 978-80-87383-71-1.
4. LIPOVSKÁ, Hana. Kdo chce naše peníze?: ekonomie bez politické korektnosti. Praha: Grada, 2018. ISBN 978-80-271-0679-0.
5. MANKIW, N. Gregory. Zásady ekonomie. Praha: Grada, 1999. Profesionál. ISBN 80-7169- 891-1.
6. MISHKIN, Frederic S. The economics of money, banking and financial markets. 11th ed. Boston: Addison-Wesley, 2015. ISBN: 978-12-9209-418-2.
7. ŠTĚDROŇ, Bohumír a kol. Prognostika. V Praze: C.H. Beck, 2019. Beckova edice ekonomie. ISBN 978-80-7400-746-0.
8. VEBER, Jaromír a kol. Digitalizace ekonomiky a společnosti. Praha: Management Press, 2018. ISBN 978-80-7261-554-4.
9. VENCOVSKÝ, František. Vzestupy a propady československé koruny: historie československých měnových poměrů, 1918-1992. V Praze: Vysoká škola ekonomická, 2003. ISBN 80-245-0497-9.
10. VON MISES, Ludwig. The theory of money and credit. Translated by Harold E. Batson. Indianapolis: Liberty Fund, 1980. 537 s. ISBN 0913966703.
11. WHITE, Lawrence H. The theory of monetary institutions. Malden, Mass: Blackwell, 1999. ISBN 0-63121214-0.

Seznam použitých internetových zdrojů:

1. A PWC FRANCE INITIATIVE, How blockchain and its applications can help grow the sport industry? [online] 2019 [cit. 2020-04-21] Dostupné z https://www.pwc.ch/en/publications/2019/Blockchain%20in%20the%20Sports%20Industry.pdf
2. ALONSO M. Kurt, KOE Zero to Monero [online] [cit. 2020-01-06] Dostupné z https://www.getmonero.org/library/Zero-to-Monero-1-0-0.pdf
3. ASOLO, Bisade. Proof of Importance Expalined [online] [cit. 2020-03-01] Dostupné z https://www.mycryptopedia.com/proof-of-importance/
4. BATABYAL, Anisa. Monero Hard Fork 2019 Coming Up On November 30th [online] [cit. 2020-03-29] Dostupné z https://coinswitch.co/news/monero-hard-fork-2019-coming-up-on-november-30th-everything-you-need-to-know
5. BESTICOFORYOU. [online] [cit. 2020-02-07] Dostupné z https://besticoforyou.com/cs/guide-to-paper-wallets/
6. BITCOINWIKI. Bitcoin history [online] [cit. 2020-02-07] Dostupné z https://en.bitcoinwiki.org/wiki/Bitcoin_history
7. BITFINEX. [online] [cit. 2020-02-07] Dostupné z https://www.bitfinex.com/trading
8. BITPAY. What is the Network Cost fee on BitPay invoices, and why is BitPay charging it? [online] Poslední aktualizace 21. 12. 2019. [cit. 2020-02-20] Dostupné z https://support.bitpay.com/hc/en-us/articles/115002990803-What-is-the-Network-Cost-fee-on-BitPay-invoices-and-why-is-BitPay-charging-it-
9. CHAUM, DAVID. Blind signatures for untraceable payments [online] [cit. 2020-02-10] Dostupné z http://www.hit.bme.hu/~buttyan/courses/BMEVIHIM219/2009/Chaum.BlindSigForPayment.1982.PDF
10. CHEN, JAMES. Liberty Dollar. Poslední aktualizace z 2. 9. 2018. [cit. 2020-01-18] Dostupné z https://www.investopedia.com/terms/l/liberty-dollar.asp
11. COINDESK. [online] [cit. 2020-02-07] Dostupné z https://www.coindesk.com/price/bitcoin

