

# Perspektiva rozšíření virtuálních měn v podnikatelském prostředí v České republice

## Bakalářská práce

*Studijní program:* B6208 – Ekonomika a management

*Studijní obor:* 6208R085 – Podniková ekonomika

*Autor práce:* **Kateřina Houdová**

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



## Zadání bakalářské práce

(projektu, uměleckého díla, uměleckého výkonu)

*Jméno a příjmení:* **Kateřina Houdová**  
*Osobní číslo:* E15000143  
*Studijní program:* B6208 Ekonomika a management  
*Studijní obor:* B6208R085 – Podniková ekonomika  
*Zadávací katedra:* katedra informatiky  
*Vedoucí práce:* doc. Ing. Jan Skrbek, Dr.  
*Konzultant práce:* Martin Svoboda  
Denso Manufacturing Czech s. r. o., vývojový technolog

*Název práce:* **Perspektiva rozšíření virtuálních měn v podnikatelském prostředí v České republice**

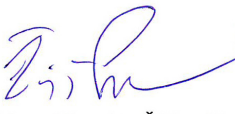
### Zásady pro vypracování:

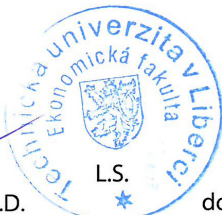
1. Stanovení cílů a formulace výzkumných otázek.
2. Literární rešerše problematiky virtuálních měn.
3. Stanovení hodnotících kritérií pro využití v podnikatelském prostředí.
4. Varianty možného vývoje a simulace jejich vlivu na podnikatelské prostředí.
5. Formulace závěrů a zhodnocení výzkumných otázek.

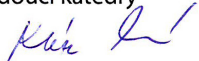
Seznam odborné literatury:

- HESSLER, Herbert. 2014. *Ekonomie bitcoinu: Analýza a modelování bitcoinu v rozvinutém stádiu*. Praha: Vysoká škola finanční a správní. ISBN 978-80-7408-104-0.
- SKALICKÝ, Jan a Dominik STROUKAL. 2015. *Bitcoin: Peníze budoucnosti*. Praha: Ludwig von Mises Institut. ISBN 978-80-87733-26-4.
- ANTONOPOULOS, Andreas M. 2015. *Mastering bitcoin*. Sebastopol: O'Reilly Media. ISBN 978-1-4493-7404-4.
- MILLER, Michael. 2015. *The ultimate guide to bitcoin*. Indianapolis: Pearson education. ISBN 978-0-7897-5324-3.
- PROQUEST. 2017. *Databáze článků ProQuest* [online]. Ann Arbor, MI, USA: ProQuest. [cit. 2017-09-28]. Dostupné z: <http://knihovna.tul.cz/>

Rozsah práce: 30 normostran  
Forma zpracování: tištěná / elektronická  
Datum zadání práce: 31. října 2017  
Datum odevzdání práce: 31. srpna 2019

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

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



V Liberci dne 31. října 2017

## Prohlášení

Byla jsem seznámena 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 vědoma 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 vypracovala 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: 11.12. 2018

Podpis: *Koudová'*

### Poděkování

Chtěla bych poděkovat doc. Ing. Janu Skrbkovi, Dr., vedoucímu mé bakalářské práce za vedení bakalářské práce, konzultace, připomínky a čas, který mi věnoval. Velký dík patří také mé rodině a přátelům, kteří mě po celou dobu studia podporovali.

## Anotace

Předmětem bakalářské práce s názvem *Perspektiva rozšíření virtuálních měn v podnikatelském prostředí* je přiblížení nejznámějších virtuálních měn a následná implementace v praxi. První část bakalářské práce je zaměřená na základní charakteristiky pěti virtuálních měn, tedy Bitcoinu, Etherea, Ripplu, Nea, Ioty, kde je obsažen koncept, platforma, způsob využití, záměry vývojářů, vlastnosti, predikce do budoucna a také problematika těchto virtuálních měn. Je zde vysvětlen základní princip Blockchainu a těžby virtuálních měn. V druhé části bakalářské práce je vyhodnocení dotazníku ohledně povědomí o virtuálních měnách, popis českého podnikatelského prostředí a možná implementace kryptoměn.

## Klíčová slova

Bitcoin, Ethereum, Ripple, Neo, Iota, Blockchain, decentralizace, peer to peer, podnikatelské prostředí v ČR, využití virtuálních měn.

### Anotation

The subject of this bachelor thesis *Perspective of cryptocurrencies in Czech business environment* is classification of best-known virtual currencies and their subsequent implementation in practice. The first part of the bachelor thesis focuses on basic characteristics of five virtual currencies, which are Bitcoin, Ethereum, Ripple, Neo, Iota. There the concept, bases, usage, developer intentions, properties, forecast for the future and issues of these cryptocurrencies are included, as well as the basic principles of Blockchain and mining of the cryptocurrencies are explained. The second part of the bachelor thesis is an evaluation of the questionnaire on the topic of awareness about cryptocurrencies, the description of the Czech business environment and the possibility of the implementation in this business environment.

### Key words

Bitcoin, Ethereum, Ripple, Neo, Iota, Blockchain, decentralization, peer to peer, business environment in the Czech Republic, use of virtual currencies.

## Obsah

<b>Seznam ilustrací</b> .....	<b>10</b>
<b>Seznam tabulek</b> .....	<b>11</b>
<b>Seznam zkratk</b> .....	<b>12</b>
<b>Úvod</b> .....	<b>13</b>
<b>1. Virtuální měny</b> .....	<b>14</b>
1.1 Historie virtuálních měn.....	14
1.1.1 Historický vývoj ceny bitcoinu.....	15
1.2 Princip současných kryptoměn.....	17
1.2.1 Blockchain.....	18
1.2.2 Mining.....	19
1.2.3 Potenciál virtuálních měn.....	20
1.3 Kryptoměny a jejich vlastnosti.....	22
1.3.1 Bitcoin.....	22
1.3.2 Ethereum.....	23
1.3.3 Ripple.....	25
1.3.4 Neo.....	26
1.3.5 Iota.....	28
1.4 Rizika virtuálních měn.....	30
1.4.1 Ohrožení výpadkem elektřiny.....	30
1.4.2 Hackerské útoky.....	32
1.4.3 Podvodné burzy a ICO.....	33
1.4.4 Limitovaná zásoba bitcoinu.....	34
<b>2. Průzkum povědomí o kryptoměnách</b> .....	<b>37</b>
<b>3. Stanovení hodnotících kritérií</b> .....	<b>42</b>
<b>4. Problematika využití kryptoměn v ČR</b> .....	<b>45</b>
4.1 Charakter českého podnikání.....	46
4.2 Informovanost veřejnosti.....	48
4.3 Nedůvěra k novým technologiím.....	49
<b>5. Simulace využití kryptoměn</b> .....	<b>50</b>
5.1 Transakce.....	50
5.2 Smart Contracty.....	51
5.3 Nefinanční využití blockchainu.....	53



