



Kryptoměny v podnikatelském prostředí

Bakalářská práce

Studijní program: B6208 – Ekonomika a management

Studijní obor: 6208R085 – Podniková ekonomika

Autor práce: **Martin Kvíz**

Vedoucí práce: doc. Ing. Jan Skrbek, Dr.





Zadání bakalářské práce

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení: **Martin Kvíz**
Osobní číslo: E16000018
Studijní program: B6208 Ekonomika a management
Studijní obor: B6208R085 – Podniková ekonomika
Zadávací katedra: katedra informatiky
Vedoucí práce: doc. Ing. Jan Skrbek, Dr.
Konzultant práce: Tomáš Příhoda
Kryptoinvestor, Trader a specialista na analýzu a správu kryptoměn

Název práce: **Kryptoměny v podnikatelském prostředí**

Zásady pro vypracování:

1. Stanovení cílů bakalářské práce.
2. Bezpečnost kryptoměn.
3. Platební možnosti a porovnání se současnými možnostmi platby.
4. Výhody, rizika a trendy použití kryptoměn v podnikatelském prostředí.
5. Formulace závěrů a zhodnocení.

Seznam odborné literatury:

- ANTONOPOULOS, Andreas M. 2015. *Mastering bitcoin*. Sebastopol: O'Reilly Media. ISBN 978-1-4493-7404-4.
- POPPER, Nathaniel. 2016. *Digital gold: bitcoin and the inside story of the misfits and millionaires trying to reinvent money*. New York: Harper. ISBN 978-006-2362-506.
- SKALICKÝ, Jan. 2018. *Bitcoin a jiné kryptoměny budoucnosti: historie, ekonomie a technologie kryptoměn, stručná příručka pro úplné začátky*. 2. vyd. Praha: Grada Publishing. ISBN 978-80-271-0742-1.
- TAPSCOTT, Alex. 2016. *Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world*. New York: Portfolio. ISBN 978-039-9564-062.
- PROQUEST. Hrůza, R. (2017). ANALÝZA BITCOINU, JEHO VÝVOJ NA TRHU A STATISTICKÉ VÝPOČTY ROZIKOVOSTI A ZISKOVOSTI. *Mladá Věda*, 5(10), 9-16. Retrieved from <https://search.proquest.com/docview/1989175514?accountid=17116>

Rozsah práce: min. 30 normostran
Forma zpracování: tištěná / elektronická
Datum zadání práce: 1. října 2018
Datum odevzdání práce: 31. srpna 2020



prof. Ing. Miroslav Žižka, Ph.D.
děkan Ekonomické fakulty

doc. Ing. Klára Antlová, Ph.D.
vedoucí katedry

V Liberci dne 31. října 2018

Prohlášení

Byl jsem seznámen s tím, že na mou bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb., o právu autorském, zejména § 60 – školní dílo.

Beru na vědomí, že Technická univerzita v Liberci (TUL) nezasahuje do mých autorských práv užitím mé bakalářské práce pro vnitřní potřebu TUL.

Užiji-li bakalářskou práci nebo poskytnu-li licenci k jejímu využití, jsem si vědom povinnosti informovat o této skutečnosti TUL; v tomto případě má TUL právo ode mne požadovat úhradu nákladů, které vynaložila na vytvoření díla, až do jejich skutečné výše.

Bakalářskou práci jsem vypracoval samostatně s použitím uvedené literatury a na základě konzultací s vedoucím mé bakalářské práce a konzultantem.

Současně čestně prohlašuji, že tištěná verze práce se shoduje s elektronickou verzí, vloženou do IS STAG.

Datum:

Podpis:

PODĚKOVÁNÍ:

Především děkuji vedoucímu bakalářské práce doc. Ing. Janu Skrbkovi, Dr., za odborné vedení, cenné rady a příkladné vedení práce. Poděkování patří i mé rodině za podporu po celou dobu studia.

ANOTACE:

Bakalářská práce se zabývá použitím kryptoměn v podnikatelském prostředí. Nejprve vysvětluje, co jsou kryptoměny a na jakém principu fungují. Dále se zabývá problematikou bezpečnosti a využitím kryptografie. Následné kapitoly se zaměřují na současné platební možnosti a porovnávají je se stávajícími platebními nástroji. Závěr práce nastiňuje budoucí vývoj a přináší celkové shrnutí hodnocení kryptoměn v podnikatelském prostředí.

Klíčová slova:

Bitcoin, Ethereum, Kryptoměny

ANNOTATION:

Cryptocurrency in a business environment

The bachelor thesis deals with the use of cryptocurrencies in business environment. First chapter explains basis of cryptocurrencies and its generic principles. Next part describes the security of cryptocurrencies and usage of cryptography. Additional chapters focus on its payment options and comparison with current payment tools. Last section outlines future development and brings a summary of cryptocurrencies in business environment.

Keywords:

Bitcoin, Cryptocurrency, Ethereum

OBSAH:

ÚVOD:.....	13
1. KRYPTOMĚNY.....	14
1.1 MĚNA.....	14
1.2 ROZDĚLENÍ KRYPTOMĚN.....	15
1.3 VÝVOJ PENĚŽ	15
1.3.1 <i>Papírové peníze</i>	16
1.3.2 <i>Funkce peněz</i>	16
1.4 HISTORIE KRYPTOMĚN.....	16
1.5 PRVNÍ DIGITÁLNÍ MĚNY.....	17
1.5.1 <i>Ecash</i>	17
1.5.2 <i>E-gold</i>	18
1.5.3 <i>Liberty Dollar</i>	18
1.5.4 <i>CyberCoin</i>	18
1.5.5 <i>E-Bullion</i>	19
1.6 NOVÉ KRYPTOMĚNY.....	19
1.6.1 <i>Tržní kapitalizace</i>	20
1.7 VZNIK DIGITÁLNÍCH MĚN	21
1.8 BITCOIN.....	22
1.8.1 <i>Těžba bitcoinů</i>	22
1.8.2 <i>Použití měny bitcoin</i>	23
1.8.3 <i>Tři hlavní formy bitcoin klientů</i>	23
1.8.4 <i>Platba</i>	23
1.9 ETHEREUM.....	24
1.9.1 <i>Chytrý kontrakt</i>	25
1.9.2 <i>Výhody Etherea</i>	25
2 BEZPEČNOST KRYPTOMĚN	26
2.1 BLOCKCHAIN.....	26
2.1.1 <i>Decentralizace</i>	27
2.1.2 <i>Genesis blok</i>	27
2.1.3 <i>Struktura bloku</i>	28
2.2 GENERACE BLOCKCHAINU	28
2.3 SPUŠTĚNÍ.....	29
2.4 SOUKROMÍ.....	29
2.5 KVANTOVÝ BLOCKCHAIN.....	30
2.6 KRÁDEŽE.....	30
2.7 KRYPTOGRAFIE (CRYPTOGRAPHY).....	30
2.7.1 <i>Kryptografie eliptických křivek</i>	31
2.7.2 <i>Úroveň zabezpečení</i>	31
2.7.3 <i>Šifrování</i>	32
2.7.4 <i>P2P (peer to peer)</i>	32
3 PLATEBNÍ MOŽNOSTI A POROVNÁNÍ SE SOUČASNÝMI MOŽNOSTMI PLATBY	33
3.1 PLATEBNÍ MOŽNOSTI.....	33
3.1.1 <i>Rozdíly v platbách</i>	33
3.2 PLATBA ZA ZBOŽÍ POMOCÍ KRYPTOMĚN	35
3.3 SMĚNÁRNY A BURZY	35
3.3.1 <i>Nevýhody při obchodování</i>	36
3.4 ZKRACHOVALÉ BURZY A SMĚNÁRNY	36
3.4.1 <i>MtGox</i>	36
3.4.2 <i>QuadrigaCX</i>	36
3.4.3 <i>Coinrail</i>	37
3.5 PENĚŽENKA	37
3.5.1 <i>Hot wallet</i>	37

3.5.2 Cold wallet.....	38
3.6 KRYPTOMĚNY Z DAŇOVÉHO POHLEDU.....	38
3.6.1 Obchod.....	38
3.6.2 Těžba.....	39
3.6.3 DPH.....	39
3.7 KRYPTOMĚNY Z ÚČETNÍHO POHLEDU.....	39
3.8 VÝHODY, RIZIKA A TRENDY POUŽITÍ KRYPTOMĚŇ.....	40
3.8.1 Výhody.....	40
3.8.2 Rizika.....	40
3.8.3 Trendy.....	40
3.9 ZÁKAZY A OMEZENÍ KRYPTOMĚŇ.....	40
3.9.1 Čínská lidová republika.....	40
3.9.2 Ruská federace.....	41
4 PODNIKATELSKÉ PROSTŘEDÍ.....	42
4.1 COINBASE.....	42
4.2 ELEKTRONICKÉ HLASOVÁNÍ.....	42
4.3 TĚŽBA BITCOINU ČÍNSKÉ LIDOVÉ REPUBLICE.....	43
4.4 MEDICALCHAIN.....	44
4.5 GENERAL BYTES.....	45
4.5.1 Nákup a prodej.....	46
4.6 GENESIS COIN.....	47
4.7 LAMASSU.....	48
4.8 GLOBALCOIN OD FACEBOOKU.....	49
4.9 VYUŽITÍ NASA.....	50
5.0 COINMAP.....	50
5 PREDIKACE VÝVOJE KRYPTOMĚŇ JAKO PLATIDLA.....	53
5.1 KRYPTOMĚNY STÁLE NA ZAČÁTKU.....	53
5.2 ROK 2017.....	53
5.3 ROK 2018.....	54
5.4 RYCHLÉ ZBOHATNUTÍ.....	54
6 ZÁVĚR - FORMULACE ZÁVĚRŮ A ZHODNOCENÍ.....	56
SEZNAM CITACÍ:.....	57
SEZNAM LITERATURY:.....	58

Seznam ilustrací:

Obrázek 1 - Ethereum logo.....	24
Obrázek 2 - platforma Medicalchain	44
Obrázek 3 - kryptoměnový bankomat General Bytes.....	46
Obrázek 4 - kryptoměnový bankomat Genesis Coin.....	48
Obrázek 5 - Sintra od Lamassu	49
Obrázek 6 - platba kryptoměnami v Praze.....	51
Obrázek 7 - možnost platby kryptoměn ve světě.....	52

Seznam tabulek:

Tabulka 1 – Tržní kapitalizace 10 největších kryptoměn.....	21
Tabulka 2 – dělení bitcoinu.....	22
Tabulka 3 - vývoj hodnoty bitcoinu.....	24
Tabulka 4 – porovnání platebních nástrojů.....	34

Seznam zkratek

BTC Bitcoin

ECC Kryptografie na bázi eliptických křivek

ETH Ethereum

ICO Počáteční nabídka mincí

Úvod:

Předmětem této bakalářské práce je predikovat vývoj v oblasti kryptoměn a zaměřit se na možnosti jejich uplatnění v budoucnu. K tomuto tématu patří rovněž vliv kryptoměn na finanční trhy a jejich použití jako platidla.

S dnešními technologiemi, které se dynamicky vyvíjí, se nabízí více možností, jak naložit s volnými finančními prostředky. Velká část populace vyspělých zemí již běžně používá bezhotovostní platby. Stále to jsou stejné peníze, jen metody placení jsou různé. S kryptoměnami je to však jiné. Za peníze je nakupována jiná digitální měna, která mění svou hodnotu dle aktuálního kurzu. Kryptoměny, na rozdíl od ostatních měn, nejsou řízeny státem, tím se odlišují od současných metod placení, to se výrazně dotýká i podnikatelského prostředí.

Kryptoměny jsou poměrně novou záležitostí, proto se první kapitola práce věnuje rozdělení kryptoměn a jejich historii. Dále je popsán vývoj peněz v čase a jejich využití k různým platbám za zboží. Následující část pojednává o prvních neúspěšných kryptoměnách, ze kterých následně vznikly ty současné, jako je bitcoin nebo ethereum. Kapitola o bezpečnosti kryptoměn je zaměřená na technologii blockchain, její význam a vývoj. Důležitou součástí tématu je možnost jejich počátečního financování. Následující kapitola se zabývá nákupem a prodejem kryptoměn, jak se uskutečňuje ve směnárnách a burzách. Významná část práce se zabývá kryptoměnami v podnikatelském prostředí. Je uvedeno několik příkladů použití kryptoměn napříč různými obory podnikatelských činností. Následně je práce završena predikcí vývoje kryptoměn s dopadem na podnikatelské prostředí.

Dílčím cílem bakalářské práce je na základě literární rešerše a dostupných databázových podkladů charakterizovat vývoj kryptoměn od počátku po současnost. Hlavním cílem je možnost zhodnocení kryptoměn v podnikatelském prostředí s možnostmi použití. Dalším dílčím cílem je analyzovat použití v podnikatelském prostředí a specifikovat vybrané obory s možnostmi jejich použití. Významným dílčím cílem je posoudit řešení bezpečnosti prostřednictvím technologie blockchain, na které kryptoměny fungují včetně možnosti bezpečného uložení. Dalším dílčím cílem je porovnat platební možnosti se současnými metodami platby a přinést několik praktických ukázek využití v obchodním styku.

Kryptoměny se stále více začínají prosazovat jako platidlo a to nejen v podnikatelském prostředí, ale i v běžném životě.

1. Kryptoměny

Kryptoměna je složením dvou slov – krypto a měna. Krypto je označení pro šifrování, které používají kryptoměny pro svou ochranu. Kryptoměny jsou digitální peníze, které nemají fyzickou hodnotu. Hodnota kryptoměn je závislá na nabídce a poptávce po konkrétní měně. Tento prvek je stejný s měnou, kterou každý zná a používá ji v každodenním životě. V dnešní době je kryptoměn několik tisíc, ale jen některé z nich uspějí.