12. COINMAP [online] [cit. 2020-04-02] Dostupné z https://coinmap.org/
13. COINMARKETCAP [online] [cit. 2020-03-29] Dostupné z https://coinmarketcap.com/
14. CROSBY Michael, NACHIAPPAN, PATTANAYAK Pradhan, VERMA Sanjeev, KALYANARAMAN Vignesh Blockchain Technology [online] [cit. 2020-02-05] Dostupné z https://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf
15. ČESKO. Zákon č. 370 ze dne 13. listopadu 2017 o platebním styku. In: Sbírka zákonů České republiky. Dostupné z: https://www.zakonyprolidi.cz/cs/2017-370#cast1
16. ČESKÝ STATISTICKÝ ÚŘAD. Podíl vysokoškoláků máme nižší než EU [online] Poslední aktualizace z 23. 7. 2018 [cit. 2020-04-12] Dostupné z https://www.czso.cz/csu/czso/podil-vysokoskolaku-mame-nizsi-nez-eu
17. FILLNER, Karel. Alza.cz vyslyšela přání zákazníků, akceptuje platbu Bitcoiny [online] [cit. 2020-03-10] Dostupné z https://btctip.cz/alza-cz-vyslysela-prani-zakazniku-akceptuje-platbu-bitcoiny/
18. FRANKENFIELD Jake, Double-spending [online] Poslední aktualizace z 2. 10. 2019[cit. 2020-03-02] Dostupné z https://www.investopedia.com/terms/d/doublespending.asp
19. HAY, Steven. Bitcoin (BTC) Halving History With Charts & Dates [online] [cit. 2020-02-07] Dostupné z https://www.coinmama.com/blog/the-bitcoin-halving-a-history/
20. HCash, The advantages of the Hybrid PoW+PoS consensus mechanism [online] [cit. 2020-03-01] Dostupné z https://medium.com/@media_30378/the-advantages-of-the-hybrid-pow-pos-consensus-mechanism-4e9ea4074ac0
21. HORČIČKA, Michal. Kryptoměny [online]. Brno, 2019 [cit. 2020-03-18]. Dostupné z: https://is.muni.cz/th/aej3x/ Bakalářská práce. Masarykova univerzita, Ekonomicko – správní fakulta. doc. Ing. Martin Svoboda, Ph.D.
22. IG. [online] [cit. 2020-02-07] Dostupné z https://www.ig.com/en/bitcoin-btc/bitcoin-halving
23. INFOCRYPTOLAND, COINOMI Wallet Review – A Complete Guide [online] Poslední aktualizace z 14. 11. 2018[cit. 2020-04-07] Dostupné z https://infocryptoland.com/language/en/coinomi-wallet-review-complete-guide/
24. JENKINSON, Gareth. Tokenizing Sports – How the Industry Is Incorporating Crypto [online] Poslední aktuali-

zace z 28. 7. 2019 [cit. 2020-04-22] Dostupné z https://cointelegraph.com/news/tokenizing-sports-how-the-industry-is-incorporating-crypto

25. LITE COIN WHITE PAPER [online] [cit. 2020-03-29] Dostupné z http://zioncoins.co.uk/wp-content/uploads/2015/06/Lite-Coin-Whitepaper.pdf-

26. NAKAMOTO, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System. [cit. 2020-03-29] Dostupné z https://bitcoin.org/bitcoin.pdf

27. PIHL, Rasmus. Crypto Hardware Maker Trezor Warns Of Fake Trezor One Devices [cit. 2020-02-07] Dostupné z https://toshitimes.com/crypto-hardware-maker-trezor-warns-of-fake-trezor-one-devices/

28. SABERHAGEN van Nicolas. CryptoNote v 2.0 [online] [cit. 2020-03-02] Dostupné z https://cryptonote.org/whitepaper.pdf

29. TRADEARENA. Co je digitální měna, kryptoměna nebo token Poslední aktualizace z 29. 7. 2019 [online] [cit. 2020-04-22] Dostupné z https://www.tradearena.cz/rubriky/aktuality/co-je-digitalni-mena-kryptomena-nebo-token_806.html

30. VPNMENTOR. How to accept Bitcoin Payments with BitcoinPay [online] [cit. 2020-03-10] Dostupné z https://www.vpnmentor.com/blog/how-to-accept-bitcoin-payments/