5.4 Decentralizovaná aplikace.....	54
5.5 Zhodnocení.....	54
<b>Závěr .....</b>	<b>56</b>
<b>Bibliografie.....</b>	<b>58</b>
<b>Citace.....</b>	<b>59</b>

## Seznam ilustrací

Graf 1 Historický vývoj ceny bitcoinu.....	17
Obrázek 1 Grafické znázornění Blockchainu.....	19
Graf 2 Kde by si respondenti nakoupili virtuální měny.....	40
Graf 3 Decentralizovanost Bitcoinu.....	40
Graf 4 Průměrný objem obchodování za posledních 30 dní .....	44

## Seznam tabulek

Tabulka 1 Počet respondentů v dané generaci.....	38
Tabulka 2 Nejvyšší dosažené vzdělání.....	39
Tabulka 3 Stanovení hodnotících kritérií.....	42

## Seznam zkratek

AI – umělá inteligence

BTC – Jednotka Bitcoinu

DAG – Directed Acyclic Graphs

Dapp – Decentralized application

DLT – Distributed Ledger Technology – plný název technologie blockchainu

ETF – Exchange traded fund – veřejně obchodovaný fond

Fintech – Finanční technologie

ICO – Initial Coin Offering

IoT – Internet of Things

P2P – peer-to-peer decentralizovaná síť

PoP – Proof of purchase

PoS – Proof of stake

PoW – Proof of work

TPS – Transaction per secon – počet transakcí za sekundu

USD – United States Dollar – Americký dolar

# Úvod

V současné době žijeme ve světě, kde se stále vyvíjí nové technologie. Stejně tak jako by před 50 lety lidé nevěřili, že se budou používat mobilní telefony, jakožto malé krabičky s poměrně dlouhou výdrží, které budou denně využívány, jak pro osobní, tak pro podnikatelské účely. Tak v nedávné době vznikla virtuální měna nazývaná se Bitcoin a zároveň blockchain technologie, která by se v budoucnu mohla využívat v podnikatelském prostředí a ulehčovat lidem každodenní činnosti.

Cílem této bakalářské práce je analyzovat a posoudit možnosti využití virtuálních měn v podnikatelském prostředí. Dílčí cíle jsou teoretické poznání virtuálních měn a jejich technologií, vyhodnocení dotazníkového šetření, stanovení kritérií a následné vyhodnocení.

Bakalářská práce s názvem *Perspektiva využití virtuálních měn v podnikatelském prostředí* se skládá ze 2 částí, a to teoretické a praktické. Teoretická část je vytvořena na základě rešerše literatury a seznamuje čtenáře s principy a možnostmi využití vybraných virtuálních měn. V praktické části je pak popsána možná implementace kryptoměn do českého prostředí. V úvodu této části je zmíněna historie virtuálních měn. Dále je zde vysvětlen princip těžby kryptoměn. Další část se zabývá teorií a technickou specifikací pěti významných kryptoměn současnosti. Nedílnou součástí je i pohled na rizika virtuálních měn.

Praktická část má na svém počátku průzkum o povědomí o kryptoměnách a jeho vyhodnocení. Následuje problematika využití kryptoměn v českém prostředí, kde je zmíněn charakter českého podnikání, informovanost veřejnosti a nedůvěra k novým technologiím. V koncové části se nachází popis využití kryptoměn v podnikání, jako jsou transakce, smart contracty, nefinanční použití Blockchainu a použití decentralizovaných aplikací. V rámci této práce se autorka snažila odpovědět na jednu výzkumnou otázku, a to: „je Bitcoin nejvhodnější virtuální měnou pro podnikatelské prostředí?“

# 1 Virtuální měny

Virtuální měna je digitální reprezentací hodnoty, jenž nemá fyzické zastoupení, není vydávána centrální bankou nebo podobnou institucí. Tato definice zachycuje decentralizované, peer-to-peer (dále jen P2P) měny, odlišené od „internetových peněz“, jak je známe z bankovních účtů či karetních transakcí, vyjádřené ve fiat měnách.

*(ECB Legal Working Paper Series No 16, 2017, s. 11)*

## 1.1 Historie virtuálních měn

První virtuální měny začaly vznikat v době, kdy se kryptografie stala globálně rozšířenou a známou, již v 80. letech minulého století. Kryptografie řeší dvě základní otázky týkající se měn:

a) Mohu věřit, že tyto peníze jsou pravé?

b) Mohu si být jist, že si tyto peníze nebude nárokovat i někdo jiný než já?

Kryptografie tyto dva problémy řeší díky digitálním podpisům uživatele. Ten je specifický pro každého uživatele a je zaznamenán u každé jednotky virtuální měny, tudíž se virtuální měna nedá zfalšovat a není možné zpochybnit jejího majitele.

První kryptoměny byly centralizované a jejich hodnota byla podložena cennými kovy. Díky centralizovanosti těchto měn byly často útokem hackerů a vlády, důsledkem čehož se žádná z těchto měn nezachovala do současné doby.

*(Mastering Bitcoin, Anantopulos A., 2015, s. 2-3)*

Jednou z prvních digitálních měn byl například E-gold, jenž byl krytý pravým zlatem. Jeho tvůrci skončili u soudu pro padělání. Jako další je možné jmenovat měnu Liberty Dollar, založenou Bernardem von NotHouse, který chtěl vytvořit alternativu k americkému dolaru. Ta měla být na rozdíl od původní měny opět krytá drahým kovem. Bernard von NotHouse byl označen za teroristu a odsouzen za padělání peněz. Soudkyně ho tehdy obvinila z toho, že se pokusil zničit měnu své země. Důležitou virtuální měnou minulého století byl také CyberCoin, jenž pohořel na přelomu roku 1999-2000, kdy některé počítače nezvládly přechod na nové milénium a vrátily se zpět k roku 1900. To vedlo k častým dvojitým útratám CyberCoinu a znamenalo to jeho konec. O rok později vyhlásil bankrot. Digitální měny se snažili zavést také Visa a MasterCard, ale ty se ukázaly jako nefunkční. Vývojáři Bitcoinu

se z těchto neúspěchů poučili hned v několika aspektech. Virtuální měna nesmí být centralizovaná, nesmí představovat žádnou existující měnu a především musí řešit dva základní problémy každé měny, již zmíněné výše, a tedy nesmí být zfalšovatelná a nesmí být možné ji utratit dvakrát. Bitcoin toto dokázal díky přelomové technologii Blockchainu. (*Bitcoin, Peníze budoucnosti, Dominik Stroukal, Jan Skalický 2015, s.25,26,27*)

### **1.1.1 Historický vývoj ceny bitcoinu**

První bitcoiny nebylo možné směnit za žádné fiat měny, tudíž technicky měl hodnotu 0 dolarů. V roce 2010 se poprvé začaly objevovat směnné kurzy na Euro nebo Americký dolar. První cena 1 BTC byla 0,003 USD na dnes již neexistující burze BitcoinMarket.com. První zboží nakoupené za Bitcoin byla pizza na Floridě, v té době za 10 000 BTC. Ta by již o měsíc později stála přes 180 000 Kč. Dnes by vás taková pizza vyšla na neuvěřitelných 1 451 146 400 Kč. To je dobrá ukázka vývojového trendu ceny bitcoinu.