Kryptoměny pomáhají rozvoji podnikatelského prostředí na globálním trhu. Díky tomu, že je možné kryptoměny kupovat a prodávat téměř kdekoli na světě, jsou platby a následná výměna za peněžní oběživo poměrně jednoduché. Nevýhodou je vyšší volatilita některých kryptoměn.

1.1 Měna

Měna je forma peněz. Je to platební prostředek vydávaný odlišnými zeměmi, ale se stejným záměrem. Používá se především jako platidlo a musí splňovat několik podmínek. Měna sama o sobě nemá žádnou hodnotu. Hodnota je stanovena obecnou hodnotou. Nejčastěji měnu vydává veřejný subjekt, kterým je centrální banka daného státu. Měna je oběživo uvnitř konkrétního státu, většinou toho, který ji vydal. Samozřejmě existuje mnoho výjimek. Jsou státy, které nepoužívají pouze jednu měnu, ale několik měn zároveň. Každá měna je označena třemi písmeny podle standardu ISO 4217. Mezi nejznámější měny patří EUR, USD, GBP. Hodnota jednotlivých měn je závislá na aktuální situaci na trhu a na měnovém kurzu. Měnový kurz se dá považovat za cenu peněz. Díky tomu si lze přepočítat, co kolik stojí v jiné měně. Měnový kurz je často používán při přepočítávání hodnoty peněz například při návštěvách zahraničních destinací. Tímto způsobem lze lehce spočítat, jaká je cena zboží v jednotlivých zemích.

Dříve byly všechny peníze kryté zlatem, hovořilo se o takzvaném zlatém standardu. Dnes již zlatý standard neplatí a peníze jsou tištěny dle potřeby, což má negativní dopad na inflaci (Peníze, 2019).

1.2 Rozdělení kryptoměn

Každá kryptoměna má své vlastní tokeny. Například u bitcoinu je token označen BTC a u etherea je označen ETH. Tokeny nemají svou vlastní síť a jsou součástí blockchainu jiné kryptoměny. Fungují pomocí chytrých kontraktů. Právě pro plnění těchto účelů vzniklo ethereum a následně i další měny, mezi které patří NXT a NEO.

Coiny jsou provozovány na své vlastní blockchainové síti. Mezi takové kryptoměny patří měna bitcoin, litecoin nebo ripple. Většina coinů se těží, ale není to pravidlem, výjimkou je již výše zmíněný ripple (Antonopoulos, 2015).

Kryptoměny vznikly především proto, aby konkurovaly měnovému systému. Mohou pomoci státům, které mají vysokou inflaci vlastní měny. Mezi takové státy můžeme zařadit například Venezuelu, kde inflace na konci roku 2018 přesáhla milion procent (Aktuálně, 2018).

Kryptoměny nabízejí velmi zajímavou nabídku v podobě rychlého převodu prostředků. Jelikož jsou kryptoměny na akciovém trhu, je možné je zakoupit kdykoliv. To dělá z kryptoměn ideálního konkurenta pro peněžní převody. Převod je zde levný a kryptoměny se dají převádět i do ostatních zemí. Kryptoměny jsou zajímavým řešením pro všechny, kteří nevěří nebo nechtějí využívat současný bankovní systém.

1.3 Vývoj peněz

Před vznikem peněz byl směnný obchod, tzv. barter, jedinou možností, jak uskutečnit obchod. Jedná se o výměnu zboží či služby za jiné zboží nebo služby, bez použití peněz. Také je označován jako starodávná forma výměnných obchodů, která se používá dodnes.

Ve starověkém Babylóně se prvním platidlem stalo obilí, v říši Aztéků to byly kakaové boby, ve starověké Číně se platilo mušlemi a Slované platili plátnem. Výhodou barteru je ušetření nákladů, směna nepotřebného zboží a nakupování bez cash flow (bez příjmu a výdeje peněžních prostředků). Mezi nevýhody patří neznalost účtování barterů, nadhodnocení barterů, nalezení oboustranné shody poptávaných či nabízených služeb a zboží.

S vývojem společnosti dochází ke vzniku nových platebních prostředků. Nejstarší písemné záznamy pořízené klínovým písmem jsou ze starověké Mezopotámie, kde se platilo formou váženého množství stříbra.

Zrod peněz je ekonomicky podmíněn rozvojem výroby, specializací výrobců a etapami rozvoje společenské dělby práce. Dělbá práce si vynutila směnu, nejdříve naturální, a poté se hledaly různé ekvivalenty. V současnosti se ve vyspělých ekonomikách používá naturální směna pod názvem barterová výměna.

Peníze jsou oběživem a všeobecným směnným prostředkem. Vystupují v různých podobách, nejčastěji jako kovové či papírové. Kovové peníze jsou mince, které jsou státem raženy z kovu pro peněžní účely. Tyto mince mají různé vlastnosti, které jsou na nich osvědčeny razidlem, jako je např. váha či jakost. Kovové peníze byly postupně nahrazovány papírovými penězi a v dnešní době se používají jen na menší platby.

1.3.1 Papírové peníze

První papírové peníze jsou z Číny, byly to ručně psané stvrzenky používané místo těžkých kovových mincí. Stát začal v 11. století vydávat vlastní stvrzenky, které mohly být úředně používány jako peníze. První tištěné papírové peníze v Evropě začala vydávat Švédská Stockholmská banka v roce 1671. Na našem území se první papírové peníze začaly vydávat za Marie Terezie. Peníze vznikly za účelem usnadnění obchodování (Peníze, 2019).

1.3.2 Funkce peněz

Peníze mají 3 hlavní funkce.

- Jednotka zúčtování – peníze slouží jako univerzální nástroj pro vyjádření hodnoty zboží či služeb.
- Prostředek směny – peníze lze libovolně směňovat za zboží a služby. Peníze jsou neutrální prostředek pro nákup.
- Uchovatel hodnoty – peníze jsou forma majetku. Pomocí peněz lze majetek akumulovat.

1.4 Historie kryptoměn

Historie kryptoměn není nijak dlouhá, začíná se datovat od počátku 90. let. Jejich oblibu způsobilo až obrovské rozšíření internetu. Ze začátku byly tyto měny nazývány digitálními

penězi. Spousta těchto digitálních peněz byla neúspěšná, ale s každou další neúspěšnou měnou se posouval vývoj stále kupředu. (Skalický, 2018)

Tyto počáteční digitální měnové projekty vydaly digitální peníze, zpravidla podporované národní měnou nebo drahými kovy, jako je zlato. Ačkoliv dřívější digitální měny fungovaly, byly centralizované, měly daného zakladatele, a v důsledku toho byly snadno napadnutelné hackery a vládami. Dřívější digitální měny používaly k vyrovnání všech transakcí v pravidelných intervalech centrální zúčtovací středisko, stejně jako tradiční bankovní systém. Naneštěstí ve většině případů byly tyto vznikající digitální měny cílem znepokojených vlád a nakonec byly eliminovány. Aby bylo možné zabránit zásahu zvenčí, bylo potřeba vytvořit decentralizovanou digitální měnu, která nemá žádný ústřední orgán nebo kontrolní bod, který by mohl být napaden. První takovou měnou je bitcoin. Ten představuje desetiletí výzkumu v oblasti kryptografie a distribuovaných systémů. Obsahuje 4 klíčové inovace spojené dohromady (Antonopoulos, 2015).

1. Decentralizovanou síť peer-to-peer (bitcoin protokol)
2. Veřejnou transakční knihu (blockchain)
3. Decentralizovanou matematickou a deterministickou distribuci měny (distribuovaná těžba)
4. Systém decentralizovaného ověřování transakcí (transakční skript)
(Antonopoulos, 2015)

1.5 První digitální měny

1.5.1 Ecash

Jedna z prvních velkých digitálních měn byla Ecash, která přišla v roce 1990. Přišla s ní společnost Digicash založená kryptografem Davidem Chaumem. David Chaum je často označován za otce kryptoměn. Ecash byl určitým předchůdcem dnešních kryptoměn, vyvinutý především pro prostředí veřejné sítě typu Internet.

David Chaum během devadesátých let představil několik klíčových inovací v prostředí digitální komunikace. Ecash vycházel z kryptografického systému pro anonymní transakce, s kterým přišel v roce 1982. Ecash měl sloužit pouze k menším transakcím peněžních prostředků, které by bylo možné jednodušeji převádět. V dané době bylo převádění i

menších peněžních prostředků složité a neefektivní, ať šlo o použití platebních karet, či šeků. Systém byl založen na anonymitě, kterou Chaum požadoval. Nejspíše kvůli tomu nebylo možné do tohoto systému začlenit i státní peníze a následně zbankrotoval. Chaum je známý svým negativním postojem vůči vládě. Přišel i s myšlenkou anonymní decentralizované komunikace, zvanou Tor. Tato komunikace je založena na principu přepojování komunikace mezi počítači po celém světě. Hlavním důvodem byla anonymita, díky tomuto principu nebylo možné zjistit, odkud komunikace pochází.

1.5.2 E-gold

V brzké době vzniklo hned několik dalších digitálních měn. Jednou z těchto měn byla i digitální měna E-gold. E-gold byla založena na principu krytí skutečným zlatem. Nevýhodou bylo, že byla měna závislá na jiné měně. Naneštěstí se ukázalo, že stát nebude podobnou konkurenci tolerovat. Jelikož tvůrci E-goldu byli známí, vláda mohla lehce dané osoby poslat před soud. Nakonec měna E-gold skončila.

1.5.3 Liberty Dollar

Bernard von NotHaus v roce 2011 založil měnu Liberty Dollar, která se postupem času stala populární. NotHaus si všiml, že od zlatého standardu nejsou peníze kryté zlatem, ani ničím jiným. Vytvořil tedy danou měnu, která byla krytá cennými kovy. Vláda následně rozhodla, že lze toto považovat za terorismus. NotHaus byl následně odsouzen za praní špinavých peněz a terorismus. U soudu prokurátorka argumentovala tím, že se NotHaus snažil zničit měnu vlastní země. Pohledy na to, zda chtěl měnu zničit, nebo zachránit, jsou různé (Skalický, 2018).

1.5.4 CyberCoin

Další neúspěšnou měnou byl CyberCoin, který poukázal na dřívější problém internetu. CyberCoin byla měna vytvořená společností CyberCash na konci devadesátých let. Počítačovní vývojáři se v devadesátých letech snažili ušetřit nějaké to místo v paměti počítače a zapisovali rok pomocí dvou čísel. Problém spočíval v tom, že počítače nedokázaly po roce 1999 nastavit rok 2000. Po konci roku 1999 některé počítače nastavily rok na 1900, některé

nesmyslně na 19100. CyberCoin se tak stal obětí roku 2000. CyberCoin kvůli této chybě zaznamenal spoustu dvojitých transakcí, což se projevilo následným bankrotem.

Dvojitá útrata je útok na danou kryptoměnu, v tomto případě CyberCoin. Útok spočívá ve snaze použít stejné CyberCoiny vícekrát. Tento útok se realizuje mnohem snadněji, pokud příjemce platby nepožaduje potvrzení příslušné transakce. Tento problém se standardně řešil vytvořením centrální autority. Této autoritě mohli uživatelé věřit. Nevýhodou je, že centrum se dalo napadnout hackerským útokem. Jak se ukázalo již dříve, vlády nemají pro tyto projekty pochopení a často je sabotují.

1.5.5 E-Bullion

Jedním z nejvíce tragických příběhů v souvislosti s kryptoměnami je digitální měna e-Bullion. Digitální měnu krytou zlatem založili manželé Jim a Pamela Fayedovi. Jejich digitální měna fungovala mezi roky 2001 a 2008. Za dobu existence dokázali nashromáždit 50 tisíc uncí zlata a přes 1 milion klientů. V roce 2008 se chtěla Pamela s Jimem rozvést. Jim se však nechtěl rozvést a nechal Pamelu zavraždit. Za tento čin byl následně odsouzen k trestu smrti. E-Bullion zabavila dočasně vláda. Následně byla všechna obvinění proti společnosti stažena, ale vláda se opět odvolala na „protiteroristický“ zákon. Vláda veškerý majetek zabavila a žádný z klientů své peníze nazpět nedostal (Skalický, 2018).

1.6 Nové kryptoměny

Z předchozích kapitol je zřejmé, že průběžně vznikají nové kryptoměny. Vývojáři těchto kryptoměn doufají v nárůst cen a možnosti prosazení právě jejich kryptoměny na trhu. Ovšem v začátcích nemají kryptoměny téměř žádnou hodnotu. Vývojáři se snaží zaujmout a přesvědčit investory pro investování do dané kryptoměny. Pro tyto účely se používá ICO (Initial Coin Offering), což v překladu znamená počáteční nabídka mincí. Pomocí ICO tedy lze koupit začínající kryptoměny velice snadno a především výhodně. Pokud investor dané kryptoměně důvěřuje, podpoří tím její vývoj. ICO se nepoužívá pouze pro nové kryptoměny, ale pro více projektů, které využívají technologii blockchain. Datum předprodeje nové měny a počet kusů bývá předem daný (Investplus, 2017).