31. WIKIPEDIA. Crowdfunding [online] [cit. 2020-04-22] Dostupné z https://cs.wikipedia.org/wiki/Crowdfunding

32. WILMOTH Josiah Bitcoin Gold Hit by Double Spend Attack, Exchanges Lose Millions [online] [cit. 2020-03-29] Dostupné z https://www.ccn.com/bitcoin-gold-hit-by-double-spend-attack-exchanges-lose-millions

Seznam obrázků

Seznam tabulek

Seznam grafů

Seznam příloh

Seznam použitých zkratek

BTC	Bitcoin
ETH	Ethereum
GRN	GreenPower
LTC	Litecoin
MAID	MaidSafeCoin
NANO	Nano
P2P	peer-to-peer
PoI	Proof of Importance
PoS	Proof of Stake
PoW	Proof of Work
SHA256	Secure Hash Algorithms
USD	Americký dolar
XMR	Monero
XRP	Ripple
ZEN	ZenCash

Příloha 1: Otázky kvalitativního dotazníkového šetření

Dobrý den,
mé jméno je Marie Bradová a jsem studentkou 2. ročníku magisterského studia Masarykova ústavu vyšších studií ČVUT v Praze. Tímto bys Vás ráda požádala o vyplnění následujícího dotazníku, který bude sloužit jako podklad ke zpracování mé diplomové práce na téma "Kryptoměny a možnosti jejich využití v praxi".

Děkuji za Vaši ochotu a spolupráci.

1) Jméno:

2) Pohlaví*
   a. Muž
   b. Žena
   c. Nechci specifikovat

3) Věk*
   a. Méně než 18 let
   b. 18 – 29 let
   c. 30 – 45 let
   d. 46 – 60 let
   e. Více než 60 let

4) Nejvyšší dosažené vzdělání*
   a. Základní
   b. Středoškolské bez maturity
   c. Středoškolské s maturitou
   d. Vyšší odborné
   e. Vysokoškolské

5) Jak dlouho jste uživatelem/uživatelkou kryptoměn?*

6) Které konkrétní druhy kryptoměn používáte?*

7) Zajímáte se o fungování kryptoměn více? Pokud ano, co Vás k tomu vede? Nebo jste pouze uživatelem (kryptoměny využíváte pouze k nákupu/prodeji zboží)?*

8) Kde všude využíváte kryptoměny k platbě? (možnost zaškrtnout více odpovědí)*
   a. Kamenné obchody

b. Internetové obchody
c. Restaurace + kavárny
d. Jiná.....

9) Vyhledáváte cíleně místa/obchody, které umožňují platbu kryptoměnou?*
a. Ano
b. Ne
c. Ne, ovšem je-li možnost platby kryptoměnou, využiji ji

10) Navštěvujete pravidelně nějakou restauraci/kavárnu, kde využíváte platbu kryptoměnou? Pokud ano, prosím konkretizujte.*

11) V čem spatřujete hlavní výhody pro uživatele kryptoměn?*

12) V čem spatřujete hlavní nevýhody pro uživatele kryptoměn?*

13) Jak vnímáte situaci akceptace kryptoměn v českém prostředí?*

14) Jste schopný/á definovat profil uživatele kryptoměn?*

15) Jaký je Váš názor na budoucnost kryptoměn?*
a. Měny s nuceným oběhem a kryptoměny budou existovat souběžně
b. Kryptoměny nahradí měny s nuceným oběhem
c. Kryptoměny zaniknou
d. Jiná.....

16) Volná poznámka k tématu

* Povinná otázka

Evidence výpůjček

Prohlášení:
Dávám svolení k půjčování této diplomové práce. Uživatel potvrzuje svým podpisem, že bude tuto práci řádně citovat v seznamu použité literatury.

Jméno a příjmení: Marie Bradová
V Praze dne: 10. 05. 2020 Podpis:

Jméno	**Oddělení/ Pracoviště**	**Datum**	**Podpis**