(*Bitcoin, Peníze budoucnosti, Dominik Stroukal, Jan Skalický 2015, s.36*)

Bitcoin zaznamenal první „bublinu“ již v roce 2011, kdy jeho cena spadla náhle téměř o 70 %. Z tohoto propadu se vrátil zpět na původní hodnotu až v roce 2013. Ve stejném roce došlo k dalšímu markantnímu propadu. Během 3 měsíců jeho cena vzrostla z 130 USD/BTC na konečných 1 149 USD/BTC. Z této ceny se propadl na hraničních 230 USD/BTC v roce 2015. (*Coinmarketcap.com, 2018*) K tomu značně přispěl mimo jiné také krach burzy Mt.Gox, jenž mezi rokem 2013 a 2014 držela až 70 % veškerého bitcoinu. Kolem 850 000 BTC bylo z burzy odcizeno či ztraceno. Co se přesně s coinu stalo, není známo dodnes. (*Ccn.com, 2017*)

Další velký nárůst Bitcoinu burzy zaznamenaly až koncem roku 2017, kdy se cena za jeden BTC vyšplhala téměř až k 20 000 USD. Lidé si brali hypotéky a prodávali nemovitosti, aby na poslední chvíli naskočili na rozjetý vlak. Když pak už v únoru 2018 byla cena zpět na 6 000 USD/BTC, mnoho z nich přišlo o všechno. Hodně lidí ale díky investici do Bitcoinu v tomto období zbohatlo. (*Coinmarketcap.com, 2018*) Cena bitcoinu dále klesala až do současných dnů, a to opět hlavně díky burze Mt. Gox. Aktiva, jenž po jejím krachu zbyla na burze, byla jejich poručníkem Brianem Kelly během roku 2018 postupně rozpuštěna na několika burzách, což vedlo k umělému snížení ceny bitcoinu. (*Ccn.com, 2018*) Dále byly tyto propady způsobeny vyšetřováním burzy Upbit, jejíž hlavní představitelé byli

vyšetřování pro manipulaci s kryptoměny uživatelů této burzy. To vedlo k tomu, že velké množství investorů začalo v panice prodávat své kryptoměny. Bitcoin trh na to reagoval okamžitým poklesem o 7 %. Tato událost proběhla v květnu 2018. (*Coingape.com, 2018*)

Do budoucna jsou predikce ceny bitcoinu z investorského hlediska z větší části pozitivní. Nejlepší zprávou pro Bitcoin je zavádění Exchange-traded fund (dále jen ETF), které usnadní investice do Bitcoinu investorům s největším kapitálem. Ti budou mít možnost investovat přímo na největších světových burzách. Jejich investice bude možné zabezpečit americkou SEC (US Securities and Exchange Commission), což přitáhne velké množství investorů s kapitálem v milionech dolarů.

(*Ccn.com, 2018*)

Dalším faktorem, který v budoucnu ovlivní cenu bitcoinu, bude rozhodně jeho míra využití. Ta v současné době poukazuje spíše na propad Bitcoinu. Díky velké konkurenci ze strany ostatních kryptoměn, jako je Ethereum, jenž podporuje větší množství funkcí, či Litecoin, který je mnohem rychlejší, je Bitcoin využíván čím dál tím méně. Jeho cena k datu 9.11.2018, 6500 BTC/USD, se odvíjí z ceny nákladů na vytěžení jednoho bitcoinu. Bitcoin měl potíže se z této ceny během posledních několika měsíců dostat. Predikce vývoje ceny a technické analýzy předpovídaly, že pokud se cena za jeden bitcoin nedostane přes rezistenci 6800 USD, půjde cena dolů.

(*Ccn.com, 2018*)

To se také stalo, 13.11.2018 se cena bitcoinu propadla za jeden den téměř o 1300 USD. Tento propad je připisován hardforku kryptoměny Bitcoin Cash. Vývojáři podílející se na této kryptoměně vedli spor o tom, jak by se měla měna nadále vyvíjet. Tento spor vyvrcholil až v takzvanou „Krypto občanskou válku“ nebo také „Hash wars“. Dohady, které byly 15.11.2018 urovnány rozdělením Bitcoin Cash na dva různé coiny, Bitcoin cash ABC a Bitcoin cash Satoshi Vision, způsobily velký rozruch na trhu, jenž byl už tak značně narušen. Nepřímo ovlivnily množství investorů a minerů, nehledě na negativní vliv, který měly na jméno Bitcoin cash coinu. Trh od této události nadále klesal a dostal se až na spodní hranici 3 800 USD/BTC. Tato cena je minimem od roku 2017.

(*Ccn.com*)





Graf 1 Historický vývoj ceny bitcoinu

Zdroj: coinmarketcap

V grafu je vidět historický vývoj ceny bitcoinu, na ose x je období a na ose y cena v USD, kdy v květnu 2013 je hodnota velice nízká. Na konci roku 2017, 17.12. 2017 dosáhl bitcoin svého prozatímního maxima na částce 19 353, 70 USD.

## 1.2 Princip současných kryptoměn

Princip fungování kryptoměn je založen na matematice a kryptografii. Tento systém je plně transparentní. To je zajištěno otevřenou licencí systému (open source). Funguje na principu P2P, tedy veškeré transakce jsou prováděné striktně od odesílatele k příjemci, bez potřeby prostředníka. To znamená, že celý systém je decentralizovaný. Virtuální měny jsou často považovány za velice nestabilní, nespolehlivé, s nízkou úrovní zabezpečení, nebo jsou považovány za platidlo, užívané ke kriminálním aktivitám. Faktem je, že systém blockchainu, který tyto měny využívají, je systém s nejvyšší úrovní bezpečnosti. Doposud neexistuje žádný způsob, jak ho obejít. Pocit, že virtuální měny jsou využívány ke kriminální aktivitě, je evokován hlavně faktem, že kryptoměny nejsou kontrolovány žádnou ústřední institucí, což však naopak zajišťuje nulovou zkorumpovatelnost těchto měn.

Bitcoin využívá postupů kryptografie, které jsou zdokonalené desítkami let výzkumu. Jeho blockchain technologie funguje na principech P2P, public ledger, neboli veřejná účetní kniha všech transakcí v blockchainu, distribuovaná těžba, čili řešení matematických rovnic blockchainu a decentralizované ověřování transakcí.