Pro tradiční společnosti existuje několik možností, jak mohou získat finanční prostředky pro rozvoj podnikání. Společnost může začít s menším kapitálem a následně se rozvíjet pomocí

zisků. V tomto případě ovšem musí společnost čekat delší dobu, než se jí podaří nashromáždit dostatečný kapitál pro rozvoj. Další možností je najít investora, který bude ochoten do společnosti investovat. V tomto případě ale investoři za poskytnutí finančních zdrojů požadují část vlastnictví společnosti. Další možností je vydání akcií. ICO funguje na principu shromáždění veřejných prostředků. Společnost, která má v úmyslu vytvořit novou měnu, spustí ICO. Investoři, kteří mají zájem na koupi dané měny, nabízejí zpravidla dvě formy platby. První možností je oběžná měna a druhou možností jsou kryptoměny jako ethereum. Investoři následně doufají, že se měně bude dařit a přinese jim mimořádné zisky.

Mnoho investorů se díky ICO stalo milionáři. V roce 2018 činily celkové investice 11,4 miliardy dolarů, což je oproti roku 2017 pouze 13% nárůst, v minulých letech však byli investice mnohem vyšší (Investopedia, 2018).

1.6.1 Tržní kapitalizace

Tržní kapitalizace určuje hodnotu aktiv dané kryptoměny. Čím větší je hodnota tržní kapitalizace, tím větší je velikost dané kryptoměny na trhu. V současné době má největší tržní hodnotu bitcoin a hned za ním ethereum.

Tržní kapitalizace se počítá dle následujícího vzorce: tržní cena X cirkulující dodávka

$$\$3\,843,54 \times 17\,556\,200 = \$67\,478\,016\,921$$

V době psaní této práce byly hodnoty tržní kapitalizace, viz Obrázek 1. Tržní cena je aktuální hodnota kryptoměny na trhu. Cirkulující dodávka je počet coinů v oběhu. Hodnota kryptoměn není všude stejná. V každé směnárně i v každé zemi jsou hodnoty dané kryptoměny jiné. Je to dáno především poptávkou a nabídkou v konkrétní směnárně. Nejlepším způsobem, jak zjistit tržní hodnotu dané kryptoměny, je zprůměrovat ceny konkrétní kryptoměny v různých směnárnách.

Existuje rovněž totální tržní kapitalizace kryptoměn, která je vyjádřena jako aktuální součet hodnot všech kryptoměn na trhu, v obrázku 1 je znázorněno deset nejvýznamnějších kryptoměn. Aktuální hodnota je \$130 173 089 278. Pokud to porovnáme s tržní kapitalizací měn, můžeme si všimnout, že bitcoin na trhu dominuje a ovládá 52% trhu. Druhou měnou v pořadí je ethereum, které má na trhu podíl 11% (Cryptosvet, 2018).

Tabulka 1 – Tržní kapitalizace 10 největších kryptoměn

Jméno	Tržní hodnota	Cena
Bitcoin	\$ 193,831,099,224	\$ 10,802.72
Ethereum	\$ 32,892,466,059	\$ 308.48
XRP	\$ 19,642,086,875	\$ 0.461444
Bitcoin Cash	\$ 8,377,456,474	\$ 469.18
Litecoin	\$ 8,315,817,300	\$ 133.32
EOS	\$ 6,536,852,538	\$ 7.10
Binance Coin	\$ 5,214,366,722	\$ 36.94
Bitcoin SV	\$ 4,170,072,032	\$ 233.57
Tether	\$ 3,565,653,462	\$ 0.998537
TRON	\$ 2,546,635,623	\$ 0.038191

Zdroj: Převzato z: <https://coinmarketcap.com/> 24. 6. 2019

1.7 Vznik digitálních měn

Vznik životaschopných digitálních měn je úzce spjat s vývojem kryptografie. Není to překvapením, pokud se člověk zabývá zásadními úkoly souvisejícími s použitím bitů. Existují dvě základní

otázky pro každého, kdo přijímá digitální peníze:

1. Mohu věřit, že digitální peníze jsou věrohodné a nepadělatelné?
2. Mohu si být jistý, že nikdo jiný nemůže tvrdit, že tyto peníze patří jemu, a ne mně? (problém dvojího utrácení)

Emitenti papírových peněz se neustále potýkají s problematikou padělání pomocí stále sofistikovanějších papírů a tisku. Fyzické peníze se zabývají problematikou dvojí útraty. Konvenční peníze jsou také používány a uloženy digitálně. V těchto případech se problematika dvojího užití řeší vyčištěním všech elektronických transakcí, pomocí úředních orgánů, jež na ně dohlíží.

Digitálním penězům, které nemohou využívat bezpečnostní prvky, jako holografické proužky, poskytuje kryptografie základ důvěryhodnosti a legitimitu nároku uživatele na hodnotu. Konkrétně, kryptografické digitální podpisy umožňují uživateli podepsat digitální aktivum nebo transakci, prokazující vlastnictví daného majetku. S příslušnou architekturou mohou být digitální podpisy použity také k řešení problému dvojí útraty (Antonopoulos, 2015).

1.8 Bitcoin

Bitcoin je virtuální měna fungující od roku 2009. Vytvořil ji neznámý autor pod pseudonymem Satoshi Nakamoto. Není jisté, jestli se jedná o jednotlivce, či skupinu lidí. Někteří spekulují, že za vznik této měny může David Chaum. Bitcoin se označuje neoficiální troj symbolovou zkratkou BTC a je to nejpůlárnější kryptoměna ze všech. Je navržena tak, že ji nikdo nedokáže ovlivňovat, ani její autor Satoshi Nakamoto. Nakamoto se v dubnu 2011 stáhl a ponechal zodpovědnost za rozvoj kódu a sítě skupině dobrovolníků. Už od začátku je dáno, že bitcoinů bude pouze omezené množství.

Nakamoto vytvořil úplně nový revoluční elektronický peněžní systém. Klíčovou inovací bylo použití distribuovaného výpočetního systému nazývaného „proof-of-work“ (důkaz práce). Tento protokol každých 10 minut povolí decentralizované síti přístup k souhlasu o stavu transakce. Je to ideální řešení pro problém dvojí útraty (Antonopoulos, 2015).

1.8.1 Těžba bitcoinů

Bitcoin se získávají těžbou, která zahrnuje soutěžení při řešení matematických problémů při zpracování transakcí. Tím, že se měna těží a je decentralizovaná, odpadá potřeba vydávání nových peněz, a tudíž není potřeba ani žádný bankovní institut. Konkrétně může být vytěženo maximálně 20 999 999,9769 bitcoinů. Většina bitcoinů se má aktuálním tempem vytěžit do roku 2030. Předpokladem zůstává vytěžení maximálního počtu bitcoinů až do roku 2140. Odměny za vytěžený blok se každé 4 roky zkrátí na polovinu. Bitcoin je měna, kterou lze dělit na menší části, viz tabulka 2. (Skalický, 2018)

Tabulka 2 – dělení bitcoinu

1 BTC	1 bitcoin
0.01 BTC	1 centibitcoin
0.001 BTC	1 milibitcoin
0.000 001 BTC	1 microbitcoin
0.000 000 01 BTC	1 satoshi

Zdroj: Vlastní zpracování dle: <https://www.btc Satoshi.com/>

Bitcoinový protokol je dostupný jako otevřený software (open source). Může být použit a provozován na velkém množství výpočetní techniky, kam patří i chytré telefony. Bitcoin je distribuovaný pomocí peer-to-peer sítě, to znamená, že neexistuje žádný centrální server a tudíž se nedá síť vypnout. Převody jsou rychlé, levné a především bezpečné. Pomocí internetu lze provádět platby kdekoliv na světě na jakýkoliv účet. Bitcoin lze koupit na speciálních burzách výměnou za peníze.

1.8.2 Použití měny bitcoin

Chcete-li začít používat měnu bitcoin, je nutné si nejdříve stáhnout aplikaci nebo použít webové rozhraní. Bitcoin je standardní kryptoměna, proto existuje mnoho implementací klientského softwaru. Existuje i referenční implementace, známá jako Satoshi klient, která je řízena jako open source projekt. Řídí ji tým vývojářů a je odvozena z původní implementace napsané Nakamotem (Antonopoulos, 2015).

1.8.3 Tři hlavní formy bitcoin klientů

1. Full client – je klient, který ukládá celou historii bitových transakcí (každou transakci každým uživatelem). Spravuje peněženky uživatelů a může iniciovat transakce přímo v bitcoinové síti. Zabývá se všemi aspekty protokolu bez spoléhání na jiné servery nebo třetí strany.
2. Lightweight client – ukládá uživatelskou peněženku, ale spoléhá na servery vlastněné třetími stranami pro přístup k bitcoinovým transakcím a sítím. Klient neuloží úplnou kopii všech transakcí, a proto musí věřit třetím stranám při ověřování transakcí.
3. Web client – je zpřístupňován pomocí webového prohlížeče a uživatelskou peněženku ukládá na servery třetích stran (Antonopoulos, 2015).

1.8.4 Platba

Neexistují žádné fyzické mince. Coiny jsou obsaženy ve všech transakcích, které přenášejí hodnotu od odesílatele k příjemci. Uživatelé bitcoinové sítě tedy vlastní pouze klíče, pomocí kterých se ověřuje hodnota vlastněné měny. Tyto digitální klíče jsou často uloženy na

zařízeních jako je pevný disk, flash disk, digitální peněženka apod. V tabulce číslo 3 je znázorněn vývoj hodnoty bitcoinu.

Tabulka 3- vývoj hodnoty bitcoinu

Rok	Cena na začátku roku (USD)	Cena na konci roku (USD)
2010	0.07	0.29
2011	0.29	5.27
2012	5.27	13.40
2013	13.40	770.44
2014	770.44	313.92
2015	313.92	426.14
2016	426.14	968.23
2017	968.23	13412.44
2018	13412.44	3869.14

Zdroj: Vlastní zpracování dle: <https://www.buybitcoinworldwide.com/price/>

1.9 Ethereum

Ethereum, logo viz obrázek 1, je stejně jako bitcoin založen na blockchain technologii. Tato kryptoměna byla vytvořena v roce 2015. V roce 2016 došlo k rozdělení etherea na ethereum a ethereum classic, která má podstatně menší tržní kapitalizaci. Ethereum vytvořil ruský programátor Vitalika Buterin. Není možné ji ovlivnit a je chráněná proti podvodům. Zásadním rozdílem oproti bitcoinu je možnost využití takzvaných chytrých kontraktů.



Obrázek 1 – Ethereum logo

Zdroj: převzato z: <https://www.ethereum.org/>

1.9.1 Chytrý kontrakt

Chytrý kontrakt je blok programového kódu, který je ověřován a nelze jej zmanipulovat. Oproti bitcoinu je ethereum mladší měna a je tedy předpoklad, že je postavena na novější technologii.

Pokud má nějaká kryptoměna uspět, měla by si vzít příklad z dřívějších měn a příčin jejich neúspěchu. Díky blockchainové technologii je možné spoustě předešlých problémů předejít.

1.9.2 Výhody Etherea

Největší výhodou etherea je skvělé zabezpečení. Díky zabezpečení a také novější technologii blockchainu je technologie etherea hojně používána. Vznikla také aliance Enterprise Ethereum Alliance. Zmíněná aliance obsahuje mnoho členů, mezi které patří Hewlett Packard, Microsoft, JPMorchan Chase a jiné (Ethereum, 2019).

2 Bezpečnost kryptoměn

Kryptoměny jsou v dnešní době velice dobře zabezpečené. Největší slabinou měn je jejich volatilita. Spousta velkých investorů nechává trh z kryptoměnami nafouknout a když se kryptoměny dostanou na přijatelnou hodnotu, začnou kryptoměny prodávat.

Nejdříve se hodnota kryptoměn téměř nehýbe, velcí investoři nakupují levně kryptoměny. Kryptoměny začínají nabírat pozitivní trend. Jejich cena se začíná pomalu, ale soustavně zvyšovat. Začínají stále větší nákupy měn od nových investorů. Velkého zhodnocení si všímají média a zprávy se rychle šíří. Začínají se objevovat nové predikce růstu hodnoty. Nyní začíná nakupovat i spousta dalších nových, nezkušených investorů a začíná se tvořit finanční bublina. Cena kryptoměn je dost vysoko a velcí investoři začínají prodávat své kryptoměny. Spustí se lavinový efekt a cena začne rapidně klesat o desítky procent. Spousta nových a nezkušených investorů v tomto případě přišla o své peníze. Velcí investoři z trhu vystoupili v čas a dosahují obrovských zisků.

Toto chování trhu se pohybuje v cyklech po několika letech a stále se opakuje. Vždy, když nastane podobná situace, kryptoměny ztratí svou důvěryhodnost. Na vině jsou investoři, kteří hledí pouze na finanční stránku (Kryptomagazin, 2019).

2.1 Blockchain

Technologie blockchain je nejdůležitější pro bezpečnost kryptoměn. Blockchain je open source technologie, která je alternativou pro převod peněz. Blockchain je decentralizovaná databáze, která obsahuje informace o všech transakcích, je to vlastně neustále se rozšiřující účetní kniha. Je důvěryhodný, protože neexistuje možnost uživatelské kontroly ani centrální autority. Založen je na principu řetězce bloků, kdy jsou jednotlivé bloky skládané stále na sebe, jako řetěz. Existují dva druhy záznamů: transakce a blok. Transakce může být téměř cokoliv, ať už finanční operace, jedna zpráva nebo záznam o převodu majetku. Záznamy přidávají uživatelé, kteří používají blockchain jako účetní knihu. Oproti tomu bloky jsou potvrzující záznamy, určující, kdy a jakým způsobem byly transakce přidány do databáze. Jeden blok obsahuje libovolný počet transakcí a odkaz na předchozí blok (Antonopoulos, 2015).

Blockchain je v dnešní době pro spoustu lidí velká neznámá. Technologie blockchainu by mohla být stejně průlomová jako internet. Na počátku internetu také spousta lidí nevěřila, že může mít podobu, jakou má dnes. Blockchain je tedy stejně jako internet v počátcích nemožné pochopit a předvídat. Blockchain sice vznikl především pro bezpečnost kryptoměn, ale v současné době má tato technologie mnohem více možností a použití (Batsaikhan, 2017).