(*Mastering Bitcoin, Anantopulos A., 2015, s. 3*)

### 1.2.1 Blockchain

Technologie blockchainu pro kryptoměny hraje podobnou roli jako pro centrální banku její systém databází. Zajišťuje jejich zabezpečení, rychlost transakcí a decentralizovanost sítě. Technologie blockchainu byla poprvé použita již v roce 1991 a následně byla zdokonalena skupinou Satoshi Nakamoto pro reálné využití pro virtuální měny v roce 2009. Pro valnou většinu jsou finanční technologie (dále jen fintech) záležitostí konvenčního bankovníctví. Internetové či mobilní bankovníctví jsou zajisté významné oblasti využití fintech, avšak zdaleka ne jediné. Technologie jako umělá inteligence (dále jen AI) či „Big data analytics“ nutí vývoj fintech k rapidní progresi. Tyto technologie by mohly přinést obrovské změny do systému konvenčního bankovníctví. DLT (distributed ledger technology), známý též jako *blockchain* technologie, je jen jedna z mnoha fintech.

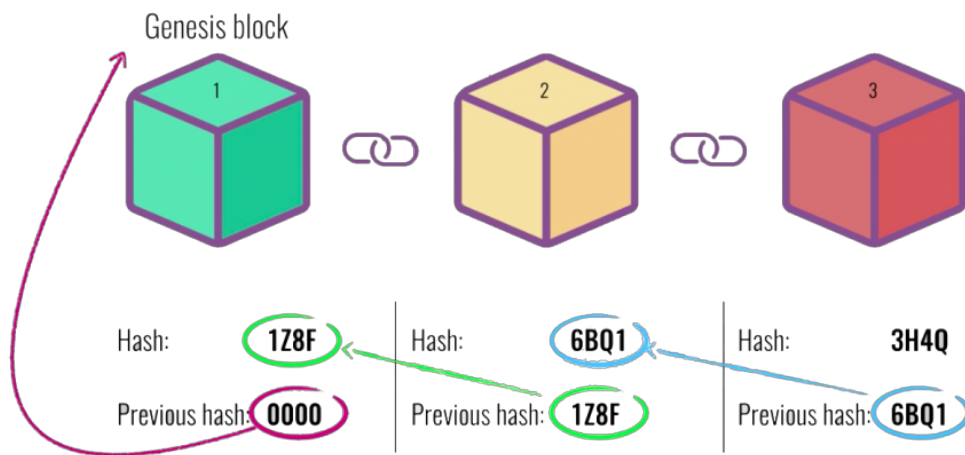
Technologie blockchainu podporuje síť databází, ve které mohou účastníci vytvářet, ukládat a prohlížet informace velice efektivním způsobem, bez nutnosti spravování této sítě centrální institucí. Využití této sítě se neomezuje pouze na virtuální měny či komodity. Tato technologie s sebou nese velký potenciál, zároveň však také mnoho právních a regulačních otázek a problémů.

Pozn: Big data analytics je pojem označující zpracování dat o velkém objemu, jenž jsou příliš komplexní pro běžné způsoby zpracování.

*(Howard Lee, Whitepaper on Distributed Ledger Technology, 2016, s.3)*

Princip blockchainu spočívá v peer-to-peer síti, kde je každý člen spojen s několika dalšími. Pokud jeden z nich vloží určitou informaci, je odeslána několika ostatním členům. Takto proces pokračuje řetězově dál, až se informace dostane ke všem účastníkům v systému. Ledger je tvořen řetězcem bloků obsahujících informace. První blok na ledgeru se nazývá „Genesis block“. Na „Genesis block“ se váže blok číslo 2, na blok číslo 2 se váže blok číslo 3. Nové bloky jsou skládány z jednotlivých transakcí. Každý z bloků obsahuje odkaz na předchozí blok v řetězci, čímž znemožňuje roztržení řetězce. Každý blok je představován vlastním specifickým identifikátorem, jenž je povětšinou reprezentován jako „hash“.

*(Whitepaper on Distributed Ledger Technology, 2016, s.18,19)*



Obrázek1 Grafické znázornění Blockchainu

Zdroj: idevji.com

Na obrázku je vidět „Genesis block“, který je první, a tedy nemůže mít hash předchozího bloku. Každý hash je unikátní a skládá se z dat vlastního obsahu, vlastního hashe a hashe předchozího bloku.

## 1.2.2 Mining

Mining, neboli těžba, je výraz popisující proces řešení matematických problémů v ledgeru. Miner je osoba, která poskytuje systému procesní výkon, jenž je potřeba k ověřování transakcí a zapisování informací do bloků. Miner sám nemůže transakci v bloku pozměnit, neboť by musel znovu vytvořit všechny následující bloky, jinak by byl jeho ledger kratší než ten aktuální a to by způsobilo odmítnutí ostatními minery. Každý miner je za úspěšně vyřešený problém v bloku odměněn, z čehož patrně pochází název celého procesu „mining“. (*Whitepaper on Distributed Ledger Technology, 2016, s.21,22*)

Transakce odeslaná uživatelem z peněženky je vyslána do tzv. „bazénu neschválených transakcí“, kde čeká, až si ji vybere miner ke schválení. Miner si vybere transakce ke schválení a zformuje je do bloku. Blok je v podstatě set transakcí, v tento moment neschválených. Miner musí schválit, zda je účet uživatele oprávněný k provedení transakce. Pokud zjistí, že jeho účet disponuje dostatečným zůstatkem, transakce je považována za platnou a může být přidána do bloku. Mineři si většinou vybírají transakce s vyššími poplatky, získávají z nich totiž vyšší odměnu.

Ke schválení každého bloku musí miner vyřešit komplexní matematický problém. K řešení tohoto problému je třeba velké množství procesního výkonu, stejně jako elektrické energie. Každý blok má jiný matematický problém, každý miner tedy řeší současně jinou matematickou rovnici. Všechny tyto problémy mají stejnou obtížnost.

Důležitým aspektem miningu je hashing. Jednoduše řečeno matematická funkce, kterou je velice těžké vyřešit, ale ověřit jeho správnost je velice jednoduché. U hash funkce jsou coby vstupní hodnota použita jakákoli data vyjádřená čísly a písmeny a její výstupní hodnotou je řetězec o 32 znacích, tvořený jinými číslicemi či písmeny. Pokud je vstupní hodnota pozměněna, výstupní hodnota se také změní. Nicméně stejná vstupní hodnota má vždy stejnou výstupní hodnotu.

Miner, jenž najde jako první řešení pro svůj blok, jej následně odešle ostatním minerům v poolu. Ti zpětně kontrolují jeho správnost (zda vstupní data souhlasí s výstupními). Odtud pochází pojmenování „proof of work“ (dále jen PoW). Miner odesílá svůj „důkaz práce“ ostatním minerům, kteří kontrolují jeho pravost. Tím je téměř nemožné na ledgeru cokoli zfalšovat. Čím více ověření transakce získá, tím těžší je pro potenciálního útočníka ji pozměnit.