Tato technologie může pomoci při snižování nákladů podnikům. Pomocí blockchainu lze snížit náklady na ověřování a vytváření sítí pro podniky, které se zabývají mnoha transakcemi s ověřováním. Spousta z těchto transakcí může být nákladná na ověřování, přezkoumávání pověření a na auditní procesy. Blockchain všechny tyto atributy v sobě obsahuje a můžou být provedeny bez vynaložení dodatečných nákladů (Ideas, 2017).

Blockchain je univerzálním nástrojem pro použití v různých odvětvích, jako jsou finance, bankovníctví, převody peněz, mikro financování, identita a soukromí, vlastnictví, internet věcí, robotika a umělá technologie. Nicméně rozvoj blockchainu se pravděpodobně projeví až v následujících letech. V oblasti, jako jsou finance, ovšem může přijít rozvoj dříve, a to především pro zabezpečené rychlé platby. Záměrem bank je začít nabízet finanční prostředky malým a středním podnikům. (Ideas, 2017)

2.1.1 Decentralizace

Decentralizace znamená, že není žádný pevný bod nebo žádný konkrétní server, který by celou síť řídil. U kryptoměn to znamená, že daná kryptoměna funguje na desítkách tisíc počítačů a každý z těchto počítačů se podílí na provozu. V praxi to znamená, že může zkolabovat půlka počítačové sítě a přesto vše bude fungovat i nadále. Výhodou tohoto systému je, že není možné danou síť vypnout a je nezávislá na kontrolních orgánech.

Opakem této sítě je centralizovaná síť. Jako příklad může být uvedena banka, která má svou centrálu, kam se lze připojit. Zde existuje možnost, že síť bude nefunkční, pokud určitá část sítě zkolabuje. (Antonopoulos, 2015)

2.1.2 Genesis blok

V blockchainu jsou bloky vázány na sebe jako řetězec a proto nelze předchozí bloky změnit. Výjimku tvoří první blok, tzv. genesis blok. Genesis blok byl vytvořen v roce 2009. Tento

blok nemá svého předka, a tudíž je zde místo hashe 0. První blok nebylo nutné ověřovat. Je to společný předek všech bloků v blockchainu. Každý uzel v blockchainové síti začíná alespoň jedním blokem. Genesis blok je zakódován v bitcoinovém klient softwaru a nemůže být změněn. Každý uzel zná genesis blok, jeho strukturu, doby vytvoření a vždy jednu transakci uvnitř bloku. Každý uzel v blockchainové síti má tedy takzvaný bezpečný kořen, na kterém lze postavit důvěryhodný blockchain. Do počátečního bloku je možné se dopravit z kteréhokoliv místa v řetězci bloků.

2.1.3 Struktura bloku

Blok obsahuje data spojená do struktury, která jsou následně zahrnuta do veřejné knihovny. Průměrný blok obsahuje více než 500 transakcí. Hlavním identifikátorem bloku je jeho kryptografický hash a digitální otisk dat. Jako příklad je uveden první hash bloku bitcoinu, který byl kdy vytvořen:

„00000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f“.

Každý hash bloku je vypočítáván samostatně každým uzlem. Identifikace bloku probíhá také pomocí stanovení jeho polohy v bloku. To znamená, jak vysoko je ve struktuře bloku. První blok, který byl vytvořen, je ve výšce bloku 0. Blok může být tedy identifikován pomocí dvou způsobů. Za prvé, odkazem na hash bloku. Za druhé odkazem na pozici ve výšce bloku. Výška bloku však není vždy zaručena. Například se může přihodit, že více bloků bude mít stejnou výšku bloku, protože soutěží o stejnou pozici v bloku (Antonopoulos, 2015).

2.2 Generace Blockchainu

Blockchain 1.0 – Platební systémy založené na technologii blockchain. Sloužil převážně pro transakce. Digitální platební systém, který lze považovat za „Internet peněz“. Hlavním představitelem je nejznámější kryptoměna bitcoin.

Blockchain 2.0 – V druhé verzi blockchainu již přišly takzvané chytré kontrakty. Slouží pro ověřování nebo vynucování konkrétních kontraktů s automatickým prováděním. Výhodou je, že blockchain neumožňuje manipulovat tyto chytré kontrakty. Chytré kontrakty snižují náklady na ověřování. V této verzi blockchainu je nejznámější kryptoměnou ethereum.

Blockchain 3.0 – Zde je hlavním přínosem implementace standardních programovacích jazyků. Díky tomu je možné vytvářet decentralizované aplikace. Aplikace využívají decentralizované úložiště a decentralizovanou komunikaci. Jsou to běžné aplikace, které běží na blockchainové síti, a mohou využívat její výhody.

Blockchain 4.0 – V této generaci je možné implementování do průmyslu. Použitelnost je možná díky základům blockchainu z předchozích verzí. V průmyslu 4.0 je plánování podnikových zdrojů, automatizace a různé prováděcí systémčy. Toto všechno vyžaduje větší míru zabezpečení, než dříve, a právě proto je zde vhodné použití technologie blockchain. Průmysl 4.0 se také hodně spojuje s „Internetem věcí“ (IoT), což je nebezpečné právě pro přístup těchto zařízení na internet. Pomocí technologie blockchain lze vytvořit bezpečnější IoT (Medium, 2017).

2.3 Spuštění

Spuštěním sítě tvůrce Satoshi Nakamoto automaticky získal odměnu 50 bitcoinů. Tyto bitcoiny jsou úplně bezcenné, jelikož nemohou být nikdy utraceny. Spojení předchozího bloku je dosaženo prostřednictvím hashe. Hash je digitální otisk dat. Princip spočívá v převodu řetězce libovolné délky do řetězce fixní délky. Data nelze převést zpětně a nelze zjistit data vstupující před převodem. Teoreticky by se současnou technologií bylo možné data prolomit, ale nebylo by to možné v rozumném časovém intervalu. Primárním účelem je zjistit, zda se původní data a hash shodují.

Blockchain je technologie, která bude využívána nadále, i kdyby všechny kryptoměny zbankrotovaly. Technologie, na které je založena nejznámější kryptoměna bitcoin, si našla spoustu obdivovatelů. Ať už se jedná o soukromý či veřejný sektor (Antonopoulos, 2015).

2.4 Soukromí

Blockchain je výborný pro práci a zároveň je to dobrý pomocník pro udržení soukromí. Blockchain uchovává všechny veřejné informace o transakcích a zároveň anonymní informace o uživatelích. V praxi je to tak, že osobní údaje jsou zabezpečené a zároveň soukromé, díky technologii blockchainu. Pomocí této technologie mohou být uchovány

veškeré důležité informace, jako jsou právní dokumenty, rodný list, licence apod (Tapscott, 2016).

2.5 Kvantový blockchain

S popularitou blockchainu se tato síť neustále vyvíjí. Jako ochrana před kvantovými počítači je kvantová technologie, která přináší několik výhod. Jednou z nejdůležitějších schopností je poskytnout neporušitelnost informací nebo zápisu. Další jsou kvantové klíče, kde odesílatel používá kryptografický klíč, který je ovšem zakódován v kvantovém signálu.

Kvantové počítače představují do budoucna pro kryptoměny velké nebezpečí. Je to dáno především tím, že kvantový počítač by byl při těžbě bitcoinu až 17 miliardkrát efektivnější než dnešní nejvýkonnější počítače. Z tohoto důvodu některé vývojářské týmy pracují na možnosti odolnosti kryptoměn vůči těmto počítačům. První, kdo implementoval odolnost vůči těmto počítačům, byli vývojáři ze společnosti IOTA. Vlády z celého světa investují nemalé prostředky do vývoje těchto superpočítačů (Kryptomena, 2018).

2.6 Krádeže

Krádeže kryptoměn v roce 2018 vzrostly oproti předešlému roku o více než 400%. Jsou to kryptoměny, které byly ukradeny z daných burz a také od důvěřivých investorů. Hodnota odcizených kryptoměn je 38,4 miliardy Kč. Tato informace přišla od americké společnosti CipherTrace, která se zabývá bezpečností v kybernetickém prostoru. Společnost uvedla, že toto je cifra, kterou může potvrdit. Předpokladem je, že hodnota skutečně odcizených měn bude ještě vyšší (Novinky, 2019).

2.7 Kryptografie (Cryptography)

Kryptografie je matematická disciplína zabývající se šifrováním zpráv. Je založena na principu převodu originálu zprávy do šifrované podoby, kterou lze opět přechíst pomocí šifrovacího klíče. Primárním úkolem je výslednou zprávu udělat nečitelnou, pro někoho jiného, než je příjemce zprávy. Účelem kryptografie je šifrování zpráv. Tyto algoritmy následně slouží pro skrytí obsahu zprávy před všemi, kromě vysílající a přijímací strany.

Přijímací strana se musí nejdříve autentizovat a pomocí správného klíče se zobrazí správný text zprávy (Cryptoworld, 2019).

V kryptoměnách, jako je bitcoin a ethereum, je používána kryptografie založená na digitálním podpisu a tvoří základ pro jejich bezpečné ověřování transakcí. Jednou z nejpoužívanějších metod pro zabezpečení kryptoměn je kryptografie eliptických křivek.

2.7.1 Kryptografie eliptických křivek

Kryptografie na bázi eliptických křivek se anglicky nazývá Elliptic Curve Cryptography (zkratka ECC). Kryptografie na bázi eliptických křivek byla v roce 1985 nezávisle navržena Nealem Koblitzem a Victorem Saulem Millerem. Tato kryptografie představuje nejmladší přírůstek do rodiny šifrovacích systémů s veřejným klíčem. Kolem roku 2005 došlo k jejímu definitivnímu prosazení do technické praxe (Oulehla, 2017).

ECC byla vytvořena kvůli stále se zvyšujícímu výpočetnímu výkonu. Čím je délka klíče delší, tím je pro šifrování požadováno více výpočetního a paměťového výkonu. Výpočetní výkon se stále zvyšuje v návaznosti na Moorův zákon, který předpovídá, že se každé dva roky počet tranzistorů v procesoru zdvojnásobí. V návaznosti na tento zákon se neustále zvyšují délky používaných bezpečných klíčů. Jako příklad lze uvést rok 2013, kdy většina webových prohlížečů ukončila podporu 1024 bitových RSA klíčů. Nyní je minimální délka RSA klíče 2048 bitů a předpoklad je, že po roce 2030 to bude 3072 bitů. Vhodnější volbou je použití zabezpečení pomocí ECC, kdy stačí použít klíč o délce 224 bitů. Po roce 2030 bude stačit klíč o délce 256 bitů. Z předchozího textu je patrné, že délka a k tomu nutný výpočetní výkon je v podobě zabezpečení pomocí eliptických křivek vhodnějším řešením i do budoucnosti (Oulehla, 2017).

2.7.2 Úroveň zabezpečení

Úroveň zabezpečení, vyjádřená v bitech, je formalizovaný způsob, který je používán, jak pro hodnocení kryptografické „síly“ daného algoritmu, tak pro bezpečnostní porovnání algoritmů mezi sebou. Daný algoritmus má bezpečnostní úroveň n bitů, pokud nejlepší známý útok požaduje provedení 2^n kroků k jeho prolomení (jedná se o zkoušení všech n -bitových sekvencí pomocí použití hrubé síly). Úroveň zabezpečení je vždy vztažena k délce klíče dané šifry (Oulehla, 2017).

2.7.3 Šifrování

Základním prostředkem pro utajení informací je šifrování. Používá se jako prostředek pro zašifrování zpráv, které nemají být čitelné pro třetí stranu. Šifrování znamená převedení zprávy do šifrovaného textu a tento text lze následně pomocí daného klíče rozšifrovat. Vzhledem k tomu, že při šifrování je obrovský počet kombinací, je nutné znát k dešifrování zprávy klíč. Pokud klíč nebude známý, je nutné generovat všechny možné klíče pro dešifrování zprávy. Jestliže existuje dostatečně velký počet klíčů, je téměř nemožné zprávu dešifrovat. Zprávu lze dešifrovat pouze v případě, že je použit správný klíč pro dešifrování zprávy.

2.7.4 P2P (peer to peer)

Označení typu počítačových sítí, kde jednotliví klienti spolu komunikují přímo, bez konkrétního serveru. Všechny počítačové uzly jsou si rovny. Čím větší je počet uživatelů, tím větší je celková přenosová kapacita.

3 Platební možnosti a porovnání se současnými možnostmi platby

3.1 Platební možnosti

V současné době lze s kryptoměny platit na mnoho místech a jejich počet se stále zvyšuje. V kapitole 4 je mapa, která zobrazuje místa, kde všude je možné s kryptoměny platit. Pomocí kryptoměn lze zakoupit různé zboží od kávy až po byty. V České republice lze například v Paralelní Polis v Praze koupit kávu. Také se podařilo v České republice uskutečnit teprve druhou platbu za nemovitost na světě. Ruský občan sháněl byt v Praze a následně za jeho koupi zaplatil 35 bitcoiny. V tu dobu byla celková hodnota asi 5 milionů korun. Je i spousta dalších věcí, které se dají za kryptoměny pořídit, ať už to jsou auta, elektronika nebo školné na určitých školách.

3.1.1 Rozdíly v platbách

Hlavní rozdíl v možnostech platby je v tom, že současné měny jsou kontrolované centrální bankou. Oproti tomu kryptoměny nemají žádný kontrolní orgán.

Základní porovnání v následujících bodech.