Po dokončení těžby jednoho bloku se miner přesune k dalšímu, jelikož předchozí blok je již přiřazen k řetězci a tak by jeho pozměnění vedlo k odmítnutí ostatními minery.

Důležitým pojmem pro těžbu kryptoměn je Nod. V podstatě je to označení minera, ale význam tohoto pojmu je odlišný. Úlohou nodů v blockchainu je:

- 1) Ověřování platnosti bloků transakcí a jejich potvrzení či odmítnutí
- 2) Ukládání a uchovávání bloků (historie blockchainu)
- 3) Rozesílání těchto záznamů ostatním nodům, kteří se potřebují synchronizovat s blockchainem

*(Jimi S., Medium, 2018)*

### **1.2.3 Potenciál virtuálních měn**

Současný platební systém funguje dobře pro většinu transakcí, stále však trpí nedostatky, které se týkají marketingových modelů založených na důvěře. Cena transakce je navýšena o

cenu jejího zprostředkování, což limituje minimální výši transakce. Pro finanční instituce není možné dosáhnout stoprocentní nenávratnosti plateb, neboť se nemohou plně vyhnout námitkám na zprostředkování transakcí. Kvůli možné návratnosti plateb stoupá potřeba důvěry mezi stranami, což nutí obchodníky k pracnému zjišťování informací o zákaznících, které by jinak nepotřebovali (adresa, občanský průkaz pozn. aut.). Tyto problémy se dají řešit platbami v hotovosti, ale žádný mechanismus bez přítomnosti třetí strany pro jejich řešení skrze komunikační kanály neexistuje. K řešení tohoto problému je třeba systém, založený na kryptografii namísto důvěry, jenž umožňuje jakýmkoli dvěma stranám jednat přímo jedna s druhou, bez přítomnosti důvěryhodné třetí strany. Transakce, které je příliš náročné odvolat z důvodu vysokých nároků na procesní výkon, poskytnou prodejům i kupujícím vysokou míru zabezpečení. Tím zajistí spolehlivost, rychlost a efektivitu v modelech, kdy dvě strany provádí transakci po komunikačních linkách bez potřeby osobního kontaktu či třetí strany k nabytí důvěry.

*(Bitcoin Whitepaper, 2009 s.1)*

Když Satoshi Nakamoto poprvé představil světu bitcoin blockchain v roce 2009, reprezentoval zároveň dva zcela nové radikální koncepty. První z nich je Bitcoin, decentralizovaná měna, jež vyvolala rozruch v bankovníctví, finančnictví i obchodování. Jedná se o prostý přenos digitální hodnoty z účtu A na účet B. Nicméně další, neméně důležitou částí, bylo i představení konceptu blockchainu, který reprezentoval decentralizované ověřování transakcí. Ten se dá využít nejen pro přenos virtuální hodnoty peněz, ale dokáže také distribuovat velké množství informací. Tento systém má široké využití, například decentralizované směnárny, finanční deriváty, identita na blockchainu a systém reputace. Dalším, neméně důležitým způsobem využití, jsou smart contracty - systém, který automaticky přemísťuje digitální fondy na základě předem specifikovaných pravidel.

*(Ethereum Whitepaper, Vitalik Buterin, 2015, s.1)*

Současný globální systém postrádá efektivitu propojení potřebnou k uspokojení potřeb současného zákazníka. Co se týče globálního dosahu, platby jsou pomalé a velice nákladné, což zapříčiňuje to, že mnoho společností je od tohoto systému pro nedostupnost naprosto odříznuto. Tyto nedostatky pramení z absence jednotného systému pro globální platby. Nedostatek standardizace v síti se projevuje na funkcích jako přenos dat. To činí systém

nespolehlivým. Výsledkem je přechod podniků a institucí od bank k fintech poskytovatelům, kteří mohou efektivněji naplnit jejich potřeby.

*(Ripple Whitepaper, 2018, s.4)*

Vývoj Bitcoinu v uplynulých letech ukázal, že technologie blockchainu má skutečnou hodnotu v reálném světě. Nicméně tato technologie má několik nedostatků, které jí brání stát se všeobecnou platformou pro kryptoměny pro celý svět. Jedním z nich je koncept poplatku za transakci při jakékoliv výši. Potřeba mikrotransakcí bude narůstat v rapidně se rozvíjejícím IoT průmyslu (Internet of Things). Platba vyššího poplatku za transakci, než je samotná transakce, je nelogická. V systému blockchainu není jednoduché zavést bezpoplatkový systém, neboť poplatky slouží jako podnět pro tvůrce bloků. To vede k dalšímu problému blockchainu, kterým je heterogenní povaha systému. V síti jsou dva typy uživatelů: ti, kteří provádí transakce a ti, kteří je schvalují. To v určité fázi může vést k diskriminaci některých participantů. Tangle řeší tuto problematiku blockchainu díky technologii DAG, jež využívá technologii DLT bez využívání blockchain technologie.

*(Serguei Popov, Tangle Whitepaper, 2018, s 1,2)*

### **1.3 Kryptoměny a jejich vlastnosti**

Jak by se dalo čekat, stejně jako kterákoli jiná technologie prošly kryptoměny mnoha proměnami a transformacemi, než nabyly současnou formu. K dnešnímu dni je na trhu s virtuálními měnami téměř dva a půl tisíce coinů a další přibývají. *(Investing.com, 2018)* V následujícím odstavci je představeno 5 z nejprogresivnějších kryptoměn, které mají svou jistou pozici na trhu a podařilo se jim dosáhnout relativní stability na jinak velice nestabilním trhu.

#### **1.3.1 Bitcoin (BTC)**

Jakožto první z kryptoměn současnosti má Bitcoin dozajista svou výhradní pozici na trhu. Jeho výhoda spočívá v tom, že byl první. Tím však výčet jeho předností oproti ostatním měnám končí. Je pomalý, má velký problém se škálovatelností a nepodporuje zdaleka všechny způsoby využití virtuálních měn. Je koncipován jednoduše jako decentralizovaná měna s vysokou možností diversifikace. Bitcoin funguje na bitcoin blockchain, který využívá technologii PoW k řešení matematických problémů. Bitcoin se v současnosti

využívá k platbám v některých internetových obchodech. Byl akceptován některými výrobci elektroniky, ale i restauracemi, hotely či aerolinkami. V současné době je možné bitcoin zakoupit v tzv. bitcoinmatech, které jsou rozmístěny po celém světě, je možné je najít i ve větších městech v České republice. V těch je možné vytisknout papírovou peněženku, na kterou si můžete přímo z bitcoinmatu nakoupit virtuální měnu. Bitcoin je též efektivní, pokud je potřeba poslat peníze do cizí země při minimální výši poplatků. Na burzách se používá jako jeden z hlavních směnných prostředků, neboť je možné jej směnit za jakýkoliv jiný coin. Je to nejrozšířenější kryptoměna, do které investuje většina velkých investorů.

*(James Altucher, Medium, 2018)*

Výhledy Bitcoinu do budoucna jsou poměrně nejasné, využívá spíše svého současného postavení na trhu a dále se moc nerozvíjí, což autorka usuzuje z velice nízkého, spíše žádného, počtu zpráv o novinkách v Bitcoinu na serverech jako ccn.com nebo kryptomagazin.cz v období letošního roku.

Počet transakcí za sekundu (dále jen TPS), jenž je bitcoin blockchain schopný zajistit, je pouhých 7. Současný průměr jsou 3. Což je ve srovnání s 24 000 tps, které zpracovává Visa směšně nízké číslo.

*(Daniel O'Keeffe, Medium 2018)*

Problematika Bitcoinu je v tento moment zjevná. Díky téměř nulovému rozvoji bitcoin blockchainu a adaptaci nových aplikací Bitcoin pomalu ztrácí svou pozici a některé jeho funkce nahrazují coiny s lepšími vlastnostmi. Predikce hodnoty bitcoinu jsou někde mezi 0 - 1 000 000 dolarů. Není možné v současné době s jistotou říct, jak se bude vyvíjet, stejně jako je těžké předpovědět potenciál využití bitcoinu v prostředí finančnictví či podnikání.

### **1.3.2 Ethereum (ETH)**

Ethereum je vývojářská platforma podporující decentralizované aplikace. To dělá z Etherea první coin, který podporuje další vývojový stupeň virtuálních měn a rozvíjí potenciál technologie DLT. Na Ethereum je možné psát smartcontracty, jež v teorii fungují podobně jako běžné smlouvy, ovšem s tím rozdílem, že jsou plně automatizované. Není potřeba odeslání částky bankovním převodem, předání hotovosti, sdělování osobních údajů ani

účetnictví. Transakce je převedena v momentě, kdy úspěšně proběhne koupě zboží či služby. Jediné, co k tomu je potřeba, je adresa peněženky odesílatele a příjemce. Dále je také Ethereum koncipováno pro decentralizované aplikace (dále jen DApp), což v jádru znamená, že je možné na jeho platformu naprogramovat další coin, například pro účel firmy či instituce, která si díky této aplikaci může založit vlastní platidlo a dát mu specifické vlastnosti. Ethereum funguje na vlastním blockchainu, v současné době jako PoW systém, do budoucna by však mělo přecházet na PoS, který má hned několik výhod oproti originálnímu systému miningu používaným v PoW. Mezi ně patří vyšší míra decentralizovanosti, nižší nároky na energii, procesní výkon a vyšší míra zabezpečení.

*(Jack Dossman, Medium 2018)*

Ethereum v současné době není ve velké míře využíván. Existují sice kavárny či restaurace, kde je jím možné platit, ale to není primární účel, ke kterému byl jeho blockchain vytvořen. Smart contracty jsou v současné době využívány firmami jako Ether party ve Vancouveru, či Propy ve Spojených Státech.

*(Polyswarm, Medium 2018)*

Jak je zmíněno výše, do budoucna vývojáři Etherea plánují přejít na PoS (Proof-of-Stake). Tento systém nevyužívá klasického principu miningu, nýbrž ověřuje transakce v blockchainu tak, že využívá procesní výkon zařízení svých uživatelů. Jednoduše, pokud chcete odeslat transakci, musíte ověřit další dvě transakce ostatních uživatelů. To zajistí vysokou decentralizaci blockchainu a nezatíží životní prostředí při výrobě množství procesorů, které se používají k těžbě a energie potřebné k jejich provozu. Tohoto přechodu se ale patrně nedočkáme dříve než v roce 2019.

*(Aleandra H., Kryptomagazin.cz 2018)*

Momentální přenosová rychlost Etherea je 25 tps, jeho současný průměr je 15 tps. Toto číslo bude muset být několikanásobně navýšeno, než bude možné Ethereum využít v praxi.

*(Daniel O'Keeffe, Medium 2018)*

Ethereum trpí stejným problémem škálovatelnosti jako Bitcoin. Jeho TPS je o něco vyšší, ale ne nějak významně. Konstantní práce developerů na jeho rozvoji se odráží na jeho růstu, ale i tak za dobu jeho existence jeho cena klesla z 1/10 BTC na 1/33 BTC. Z toho by se mohlo dokonce zdát, že Ethereum od svého vzniku pomalu umírá, až zmizí úplně. V



testování jeho nové sítě se objevily cílené útoky minérů, kteří napadli síť a výrazně tak zpomalili testování PoS.

V horizontu dalších několika let by se Ethereum mělo držet na podobné úrovni jako doteď, možná ve vztahu k Bitcoinu bude jeho cena pomalu růst. Vše záleží na tom, jak dlouho bude trvat testování a zavádění PoS pro jeho blockchain. V každém případě potenciál využití Etherea ve světě budoucnosti je veliký.

### **1.3.3 Ripple (XRP)**

Ripple je koncipován jako síť, která poskytuje služby v oblasti mezinárodních převodů peněz a velkých transakcí. Jeho zákazníky jsou hlavně banky a finanční instituce. Tím se Ripple trochu odklání od primárního smyslu kryptoměn, jenž se povětšinou snaží bankám vyhnout. Je to však efektivní přechod mezi současným bankovním systémem a decentralizovanou technologií kryptoměn. Princip Ripple ho činí méně decentralizovaným, díky čemuž ho někteří vývojáři často vůbec neoznačují za kryptoměnu.

Ripple funguje na platformě DLT, ale nikoli na blockchainu, čímž představuje výjimku mezi ostatními virtuálními měnami.

*(Medium, Jack Dossman, 2018)*

V současné době je Ripple vyžíván několika společnostmi pro jednoduché, bezpečné a nenákladné mezinárodní převody. Kromě tohoto prvotního záměru nemá Ripple další využití. Mezi společnosti využívající Ripple patří americký finanční gigant PNC nebo bankovní společnost Santander. Podle vývojářského týmu, který stojí za rozvojem Ripple, by v roce 2019 měly Ripple net využívat desítky bank.

*(Ripplecoinnews.com 2018)*

Ripple se chlubí kapacitou až 50 000 tps. Jeho reálná hodnota se však pohybuje kolem 1 500 tps.

*(Daniel O'Keeffe, Medium 2018)*

Ripple má ve světě fintech velmi silnou propagační kampaň. Stojí za ním hned několik osobností obecně známých na kryptoscéně. Díky tomu je možné se na něj dočíst mnoho

chvály na téměř všech informačních serverech. V posledních dnech byl dokonce prohlášen za nejlepší investici pro měsíc říjen. Prognózy jeho budoucího vývoje jsou vesměs pozitivní, předpovídá se, že Ripple net by měl dosáhnout pozice jednotného systému pro globální finanční transakce. Díky zavedení bankou Santander, jež je největší evropskou bankou vzhledem k tržní kapitalizaci, bude možné Ripple net využívat ve Španělsku, Anglii, Brazílii a v Polsku. Tato společnost plánuje postupem času rozšiřovat tuto službu i do ostatních ekonomicky významných zemí.