Kryptoměny:

- Nemají žádný kontrolní orgán
- Platby jsou rychlé a levné
- Platby lze provádět téměř po celém světě
- Platby lze provádět i během víkendů, svátků
- Hodnota je závislá na kurzu, který je vysoce volatilní

FIAT peníze:

- Mají kontrolní orgán, jsou řízené
- Emisi nových bankovek řídí centrální banka daného státu
- Přijímané na území konkrétního státu

- Nadnárodní měny jako euro, přijímané ve všech členských zemích
- Nejsou žádné velké výkyvy hodnot
- Platby pouze během pracovního týdne.

PayPal: je internetový platební systém a prozatím celosvětově nejrozšířenější digitální peněženka. Je nejbezpečnějším způsobem pro platby na internetu po celém světě (Oulehla, 2017).

- Možnost internetových plateb
- Protistrana nemusí vědět údaje o vaší platební kartě
- Na PayPal lze nahrát peníze z platební karty a platit
- Nebo lze prostřednictvím PayPal platit a částka se rovnou strhává z karty
- Bez ověření karty je nastaven limit na 2500 Kč
- Je rychlejší než klasické posílání peněz z účtu
- Může být veden jako multi měnový účet
- Chybí čeština a česká podpora (Peníze, 2014)

Tabulka 4 - porovnání platebních nástrojů

	Přehled platebních nástrojů		
Rozdíly v platbách	Kryptoměny	FIAT peníze	PayPal
Kontrolní orgán	NE	ANO	ANO
Platby během pracovního týdne	ANO	ANO	ANO
Platby během víkendů a svátků	ANO	NE	ANO
Stabilní kurz	NE	ANO	ANO
Anonymní	ANO	NE	ANO
Celosvětové	ANO	NE	ANO

Zdroj: Vlastní zpracování

Z uvedeného přehledu je možné konstatovat, že kryptoměny mají význam pro rychlé a levné platby po celém světě. Přinášejí možnost anonymních plateb. Nevýhodou této možnosti je vysoká volatilita kurzu spojená s vysokým rizikem ztráty hodnoty.

3.2 Platba za zboží pomocí kryptoměn

Platbu za zboží pomocí kryptoměn nabízí například obchod Alza. V Alze lze platit BTC, ETH a LTC. Platba probíhá tak, že si zákazník vybere konkrétní zboží a přidá do košíku. Následně si vybere druh dopravy a zvolí možnost platby, kde lze vybrat již určitou kryptoměnu. Zákazník je přesměrován na konkrétní platební bránu. Pro BTC je to Bitcoinpay, kde zákazník provede platbu v příslušné hodnotě a Alze jsou podle příslušného kurzu připsány již Kč na její účet. Zde se zobrazí počet bitcoinů, které má zákazník zaplatit. Pokud má zákazník bitcoinovou peněženku může částku uhradit z dané peněženky lehce kliknutím na tlačítko „Uhradit z peněženky“. Pokud vše proběhne správně, platba se během pár minut ověří. V tomto případě tedy platba proběhla ihned a určená suma je připsána Alze na účet (Alza, 2019).

3.3 Směnárnny a burzy

Kryptoměny se dají pořídit na burzách nebo kryptoměnových směnárnách. Mezi nejznámější patří:

- **CoinBase**: je jednou z největších směnáren na světě. Tato americká firma nabízí možnost zakoupení kryptoměn. Poplatky za nákup jsou v rozmezí 3 - 5 %.
- **Binance**: je největší kryptoměnová burza na světě. Je zde možnost koupě stovek kryptoměn. Je vhodnější pro uživatele, kteří už nějaké zkušenosti s nákupem a prodejem kryptoměn mají.
- **CoinMate**: v současné době je jedna z nejmodernějších burz. Je zde od roku 2014. Prozatím funguje, na rozdíl od jiných, bez problémů. Jako první burza na světě přešla na nedobytnou hardwarovou peněženku bitcoin trezor. Přístup k privátním klíčům mají pouze dva zakladatelé.
- **Bitfinex**: jedna z největších kryptoměnových burz. Nabízí možnost obchodování s finanční pákou 1:3.
- **SimpleCoin**: je česká firma, která přijímá platby v Kč. Výhodou je, že není nutná registrace pro nákup měn. Stačí provést objednávku a platbu pomocí bankovního převodu. Zakoupenou měnu lze následně převést přímo do peněženky (Kryptomena, 2018).

3.3.1 Nevýhody při obchodování

Pokud chceme obchodovat s kryptoměny, přináší to i spoustu nevýhod a možných problémů. Největší nevýhodou při obchodování je nutnost nahrát danou kryptoměnu z peněženky na burzu. V tomto případě je tu riziko ztráty celé sumy nahrané ke třetím stranám, jako jsou například burzy či směnární. Pokud v dané chvíli burza zkrachuje, přijdeme o všechny prostředky nahrané na účtu. Může se také stát, že hacker prolomí zabezpečení a odcizí veškerou měnu z dané směnární. I v tomto případě hrozí riziko ztráty všech prostředků, které byly na účtu konkrétní směnární nahrané.

3.4 Zkrachovalé burzy a směnární

Existuje množství burz a směnáren, které zkrachovaly. V těchto případech přišli klienti o své vklady nebo část vkladů. V dalších kapitolách je přehled několika zkrachovalých nebo problémových burz.

3.4.1 MtGox

Burza se řadí mezi jednu z prvních burz na světě. Založil ji americký programátor Jed McCaleb v roce 2010 a následně ji prodal francouzskému developerovi Marku Karpelesovi. V době své největší slávy se přes tuto burzu obchodovalo přes 70% všech obchodů s bitcoinem. Burza byla po pár měsících hacknutá a odcizeno bylo 2000 BTC. Druhý útok přišel v roce 2014. Během tohoto útoku však bylo odcizeno 850.000 BTC s tehdejší cenou okolo 500 milionů dolarů. O měsíc déle přišla pro klienty částečně dobrá zpráva, protože se podařilo zachránit 200.000 BTC v offline úschovně. Tyto BTC byly převedeny do japonské právní úschovny (CCN, 2019).

3.4.2 QuadrigaCX

Kanadská kryptoměnová směnárna ztratila přístup ke svému offline uložení s kryptoměny. V návaznosti na tuto událost vydal web Coinmarketcap.com zprávu a zdůrazňuje důležitost zabezpečení uchování vlastních prostředků. Podle informací z představenstva společnosti se burza nachází ve finančních problémech. Tyto problémy ovlivnily funkce burzy, které využívají její uživatelé. Společnost chtěla vyřešit problémy s

likviditou a snažila se najít své významné rezervy uložené v cold wallets. Nestává se, aby burza ztratila přístup ke svým cold wallets. Ve většině případů je burza hacknutá a měna převedena (NEWSBTC, 2019).

3.4.3 Coinrail

Kryptoměnová směnárna Coinrail v Jižní Korei byla v roce 2018 hacknuta. Odcizeno bylo několik druhů kryptoměn, mezi kterými bylo i ethereum. Data z Etherscan.io ukázala, že se neznámý pachatel okamžitě snažil prodat na IDEXu, což je decentralizovaná ethereová směnárna, přes 26 milionů tokenů NPXS. Odcizeno bylo ale mnohem větší množství, přibližně 2,6 miliardy NPXS. Při útoku byly odcizeny kryptoměny za více než 40 milionů dolarů. Firma uvedla, že má 70% svých aktiv bezpečně uloženo v cold wallet. Z ukradených 30% jsou přibližně dvě třetiny zmrazeny a čeká se na výsledek vyšetřování policie (COINDESK, 2018).

3.5 Peněženka

Peněženka je nástroj pro generování adres, které slouží pro odesílání a přijímání dané kryptoměny. Každá adresa je unikátní řetězec 34 znaků. Transakce je odeslaná do sítě dané kryptoměny, kde je ověřena pomocí blockchainové technologie. Tato transakce je následně ověřena dalšími členy a provede se platba, která je nevratná. Existují dva druhy peněženek. Prvním je Hot wallet, které jsou stále připojeny k internetu. Druhou je Cold wallet, které jsou offline (Antonopoulos, 2015).

3.5.1 Hot wallet

- **NAGA WALLET:** Tato peněženka je pravděpodobně nejlepší peněženka pro uchování kryptoměn. Její nespornou výhodou je možnost jednoduchého procesu uložení a možnosti obchodování se zakoupenými kryptoměnami. Podporuje více jak 1200 kryptoměn.
- **Coinbase:** Je jednou z nejlepších peněženek na trhu. Má velmi přehledné a jednoduché rozhraní. Prostředky uživatelů v USD jsou pojištěné v plné výši. Slabou stránkou je podpora pouze 4 měn: bitcoin, ethereum, litecoin a bitcoin cash.

3.5.2 Cold wallet

- **Papírová:** Jsou vyrobené především z papíru, ale mohou být vyrobeny z jakéhokoliv materiálu, na který se dá tisknout. Na peněžence je vytištěn privátní klíč. Tyto peněženky se dají lehce vytvořit pomocí webových služeb, které jsou nabízeny bezplatně.
- **Hardwarová:** Nejdražší forma pro ukládání kryptoměn. Po stránce zabezpečení je nejlepší volbou (Kryptomagazin, 2018).

3.6 Kryptoměny z daňového pohledu

Žádná z kryptoměn není oficiálním platidlem. V České republice jsou kryptoměny dle české legislativy považovány za nehmotný movitý majetek. Česká národní banka nepovažuje kryptoměny za peněžní prostředky, elektronické peníze, cizí měnu ani cenné papíry. Právní legislativa není ještě na kryptoměny připravena a bude nějaký čas trvat, než se přizpůsobí. Je to dáno především díky rychlému vývoji kryptoměn. Protože neexistují přesné právní normy a postupy, řídí se tedy obecními právními předpisy. Avšak při kontrole může být rozdílný pohled na postup, a v těchto případech rozhoduje soud.

3.6.1 Obchod

V České republice spadají veškeré obchody na burzách pod §10 Zákon o daních z příjmů – Ostatní příjmy. Předmětem daně jsou směny kryptoměn za fiat měnu nebo jinou kryptoměnu. Postup zdanění následně záleží na tom, zda je to jednorázový, či pravidelný příjem. Nákup zboží placený kryptoměnou je také předmět daně. Pokud s kryptoměny obchoduje fyzická osoba, následně zdaňuje své příjmy jako ostatní příjmy. Pokud je to pouze jednorázová činnost, lze využít osvobození daně, ale pouze do výše příjmu 30 tisíc korun za rok. Převážná většina lidí ovšem s kryptoměny obchoduje delší dobu, proto většinou spadají do kategorie pravidelného příjmu.

Pokud někdo obchoduje pouze se svými prostředky, není třeba mít živnostenské oprávnění. Pokud ovšem spravuje finanční prostředky jiných lidí, živnostenské oprávnění je nutné.

3.6.2 Těžba

Těžení kryptoměn spadá pod poskytování služeb. V tomto případě je nutné mít živnostenské oprávnění na volnou živnost.

Problém bude s určením výdajů na dosažení, udržení a zajištění příjmu. Je to způsobeno tím, že každá kryptoměna byla nakoupena za jinou hodnotu. Zde je možnost uplatnění dvou metod výpočtu. Za prvé je to metodou FIFO, kde počítáme pořizovací cenu první kryptoměny. Druhou možností je využití váženého aritmetického průměru. Touto metodou spočítáme průměrnou cenu, za kterou jsme danou kryptoměnu nakoupili. (Eprávo, 2018)

3.6.3 DPH

Daň z přidané hodnoty se počítá mnohem jednodušeji. Je to dáno především zákonem o DPH, který je stejný pro celou Evropskou unii. U směny kryptoměn se DPH počítá kvůli provozování služby. Konkrétně je myšleno provozování služby směny za úplatou. Je zde možnost osvobození od daně, pokud činnost zařadíme jako finanční činnost. Těžba kryptoměn nepodléhá DPH. Je to dáno stanoviskem Soudního dvora EU, podle kterého musí existovat spojitost mezi poskytnutou službou a přijatou úplatou. U těžby kryptoměn je však odměna nahodilá a nepravidelná.

3.7 Kryptoměny z účetního pohledu

Stejně jako v pohledu na kryptoměny z pohledu daní, i v z pohledu účetního je zde spousta nejasností. Aktuálně je doporučeno účtování kryptoměn jako zásob. Dle vyjádření ministerstva financí by mělo docházet při snížení hodnoty kryptoměn k vytvoření opravné položky. Jedním z dalších problémů může být doložení zůstatku při účetní závěrce. Je zde několik způsobů, jak zůstatek doložit. Některé elektronické peněženky zobrazují aktuální zůstatek. Jinak je nutné doložit alespoň čestné prohlášení nebo výpis z burzy.

Cena kryptoměn se stanovuje pomocí běžné právní úpravy. Pokud tedy nakoupíme danou kryptoměnu, použije se pořizovací cena + vedlejší pořizovací náklady (Eprávo, 2018).

3.8 Výhody, rizika a trendy použití kryptoměn

3.8.1 Výhody

Jednou z hlavních výhod kryptoměn je zabezpečení plateb pomocí blockchainové technologie, které znemožňuje padělatelnost. Možnost posílání levných online plateb. Rychlost provedení platby i s ověřením. Možnost posílání kamkoliv po světě i během víkendu. Platby mohou být anonymní a přináší více anonymity při používání.

3.8.2 Rizika

Mezi největší rizika při platbě kryptoměnami patří volatilita kurzu a případná ztráta hodnoty. Hodnota kryptoměn je daná pouze kurzem na trhu a tudíž závisí na investorech. Problém může nastat v případě, pokud je špatně zadána adresa příjemce, peníze již není možné získat zpět. Oproti standardním měnám nejsou kryptoměny kryté centrální bankou. Není žádná centrální autorita, kterou jsou kryptoměny řízeny. Rizikem do budoucna může být regulace ze strany vládních a kontrolních orgánů. Platby mohou být používány pro nelegální činnosti.