*(Ripplecoinnews.com 2018)*

Ripple je však v kryptokomunitě vysoce kritizovaná virtuální měna. Většina vývojářů s jistotou řekne, že Ripple není kryptoměna, jeho síť není vůbec decentralizovaná a celkově absolutně maří záměr kryptoměn. Více než 50 % XRP tokenů je ve vlastnictví Ripple, stejně jako většina ověřovacích serverů, které zajišťují chod Ripple net sítě. Pokud vezmeme v úvahu všechny tyto údaje, jedná se v tomto případě spíše o globální finanční službu využívající DLT technologii než o decentralizovanou kryptoměnu.

*(Jack Dossman, Medium, 2018)*

#### **1.3.4 Neo (NEO)**

Neo je také označováno za čínské Ethereum. Je koncipováno v podstatě stejně, podporuje smart contracty, digitální identitu, decentralizované aplikace či služby jako decentralizované směnárny. Liší se jen v drobných, ale zato velice podstatných detailech, které z něho dělají velice schopného konkurenta pro Ethereum blockchain. Hlavním rozdílem je zaměření vývojářů Nea na tzv. Smart Economy. Princip tohoto konceptu spočívá v digitalizaci fyzických prostředků. Ty budou mít v blockchainu specifický průkaz vlastnictví, bude možné s nimi obchodovat v rámci smart contractů. Jejich vlastnictví může být ověřeno v decentralizovaném modelu blockchainu. Tento koncept se od Etherea nejvíce liší v tom, že je plánován jakožto systém kontrolovaný a regulovaný vládou. Tento systém tedy nebude natolik anonymní a pro registraci bude potřeba osobních údajů. *(Noam Levenson, Hackernoon.com, 2018)* Decentralizované aplikace a další služby, které Neo blockchain poskytuje, jsou využívány společnostmi po celém světě. Telekomunikační gigant KPN se podílí na decentralizaci Neo Main net. Společnost Deep brain, která se zabývá vývojem umělé inteligence, využívá Neo DApp pro svůj vlastní token. Singapurská společnost Aquit využívá Neo smart contract. Dále Neo využívají některé společnosti z herního průmyslu.

Spousta dalších společností testuje aplikace na Neo blockchain, mezi ně patří například Apex Network, New Econo Labs nebo O3 Labs.

*(Noam Levenson, Hackernoon.com, 2018)*

Neo funguje na Neo MainNet, což je jméno Neo Blockchainu. Využívá systém PoS k ověřování transakcí, to jej opět staví o krok napřed oproti Ethereumu.

*(Daniel O'Keeffe, Medium 2018)*

Vývojářský tým Nea se soustředí na zavádění Smart Economy do praxe, zatímco jeho marketingový tým uzavírá nové partnerství se zainteresovanými firmami. Neo je bezpochyby jednou z nejprogresivněji rostoucích kryptoměn na trhu. V nedávné době, na oslavu druhého výročí od založení svojí sítě MainNet, vyhlásil vývojářský tým soutěž o NEO tokeny. Tyto akce Neo podniká pro svou propagaci, úspěšně rozšiřují komunitu kolem této kryptoměny a lákají potenciální investory a partnery. Neo také nabízí široké spektrum jazyků, kterými se dají jeho aplikace programovat, na rozdíl od Ethereumu, které se totiž vyloženě zaměřuje na zavedení svého vlastního programátorského jazyka. Smart contracty a DApps je možné programovat v běžných jazycích, jako JavaScript, TypeScript, C, C++ či Python, což rozhodně hovoří ve prospěch Nea. Díky tomu jsou Neo aplikace dostupnější a partnerství s ostatními společnostmi mnohem jednodušší.

*(Neonewstoday.com, 2018)*

Přenosová rychlost Nea se pohybuje okolo 350 tps, nejvyšší zaznamenaná hodnota je však celých 2433 tps. Cílem týmu za Neo coinem je dosáhnout hodnoty 100 000 tps do konce roku 2020.

*(Daniel O'Keeffe, Medium 2018)*

Cena NEO coinu od jeho zavedení postupně klesá, podobně jako tomu bylo u Ethereumu. Jeho partnerů však stále přibývá a na jeho informačních kanálech je možné se téměř denně dočíst o nových partnerských projektech. Jeho vývoj je povětšinou předpovídán jako velký úspěch nebo úplné fiasko. Někteří lidé na kryptoscéně označují Neo za podvod a celkově je možné se na něj dočíst spoustu negativních názorů a recenzí. To je nejspíše způsobeno tím, že tým Neo se tolik nezabývá názorem veřejnosti na jejich koncept jako je tomu například u Ripple, ale soustředí se na jeho neustálý rozvoj. To je ve výsledku dobře, protože rapidní vývoj technologie je důležitější než to, jaký názor na ni má veřejnost, jež se na ní nepodílí.

Navzdory množství řečených pozitiv stojí Neo před několika fatálními problémy, které mu značně znesnadňují jeho zavádění na trh. První, a patrně největší z nich, je problematika zavádění kryptoměn v Číně. Čínská vláda v létě 2018 úplně zakázala jakékoliv aktivity spojené s finanční stránkou kryptoměn. Důvod tohoto kroku je předmětem spekulací. Možná proto se Neo v poslední době začalo soustředit spíše na nefinanční aspekt blockchainu. (*Bitcoinist.com*) Další vysoce kritizovanou vlastností Nea je jeho nízká úroveň decentralizace, a to z důvodu jednotného týmu vývojářů, jenž za ním stojí. Na rozdíl od ostatních kryptoměn, které operují na open source licenci, což umožňuje v podstatě komukoliv prohlížet a upravovat jejich zdrojový kód, je Neo spravováno vývojářským týmem zajišťujícím veškeré změny a úpravy v jeho síti. Pokud se tedy vývojářský tým Nea rozhodne celou síť zrušit, nikdo s tím nemůže nic udělat. Toto také přidává blockchainu na zmanipulovatelnosti. NeoNet může být upraven bez povšimnutí veřejnosti, tudíž je v teorii opravdu jednoduché ho zkorumpovat či zmanipulovat ve vlastní prospěch. (*Neonewstoday.com, 2018*)

### **1.3.5 Iota (IOTA)**

Iota reprezentuje kryptoměnu, která posouvá technologii blockchainu ještě o něco dál. V jejím případě se ani nedá mluvit o blockchainu, jelikož v jejím ledgeru nenajdeme žádné bloky, řetězce, a dokonce ani minery. Podobně jako v PoS sítích, každý participant musí pro schválení vlastní transakce ověřit dvě další. V oběhu je téměř 2,78 triliónů Iota a počet coinů se do budoucna nebude navyšovat jako je tomu u Bitcoinu. Díky tomu Iota nepodléhá inflaci. V síti neexistují žádní mineři, tudíž není potřeba nikoho odměňovat za řešení matematických problémů. Díky tomu je Iota vysoce škálovatelná, decentralizovaná a má nulové poplatky za transakce.