3.8.3 Trendy

Možnost platby kryptoměnami u vybraných společností je způsob zvýšení příjmů a zviditelnění se. Příkladem je obchod Alza, která nabízí možnost platby již třemi kryptoměnami. Pro Alzu, která je příjemcem platby, je tato forma placení výhodná z důvodu zvýšení poptávky po nabízených produktech, pro těžaře je jednodušší zaplatit zakoupený hardware. Těžaři mohou lehce nakupovat za vytěžené měny na Alze, čímž ušetří čas, který by museli investovat do směny za peníze (Alza, 2019).

3.9 Zákazy a omezení kryptoměn

3.9.1 Čínská lidová republika

Čína plánuje na svém území zakázat těžbu kryptoměn. Čína vydala prohlášení, ve kterém vyzývá občany se k návrhu na zákaz těžby kryptoměn vyjádřit. Těžba kryptoměn by se nezastavila okamžitě, ale postupně. Pro zdejší těžaře kryptoměn by to byl velký problém, neboť v Číně je největší trh s hardwarem pro těžení. Navíc v Číně je největší počet těžařů a

proto Čína v těžbě kryptoměn dominuje, i když v roce 2017 Čína zavřela všechny lokální burzy kryptoměn. V Číně je těžba kryptoměn oblíbená pro levnou cenu elektrické energie (Novinky, 2019).

3.9.2 Ruská federace

Ruská federace nechce kryptoměny zcela zakázat, ale chce je regulovat. Dle ruského prezidenta by kryptoměny měly být mnohem více regulované a zdanitelné.

V současné době Rusko nereguluje kryptoměny jak je jeho záměrem, z toho důvodu spousta ruských programátorů začala se zakládáním svých vlastních projektů a financování pomocí ICO (Novinky, 2019).

4 Podnikatelské prostředí

Od vzniku popularity kryptoměn díky bitcoinu bylo spuštěno několik podnikatelských projektů, především za účelem zisku a nahrazením bitcoinu na vrcholu. Existují i případy, kdy společnosti a instituce chtějí lidi vzdělávat. Mezi jednu takovou instituci patří i směnárna Coinbase.

4.1 Coinbase

Zakladatelé směnárny Coinbase se rozhodli, že začnou vzdělávat lidi v oblasti kryptoměn a navíc je odmění. Rozhodnutí padlo v roce 2018, kdy se hodnota bitcoinu propadla a spousta lidí přišla o peníze. Většina lidí kupovala kryptoměny s vidinou nárůstu hodnoty a následného možného zbohatnutí. Směnárna spustila program Coinbase Earn, který slouží jako výukový portál. Směnárna zde pomocí výukových videí vysvětluje, jak jednotlivé kryptoměny fungují. Po zhlédnutí výukového videa a po správném zodpovězení kontrolních otázek, náleží účastníkům odměna. Zodpovězením otázek je zřejmé, že dané měně účastník porozuměl, a náleží mu odměna ve výši 1 \$. Takto si může uživatel vyzkoušet obchodování a navíc prohloubit své znalosti. V současné době jsou prozatím videa dostupná pouze pro kryptoměnu ZRX. Do budoucna však směnárna plánuje výuková videa pro další kryptoměny.

Zakladatelé směnárny si od tohoto kroku nejspíše slibují navýšení klientely. Navíc, pokud si uživatelé vytvoří účet, mohou začít obchodovat. Pokud se jim povede dobře obchodovat, můžou následně směnárně generovat další zisk (Zive, 2019).

4.2 Elektronické hlasování

Zabezpečené elektronické hlasování pomocí technologie blockchain u etherea.

S touto technologií lze provádět mnoho dalších administrativních operací a každodenních činností. Tyto operace lze provádět prostřednictvím internetu nebo osobně. Především je lze provádět bezpečně. Pomocí technologie etherea je možné každodenní služby zdigitalizovat pomocí chytrých kontraktů. Chytré kontrakty jsou součástí kódu blockchainu a provádí se vždy s aktualizacemi. Elektronické hlasování je dalším trendem v souvislosti s blockchain technologií. Technologie se jeví jako nejlepší pro využití při elektronickém hlasování.

Ethereová síť je nejvhodnější díky jejímu rozšířenému použití a využívání chytrých kontraktů. Bylo by možné vytvořit systém hlasování, který bude bezpečnější, levnější, transparentnější a snadno použitelný pro většinu lidí. Systém musí být bezpečný, aby nebylo možné duplicitní hlasování, a zároveň musí chránit soukromí zúčastněných osob.

Byla vyzkoušena testovací aplikace pro elektronické hlasování s použitím ethereum peněženek. Je zřejmé, že ne každý má ethereum peněženku, a proto se vyzkoušelo ještě hlasování pomocí Android platformy. Po odeslání hlasů pomocí ethereum peněženky nebo přes android se hlasy sečtou (Yavuz, 2018).

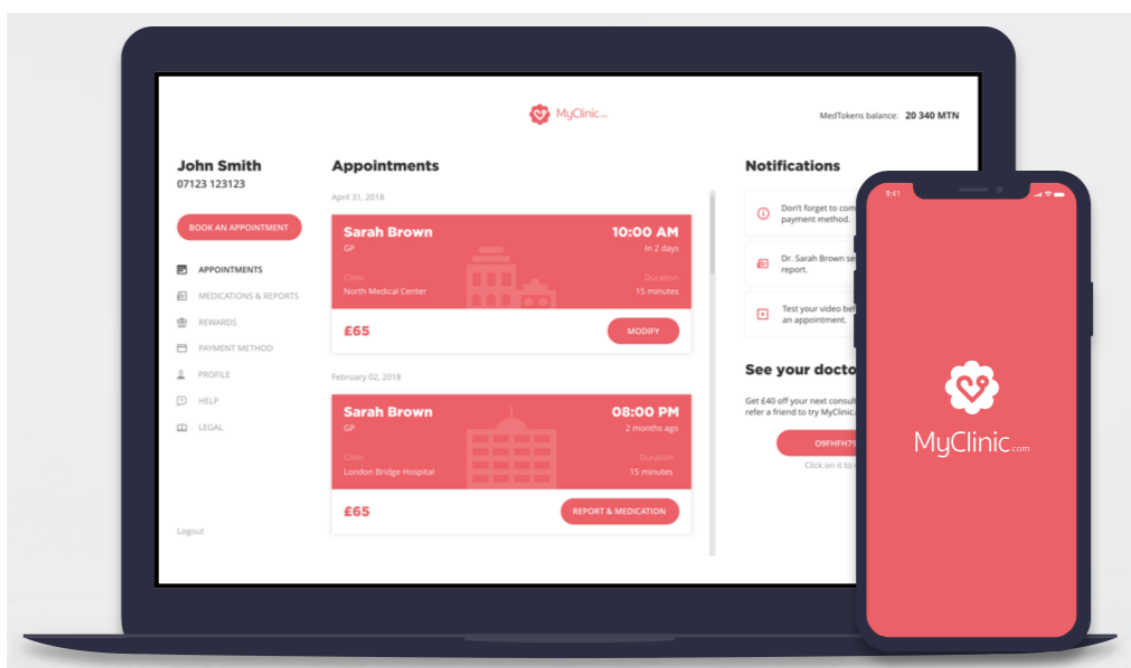
4.3 Těžba bitcoinu Čínské lidové republiky

Těžba bitcoinů znamená těžení pomocí speciálního hardwaru. Těžba kryptoměn je výhodná v zemích, kde je nízká cena elektřiny. Těžaři v Číně se spojují do velkých firem, protože následně roste jejich možnost vytěžení hodnoty dané měny. Zaměstnanci se v těchto bitcoinových dolech mohou vydělat až 13.000 Kč, což je tamější dvojnásobek minimální mzdy. Do města Ordos se stěhují těžaři virtuální měny bitcoin především kvůli levné elektřině. Na okraji města stojí jeden menší těžební pool, který v osmi přízemních budovách zaměstnává 50 lidí. Denní pracovní doba zaměstnanců je 10 hodin. Většina lidí je zde spokojena, protože práce je pro ně lehčí, než v místních firmách či na nějaké farmě. Celkem je zde umístěno 21 tisíc těžebních strojů, které jsou vybaveny speciálním hardwarem ASIC, který slouží pro efektivní těžbu kryptoměn. Zaměstnanci musí udržovat bezprašné místo, stálou teplotu pro počítačové systémy. Zaměstnanci se starají především o funkčnost všech strojů a v případě potřeby musí vyměnit vadné součásti. Musí zajistit, aby stroje pracovaly 24 hodin denně, 365 dní v roce. Město Ordos místním těžařům poskytuje 30 % slevu na elektřinu. I přesto jsou náklady na elektřinu enormně vysoké. Například námi zmíněný těžební pool denně zaplatí pouze za elektřinu 870 tisíc korun. Měsíční účet za spotřebu elektřiny je kolem 26 miliónů korun (Euro, 2017).

4.4 Medicalchain

Soukromá společnost Medicalchain využívá blockchainovou technologii pro svůj podnikatelský záměr. Používá technologii blockchain pro bezpečné uložení zdravotních záznamů pacientů. Do těchto záznamů mají přístup lékaři, nemocnice, laboratoře, pojišťovny. Mohou zažádat o povolení pro přístup k informacím daného pacienta. Výhodou tohoto použití je jedna verze lékařské složky, která bude obsahovat veškeré lékařské záznamy o pacientovi. Pacienti mají plný přístup ke svým datům. Mohou poskytnout určité úroveň přístupu ke svým záznamům pro jednotlivé organizace, či jednotlivce. Navíc pacienti mají zcela pod kontrolou, kdo a kdy přistoupil k určitým datům. Bude možné také nastavit časový přístup k vybraným datům, což zlepší zabezpečení dat. Schválené kliniky na platformě Medicalchain, viz obrázek 2, budou mít možnost číst a zapisovat do záznamů pacientů.

Do budoucna mají svůj význam také online konzultace s lékařem pomocí webové kamery. Pacienti budou moci povolit danému doktorovi přístup ke svým zdravotním záznamům, které pro něho budou relevantní, a to po dobu potřebnou k vyřešení problému (Medicalchain, 2019).



Obrázek 2 – platforma Medicalchain
Zdroj: Převzato z: <https://medicalchain.com/en/>

4.5 General Bytes

General Bytes je česká firma založena 18. září 2013. Právní forma podnikání je Společnost s ručením omezeným. Podle aktuálních údajů zaměstnává v české republice do dvaceti zaměstnanců. Společnost má sídla v Praze a na Floridě v USA. General Bytes je druhým největším výrobcem kryptoměnových bankomatů na světě. Od roku 2013 se zabývá technologií blockchainu a bitcoinu. Na světovém trhu má podíl přibližně 31%. Podle dosavadních údajů je nyní na světě více než 4100 kryptoměnových bankomatů. V České republice se nachází celkem 65 a z toho je jich 40 pouze v Praze. V současné době společnost provozuje téměř 1400 těchto kryptoměnových bankomatů, nejprodávanější viz obrázek 3.

Nejvíce kryptoměnových bankomatů se nachází v Severní Americe, kde je skoro tři čtvrtiny všech bankomatů. Nejvíce těchto bankomatů je ve Spojených státech, kde se nachází přibližně 2300 strojů. To tvoří více než polovinu všech bankomatů na světě. Na druhém místě je Kanada, kde je 620 kryptoměnových bankomatů. Na třetím místě je Rakousko s 263 bankomaty. Těsně za Rakouskem se nachází Velká Británie (Fxstreet, 2018).

Název: GENERAL BYTES s.r.o.

IČO: 02120542

Právní forma: Společnost s ručením omezeným

Adresa: U Pergamenky 1522/2, Holešovice (Praha 7), 170 00 Praha

Datum vzniku: 18. září 2013

Počet zaměstnanců: 10 - 19 zaměstnanců



Obrázek 3 – kryptoměnový bankomat General Bytes

Zdroj: Převzato z: <https://www.generalbytes.com/batmthree/>

Ceny těchto kryptoměnových bankomatů začínají se základním modelem na 7.499\$, což je při současném kurzu 171.300 Kč. Nejdražší model od společnosti stojí 9.499\$, což je při dnešním kurzu 217.000 Kč.

4.5.1 Nákup a prodej

Nákup a prodej kryptoměn není přes tyto kryptoměnové bankomaty složitý. Nákup kryptoměny přes kryptoměnový bankomat znamená vybrat příslušnou měnu, načíst peněženku, případně vygenerovat novou papírovou, vložit hotovost a nakonec potvrdit nákup. Prodej se v bankomatech od General Bytes nepatrně liší od konkurence. Rozdíl je především v tom, že ostatní bankomaty tisknou papírový platební příkaz, ale u těchto bankomatů je platební příkaz vygenerován pouze na obrazovku po dobu 200s. Během této doby je nutné načíst platební příkaz svou mobilní peněženkou a potvrdit odeslání.

Jakmile se platba potvrdí, vytiskne se číselný kód na papír pro výběr hotovosti. Příklad je aktuálně nastaven na vydávání hotovosti do 5000 Kč okamžitě. Při částkách vyšších je nutné počkat na potvrzení transakce (Kříž, 2017).

4.6 Genesis Coin

Genesis Coin je americká společnost vyrábějící BitcoMATy. Společnost má sídlo v Portoriku a její podíl na trhu je přibližně 32%. BitcoMAT se někdy nazývá též jako bitcoinový automat, ovšem toto označení je zavádějící a nepřesné. Jsou tak nazývány pro svou vnější podobu s bankomaty pro výběry hotovosti.

Jeden kryptoměnový bankomat je umístěn i v Liberci, viz obrázek 4 a to konkrétně ve Fóru v Liberci. Konkrétní model je nejlevnější, který firma nabízí a stojí 6.800\$, což je při dnešním kurzu 155.300 Kč. Nejdražší model, který firma nabízí, vyjde na 14.500\$, což je 331.000 Kč (Genesiscoin, 2019).



Obrázek 4 – kryptoměnový bankomat Genesis Coin

Zdroj: Převzato z: <https://www.bitcomat.cz/novy-bitcomat-v-liberci/>

4.7 Lamassu

Lamassu je třetím největším výrobcem kryptoměnových bankomatů na světě. Její podíl na trhu je přibližně 11%. Lamassu podporuje několik nejvýznamnějších kryptoměn. V současné době jsou to kryptoměny bitcoin, zcash, ethereum, bitcoin cash, litecoin a dash. Jeden z modelů, který firma nabízí, viz obrázek 5, je Sintra, který umožňuje nákup a prodej kryptoměn. Cena je 7.500\$, což je při dnešním kurzu přibližně 171.000 Kč (Lamassu, 2019).



Obrázek 5 - Sintra od Lamassu

Zdroj: Převzato z: <https://lamassu.is/product/sintra>

4.8 GlobalCoin od Facebooku

Facebooku se po finanční stránce daří velmi dobře, ale i tak se snaží přijít s inovacemi, které by mohly zvýšit hodnotu firmy. Navíc si společnost potřebuje upevnit důvěru více jak dvou miliardy uživatelů této sítě. Facebook proto plánuje přijít s novým kryptoměnovým systémem s označením Project Libra. Tento projekt zaštiťuje novou měnu s označením GlobalCoin. Kryptoměna je odlišná od většiny známých kryptoměn především proto, že spadá do skupiny tzv. stablecoinů. Stablecoin je token s hodnotou vázanou na zákonnou měnu, která udržuje konzistentní cenu. Stablecoin oproti běžným tokenům udržuje menší volatilitu hodnoty dané měny.

GlobalCoin je podobný jako bitcoin, avšak nebudou mít moc společného. Společné pro obě měny je použití blockchainové technologie. Jedním z rozdílů je omezený přístup. Bude se

jednat o soukromý blockchain na rozdíl od bitcoinu či etherea. Je možné, že facebook vytvoří bezpečný, efektivní a rychlý platební systém. Díky velikosti facebookové sítě může globalcoin urychlit rozšíření plateb pomocí kryptoměn. Facebook plánuje svoji kryptoměnu spustit v prvním čtvrtletí roku 2020.

Vedení Facebooku jedná s finančními i vládními institucemi z klíčových jurisdikcí o navrhovaném systému. Snaží se vyřešit regulační požadavky, které jsou požadovány.

Mark Zuckerberg pro možnost obchodovat a uschovávat globalcoin oslovil kryptosměnárnu Gemini. Provozovatelé této kryptosměnárny mají totiž bohaté zkušenosti s regulátory, což je pro Zuckerberga velmi výhodné. Navíc kryptosměnárna Gemini už má svůj vlastní stablecoin, ale prozatím se mu nedaří (Forbes, 2019).

4.9 Využití NASA

Organizace NASA uvažuje o využití blockchainu pro vytvoření chytrého autonomního hardwaru. NASA má od tohoto projektu za cíl především výrazné zrychlení komunikace. Předpokládá, že technologie bude využívána pro rychlejší zpracování dat. To může mít zásadní vliv na vesmírný program. Například při komunikaci mezi vesmírnými stanicemi a raketoplány. NASA se také snaží pomocí inženýrů propojit blockchain s umělou inteligencí. To by mohlo v budoucnu umožnit rychlejší učení strojů a vývoj umělé inteligence.

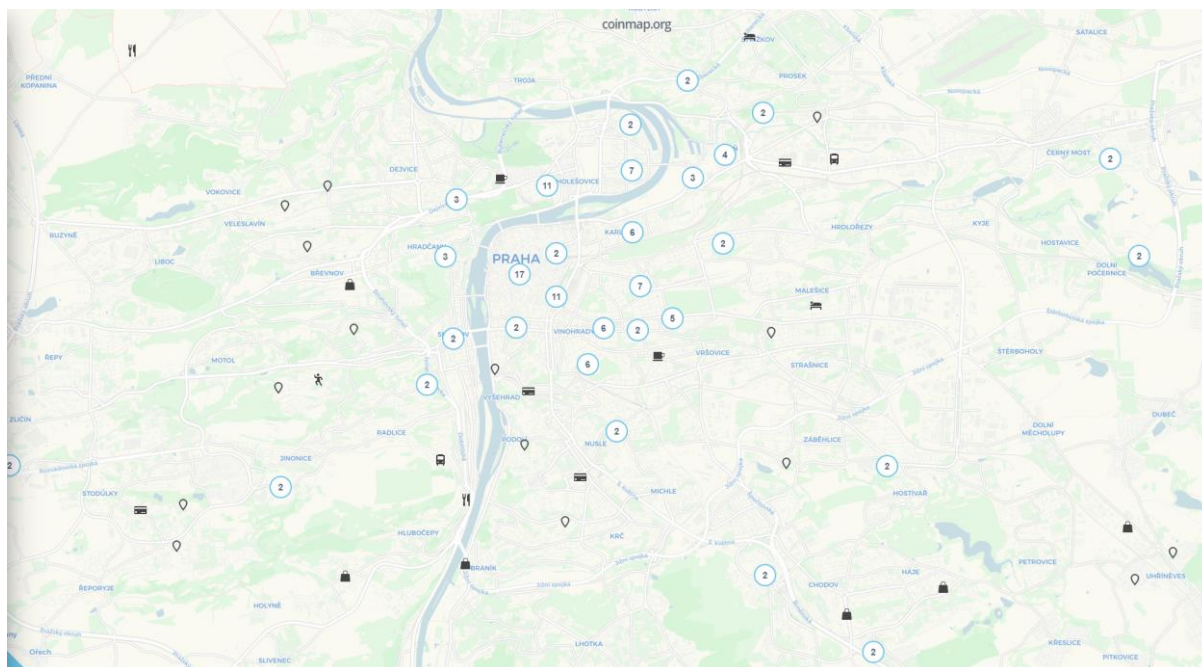
Technologii blockchain je možné dále použít pro bezpečnější a rychlejší přenosy dat. NASA uvažuje o využití chytrých kontraktů u Etherea pro použití u satelitních systémů.

5.0 Coinmap

Coinmap je internetová stránka, která zobrazuje, kde je možné platit kryptoměnami. Po přiblížení ukazuje v daném městě přesná místa a názvy obchodů a podniků, kde je možné platit.

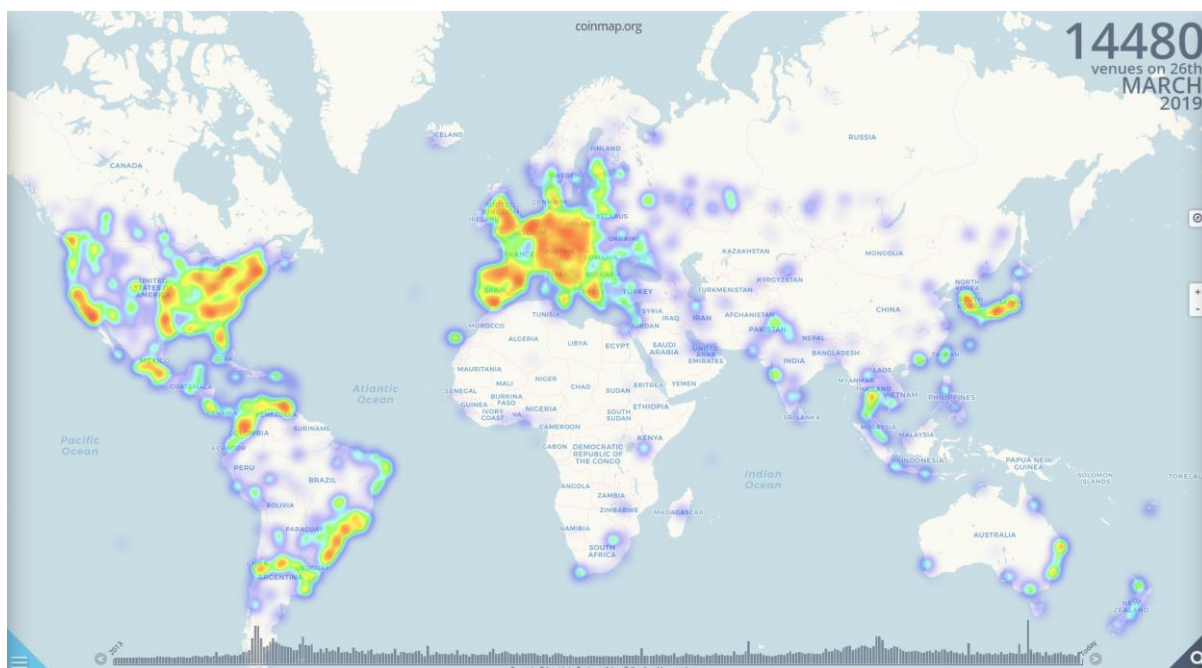
Obrázek 6 znázorňuje, kde všude je možné v Praze platit kryptoměnami. Praha byla vybrána z důvodu největšího počtu platebních možností v České republice. V Praze je okolo 170 obchodů a podniků, kde přijímají kryptoměny. Pro názornost je zde uvedeno několik příkladů:

- Prague Siesta Apartments – nabízí ubytování v centru Prahy. Přijímají platbu v BTC.
- Alza – internetový obchod, kde je možné zakoupit široké spektrum výrobků. Alza přijímá platby v BTC a LTC.
- Krypto – krypto je čerpací stanice, první svého druhu v České republice. Nabízí možnost platby za pohonné hmoty v BTC.
- Meebio – se zabývá tvorbou reklamy a tvorbou webů a e-shopů. Platby přijímá v BTC, LTC a ETH.



Obrázek 6 - platba kryptoměnami v Praze
 Zdroj: Převezato z: <https://coinmap.org>

Obrázek 7 znázorňuje možnost použití kryptoměn ve světě. Z obrázku je patrné, že k dnešnímu dni 26. březnu 2019, je možnost platby kryptoměn na 14.480 místech na světě. Největší platební možnosti jsou v Evropě a v USA (Coinmap, 2019).



Obrázek 7 – možnost platby kryptoměn ve světě
Zdroj: Převezato z: <https://coinmap.org>

5 Predikace vývoje kryptoměn jako platidla

Kryptoměny jako platidlo a technologie mají pro fungování společnosti a pro budoucnost velký potenciál. Je možné, že to nebude aktuálně nejpopulárnější kryptoměna bitcoin, ale je velký předpoklad úspěšnějšího nástupce.

S rozšířením kryptoměn a hlavně díky jejich rychle rostoucí hodnotě spousta lidí zbohatla. Bylo to především v období, kdy vzrůstala hodnota bitcoinu až na nějakých 20.000 USD. Následně se jeho hodnota propadla až na 3.000 USD. V současné době je často slyšet, že na investování do kryptoměn je pozdě. Tyto předsudky mají především lidé, kteří o kryptoměnách moc nevědí, nebo přišli kvůli pádu hodnoty o peníze. Je pravda, že se bitcoin na svém počátku prodával za halíře a udělal zhodnocení o desetitisíce procent. Většina lidí se domnívá, že bitcoin už nemá kam růst (Finex, 2019).

5.1 Kryptoměny stále na začátku

Názory na to, kam se bude vyvíjet trh s kryptoměnami, se liší. Ať už kryptoměnový trh bude mít další několikatisícové nárůsty hodnot, nebo úplný krach, vše se projeví až v následujících letech. Okolnosti kolem kryptoměn ovšem poukazují na to, že trh je stále na počátku. Dle několika predikcí je vysoká pravděpodobnost, že většina kryptoměn teprve čeká na zhodnocení. Dle CEO kryptoměnové burzy Binance se na kryptoměnách a přidružených projektech neustále pracuje a jejich využitelnost není možné zpochybnit. Jedná se o rychlé, anonymní transakce nebo nákup tokenizovaných akcií (Finex, 2019).

5.2 Rok 2017

V roce 2017 se díky obrovskému růstu kryptoměnového trhu dostaly kryptoměny do povědomí. Do kryptoměn investovala spousta lidí, aniž by věděla, jak fungují. O kryptoměnách se začalo mluvit ve velké míře v televizi, rádiu, psaly se články do novin a na internet. Díky tomu začaly vznikat firmy, které kryptoměny dostaly k obyčejným lidem. Jako příklad můžeme uvést kryptoměnové automaty. V těchto automatech mohou lidé za hotovost nakoupit kryptoměny, aniž by museli zakládat účet na nějaké burze. Navíc díky

popularitě bitcoinu vzrostly hodnoty dalších kryptoměn, mezi které patří například ethereum a litecoin.

5.3 Rok 2018

Rok 2018 byl pro kryptoměnový trh méně úspěšný. To je dáno především poklesem celkové tržní hodnoty kryptoměn. Tato situace nenastala poprvé, bitcoin již několikrát takový propad zažil. Níže je uvedeno několik příkladů:

- Zář 2010: BTC ztratil 94% své hodnoty poté, co hodnota klesla z 0.17 USD na 0.01 USD
- Listopad 2010: BTC ztratil 72 % své hodnoty poté, co hodnota klesla z 0.5 USD na 0.14 USD
- Srpen 2011: BTC ztratil 94% hodnoty poté, co hodnota klesla z 32 USD na 1.99 USD
- 2012: BTC ztratil 40% hodnoty poté, co hodnota klesla ze 7 USD na 4 USD
- 2013 a 2014 BTC ztratil 83% své hodnoty, poté co hodnota klesla z 1100 USD na 190 USD
- 2018: BTC ztratil 85% své hodnoty poté, co hodnota klesla z 20.000 USD na 3.000 USD

Z textu výše je zřejmé že, BTC již několikrát ztratil na hodnotě, ale pokaždé hodnota opět vzrostla. Dalo by se říci, že tyto výkyvy hodnot přicházejí pravidelně. Je tedy pravděpodobné, že hodnota kryptoměn opět poroste. Otázkou ovšem zůstává, kam až poroste hodnota BTC. Existují odlišné spekulace na budoucí vývoj hodnoty. Další spekulace jsou zaměřené na měny s nejvyšším potenciálem růstu (Finex, 2019).

5.4 Rychlé zbohatnutí

Mnoho investorů do kryptoměn investovalo právě v roce 2017, kdy hodnota prudce stoupla. Převážně noví investoři měli vidinu rychlého zbohatnutí, což vedlo k velkým finančním ztrátám na jejich účtech. Na kryptoměny by se však nemělo dívat pouze jako na nástroj pro

rychlé zbohatnutí, o tom kryptoměny nejsou. Pokud investoři nahlíží na kryptoměny jako na investiční nástroj, musí počítat s dlouhodobou investicí. Znásobení investic může trvat i několik let (Finex, 2019).

6 Závěr - formulace závěrů a zhodnocení

Hlavním cílem práce bylo na základě rešerše literárních zdrojů zhodnotit možnosti využití kryptoměn v podnikatelském prostředí. Dílčími cíli bylo zhodnotit bezpečnost a možnosti jejich dalšího použití mimo finanční oblasti.

Domnívám se, že se vzrůstající popularitou kryptoměn a s jejich neustále se rozšiřujícími platebními možnostmi budou s vysokou pravděpodobností kryptoměny i v budoucnu významným platebním nástrojem. Technologie, na kterých jsou kryptoměny založeny, mají pro budoucí vývoj značný potenciál, a jak naznačují předchozí kapitoly, možnosti využití v praxi jsou nezměrné.

Využití virtuálních měn je spojeno s řadou rizik. Vidina snadného zisku například přilákala v roce 2018 řadu nezkušených investorů, kteří svými neuváženými nákupy vyvolali raketový růst hodnoty bitcoin a tím nepřímou ovlivnili její nestabilitu. Následný strmý pád kurzu se negativně podepsal nejen na hodnotě bitcoinu, ale i na důvěryhodnosti všech kryptoměn. Kryptoměny se dnes opět dostávají z krize a jejich hodnota začíná pozvolna růst.

Kryptoměny pravděpodobně nikdy plně nenahradí standardní měnu jako platidlo, ale je spousta možností, kde je lze efektivně využít. Nelze na ně pohlížet pouze z hlediska finančních nástrojů, ale především jako na inovativní technologie, která je dle mého názoru převratné.

Seznam citací:

ANTONOPOULOS, Andreas M. *Mastering bitcoin*. Sebastopol: O'Reilly Media, c2015. ISBN 978-1-4493-7404-4

POPPER, Nathaniel. *Digital gold: bitcoin and the inside story of the misfits and millionaires trying to reinvent money*. New York: Harper, 2016. ISBN 978-006-2362-506

SKALICKÝ, Jan. *Bitcoin a jiné kryptopeníze budoucnosti: historie, ekonomie a technologie kryptoměn, stručná příručka pro úplné začátky*. 2., rozšířené vydání. Praha: Grada Publishing, 2018. Finance pro každého. ISBN 978-80-271-0742-1

TAPSCOTT, Alex. *Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world*. New York: Portfolio / Penguin, 2016. ISBN 978-039-9564-062

PROQUEST. Hrůza, R. (2017). ANALÝZA BITCOINU, JEHO VÝVOJ NA TRHU A STATISTICKÉ VÝPOČTY ROZIKOVOSTI A ZISKOVOSTI. *Mladá Věda*, 5(10), 9-16. Dostupné z: <https://search.proquest.com/docview/1989175514?accountid=17116>

PENÍZE. 2019. Historie peněz [online] [cit. 2019-04-13]. Dostupné z: <http://penize.org/historie-penez>.

ZIVE. 2019. Služba Coinbase Earn chce lidí vzdělávat v kryptoměnách a ještě jim za to zaplatí [online] [cit. 2019-01-01]. Dostupné z: <https://www.zive.cz/clanky/služba-coinbase-earn-chce-lidi-vzdelavat-v-kryptomenach-a-jeste-jim-za-to-zaplati/sc-3-a-196535/default.aspx> <https://www.zive.cz/clanky/služba-coinbase-earn-chce-lidi-vzdelavat-v-kryptomenach-a-jeste-jim-za-to-zaplati/sc-3-a-196535/default.aspx>.

INVESTPLUS. 2017. Novinky mezi kryptoměnami – probíhající ICOs a nejnovější zalistované kryptoměny [online] [cit. 2019-04-17]. Dostupné z: <https://investplus.cz/investice/nejnovejsi-kryptomeny/>.

NOVINKY. 2019. Krádeže kryptoměn loni vzrostly o 400 procent [online] [cit. 2019-02=01]. Dostupné z <https://www.novinky.cz/internet-a-pc/495924-kradeze-kryptomen-loni-vzrostly-o-400-procent.html>.

INVESTOPEDIA. 2018. Initial Coin Offering (ICO) [online] [cit. 2018-12-20]. Dostupné z: <https://www.investopedia.com/terms/i/initial-coin-offering-ico.asp>.

Yavuz, E., Koc, A. K., Cabuk, U. C., & Dalkilic, G. (2018). Towards secure e-voting using ethereum blockchain. Piscataway: The Institute of Electrical and Electronics Engineers, Inc. Dostupné z: <https://search.proquest.com/docview/2035266404?accountid=17116>

Seznam literatury:

MEDICALCHAIN. 2019. Medicalchain [online] [cit. 2019-13-02]. Dostupné z: <https://medicalchain.com/en/>

CRYPTOSVET. 2018. Co je tržní kapitalizace kryptoměn: Vše o market cap a jiné termíny [online] [cit. 2018-09-07]. Dostupné z: <https://cryptosvet.cz/co-je-trzni-kapitalizace-kryptomen-vse-co-potrebuje-vedet-o-market-cap/>.

CRYPTOWORLD. 2019. Základy kryptografie VI, Jaroslav Pinkava [online] [cit. 2019-02-26]. Dostupné z: www.cryptoworld.info/pinkava/uvod/bulletin6.pdf

AKTUALNE. 2018. Inflace ve Venezuele v listopadu přesáhla milion procent, zlepšení se nečeká [online] [cit. 2018-12-10]. Dostupné z: <https://zpravy.aktualne.cz/ekonomika/svetova-ekonomika/inflace-ve-venezuele-v-listopadu-presahla-milion-procent/r~53e42e3cfc9e11e898daac1f6b220ee8/?redirected=1551373596>.

OULEHLA, Milan a Roman JAŠEK. Moderní kryptografie. Praha: IFP Publishing, 2017. ISBN 978-808-7383-674.

EURO. 2017. Dobývají digitální zlato. Čínští těžaři bitcoinu vydělají dvojnásobek minimální mzdy [online] [cit. 2017-08-21]. Dostupné z: https://www.euro.cz/byznys/dobывaji-digitalni-zlato-cinsti-tezari-bitcoinu-vydela-ji-dvojnásobek-minimalni-mzdy-1366969#utm_medium=selfpromo&utm_source=euro&utm_campaign=copylinkhttps://www.euro.cz/byznys/dobывaji-digitalni-zlato-cinsti-tezari-bitcoinu-vydela-ji-dvojnásobek-minimalni-mzdy-1366969

FXSTREET. 2018. Česká firma je druhým největším výrobcem bankomatů na kryptoměny [online] [cit. 2018-12-31]. Dostupné z: <https://www.fxstreet.cz/zpravodajstvi-100671.html>.

KRIZE15. 2017. BTCmat v LIBERCI [online] [cit. 2017-07-26]. Dostupné z: <https://krize15.cz/zpravy/clanek/btcmat-v-liberci>

KRYPTOMAGAZIN. 2018. Kvantový blockchain jako finální řešení [online] [cit. 2018-05-31]. Dostupné z: <https://kryptomagazin.cz/kvantovy-blockchain-jako-finalni-reseni/>

KRYPTOMENA. 2018. Ethereum – Kurz, wallet, kde koupit [online] [cit. 2018-03-27]. Dostupné z: <https://finex.cz/kryptomena/ethereum/>

KRYPTOMAGAZIN. 2018. Víte, jaký je rozdíl mezi hot wallet a cold wallet [online] [cit. 2018-12-17]. Dostupné z: <https://kryptomagazin.cz/vite-jaky-je-rozdil-mezi-hot-wallet-a-cold-wallet/>.

EPRAVO. 2018. Kryptoměny z účetního a daňového hlediska [online] [cit. 2018-09-14]. Dostupné z: <https://www.epravo.cz/top/clanky/kryptomeny-z-ucetniho-a-danoveho-hlediska-108117.html>

LAMASSU. 2019. Lamassu Bitcoin ATMs [online] [cit. 2019-02-26]. Dostupné z: <https://lamassu.is/>

COINMAP. 2019. COINMAP [online] [2019-03-08]. Dostupné z: <https://coinmap.org>

FINEX. 2019. Velká predikce kryptoměn na rok 2019 – konec kryptoměn, nebo obří růst [online] [cit. 2019-01-24]. Dostupné z: <https://finex.cz/predikce-pro-kryptomeny-2019/>.

MEDIUM. 2017. Blockchain evolution: from 1.0 to 4.0 [online] [cit. 2017-12-07]. Dostupné z: <https://medium.com/@UnibrighIO/blockchain-evolution-from-1-0-to-4-0-3fbdccfc666>.

Batsaikhan, U. (2017). Cryptoeconomics - the opportunities and challenges of blockchain. St. Louis: Federal Reserve Bank of St. Louis. Retrieved from <https://search.proquest.com/docview/1917102969?accountid=17116>

ETHEREUM. 2019. ETHEREUM [online] [2019-02-14]. Dostupné z: <https://www.ethereum.org/>.

KRYPTOMAGAZIN. 2019. Tři důvody, proč většina lidí na kryptoměnách prodělá + řešení [online] [cit. 2019-02-24]. Dostupné z: <https://kryptomagazin.cz/tri-duvody-proc-vetsina-lidi-na-kryptomenach-prode-la-reseni/>.

ALZA. 2019. V Alze nyní zaplatíte i Bitcoin [online] [2019-03-02]. Dostupné z: <https://www.alza.cz/platba-bitcoiny-a-btc-automaty-alza>

PENÍZE. 2014. PayPal krok za krokem: Jak jednoduše platit na internetu [online] [cit. 2014-12-15]. Dostupné z: <https://www.penize.cz/nakupy/293651-paypal-krok-za-krokem-jak-jednoduse-platit-na-internetu>

NOVINKY. 2019. Příliš velké plýtvání. Čína chce zakázat těžbu bitcoinů [online] [cit. 2019-04-10]. Dostupné z: <https://www.novinky.cz/internet-a-pc/502135-prilis-velke-plytvani-cina-chce-zakazat-tezbu-bitcoinu.html>

GENESISCOIN. 2019. genesiscoin [online] [cit. 2019-02-15]. Dostupné z: <https://bitcoinatm.com/>

PENIZE. Historický vývoj peněz. Peníze.org. [online]. [cit.2018-09-14] Dostupné na internetu: <https://www.epravo.cz/top/clanky/kryptomeny-z-ucetniho-a-danoveho-hlediska-108117.html>

EPRAVO. Kryptoměny z účetního a daňového hlediska. epravo.cz. 2018. [online]. [cit.2018-09-14] Dostupné na internetu: <https://www.epravo.cz/top/clanky/kryptomeny-z-ucetniho-a-danoveho-hlediska-108117.html>

CCN. 5 Years Later, Mt. Gox Victims Still Want to Know: ‘Where’s our Bitcoin? Ccn.com 2019 [online]. [cit. 2019-02-24] <https://www.ccn.com/5-years-mt-gox-bitcoin-exchange-collapse>

NEWSBTC. Canadian Crypto Exchange Has Lost Access to its Cold Storage. newsbtc.com 2019 [online]. [cit. 2019-01-31] <https://www.newsbtc.com/2019/01/31/crypto-exchange-quadrigacx/>

COINDESK. Coinrail Exchange Hacked, Loses Possibly \$40 Million in Cryptos coindesk.com 2018 [online]. [cit. 2018-06-11] <https://www.coindesk.com/coinrail-exchange-hacked-loses-possibly-40-million-in-cryptos>

FINEX. Velká predikce kryptoměn na rok 2019 – konec kryptoměn, nebo obří růst? finex.cz 2019 [online]. [cit. 2019-01-24] <https://finex.cz/predikce-pro-kryptomeny-2019/>

IDEAS. Cryptoeconomics - the opportunities and challenges of blockchain. proquest.com 2017 [online] [cit. 2017] <https://ideas.repec.org/p/bre/polbrf/21169.html>

FORBES. Facebook chystá vlastní kryptoměnu. Tady je všechno, co o ní musíte vědět. forbes.cz. 2019 [online]. Dostupné na internetu: <https://www.forbes.cz/facebook-chysta-vlastni-kryptomenu-tady-je-vsechno-co-o-ni-musite-vedet/>