Její název obsahuje zkratku pro „Internet of Things“ neboli „internet věcí“ (dále jen IoT). Síť, na níž Iota funguje tangle, vytváří propojení inteligentních spotřebičů, ať už v domácnosti, ve firmě nebo na ulicích měst. Tyto spotřebiče jsou schopny spolu komunikovat v rámci sítě Tangle, tudíž mohou být plně automatizovány pro použití zcela bez lidské interakce.

Iota funguje na platformě tangle, neboli DAG (Directed Acyclic Graph). Je jedinou kryptoměnou využívající této technologie a byla přímo designována pro IoT.

*(The Iota Developer Hub, 2018)*

Iota je v současnosti využívána v několika případech. Společnost DXC Technology využívá Iota tangle pro zabezpečené zpracování velkého objemu dat. *(DXC.technology 2018)* Fujitsu Computers využívá technologie Proof of Concept jakožto bezpečné úložiště pro svoje sdílená data. (něco jako vylepšený iCloud pozn.aut.) *(Marrie Huilet, Cointelegraph, 2018)* Mezi další společnosti, které spolupracují s Iotou, patří Pass, společnost zabývající se hostingem, nebo australská EYEfi, jež testuje projekt Smart Drains, neboli inteligentní systém kanalizace. *(Chris Mueller, Medium, 2018)*

V Taipei jako první začali realizovat projekty inteligentních měst. Projekt TangleID zajišťuje výdej a kontrolu občanských průkazů obyvatel Taipei, čímž minimalizuje šance pro odcizení průkazů či zmanipulování volebních hlasů. Program Airbox v reálném čase poskytuje obyvatelům informace o teplotě, vlhkosti a znečištění ovzduší, jež snímá pomocí senzorů rozmístěných po celém městě. Projekt inteligentních měst dostal od Evropské Unie grant ve výši 20 miliónů Euro.

*(Datadriveninvestor.com, 2018)*

Jedním z projektů, k jejichž vzniku Iota aktivně přispívá, jsou i ekologické smart vesnice ReGen. Jedná se o projekt výstavby vesnic po celém světě, jmenovitě v Nizozemí, Německu, Velké Británii či USA, které budou produkovat svou vlastní energii a jídlo, zpracovávat svůj vlastní odpad a budou tak zcela soběstačné a šetrné k životnímu prostředí. Celá vesnice bude řízena pomocí IoT, a to od půjčovny elektromobilů, přes produkci jídla a energie, po zpracování odpadu a monitoring emisí v ovzduší. Systém IoT je nezbytný pro funkci soběstačné vesnice, protože všechny části města spolu musí neustále aktivně komunikovat, aby zajistily plynulý chod služeb a produkce ve městě. První z vesnic již roste v Nizozemí nedaleko města Amsterdam. Součástí vesnice bude i „banka“ založená na decentralizované měně. V rámci projektu ReGen je do budoucna v plánu rozšířit chytré vesnice i do míst jako je Indie či Afrika.

*(Czechcrunch.cz, 2018)*

Stejně jako o většině ostatních kryptoměn, i o Iotě můžeme říci, že do budoucna má velice široké spektrum využití. Iota se však od ostatních virtuálních měn liší v časovém horizontu, ve kterém můžeme zvážit reálné využití jejího potenciálu. Iota s její technologií tangle si klade za cíle využití v aspektech inteligentních měst a domů, automatizovaných domácích spotřebičů či počítačů. Těchto technologických vymožeností se patrně nedočkáme dříve než za deset let, pravděpodobněji pak v následujících 15 až 20 letech. V reálu bude možné Iotu využít od inteligentních domácností, přes elektromobily, které se budou schopny řídit samy a komunikovat s ostatními vozidly v dopravě, až po inteligentní města, která budou automaticky řídit provoz na svých ulicích a zamezí tak dopravním zácpám. Kromě ostatních technologií, které v současnosti ještě nejsou na úrovni, kdy by bylo možné je využít v praxi, bude k funkčnosti zmíněných konceptů potřeba také síť, která zajistí bezplatnou, rychlou a bezpečnou komunikaci jednotlivých mikročipů v autech, spotřebičích, smartphonech a dopravním značení. To je možné zajistit právě díky technologii tangle.

*(Finder.com, 2018)*

## **1.4 Rizika virtuálních měn**

Jako každá jiná technologie, i virtuální měny s sebou nesou určitá rizika. Ač nejsou tak vysoká, jako například u AI, kde je reálná hrozba, že by se umělá inteligence mohla naučit fungovat samostatně a tudíž nahradit lidstvo, stále je tu vážné riziko. Ať už co se týče zneužití k ilegálním či podvodným transakcím, hackerským útokům nebo možných mezer, které technologie blockchainu může obsahovat, jejichž následkem může konkrétní virtuální měna zcela zaniknout. V následujících několika odstavcích jsou popsána právě tato úskalí technologie virtuálních měn.

### **1.4.1 Ohrožení výpadkem elektřiny**

V případě místního výpadku elektřiny není Bitcoin ani jiná měna fungující na technologii blockchainu markantně ohrožena. Může sice dojít k poklesu procesního výkonu v síti nebo určitým neshodám v ledgeru různých minerů, ale žádný větší problém to nezpůsobí. Co opravdu ohrožuje technologii blockchainu, je absolutní black out, tedy moment, kdy elektřina vypadne na celém světě. V takový moment jednotlivé nody (mineři) v síti ztratí kontakt jeden s druhým, takže nebudou schopni kontrolovat bloky přidané ostatními minery do blockchainu. V ten moment je možné přidat do ledgeru blok obsahující smyšlené či

zfalšované transakce a nikdo nebude schopný je zkontrolovat. Ani v tento moment však není možné učinit transakci z cizího účtu, jelikož k tomu je potřebný privátní klíč uživatele. Jediným rizikem tak je dvojitá útrata nabytých coinů.

Schopnost blockchainu vzpamatovat se z celosvětového výpadku proudu značně závisí na délce trvání tohoto výpadku. V momentě, kdy se proud navrátí do sítě, podle technické specifikace v DLT whitepaperu, bude za platný ledger považován ten, jenž bude potvrzen 51 % nodů nebo více. V případě, že takový ledger nebude nalezen, tzn. že v síti bude příliš mnoho rozdílných ledgerů způsobených rozdílnými transakcemi různých nodů, povede to k zániku blockchainu. Takový systém už je prakticky nemožné uvést zpět do původního stavu. Ověřit, které transakce jsou platné a které falešné, je v tento moment nemožné.

V případě trvání výpadku v rozmezí několika minut až hodin se dá očekávat, že se v blockchainu po opětovném zapnutí proudu najde alespoň 51 % shodných ledgerů. V případě, že výpadek potrvá dva a více dní, dá se očekávat, že se příliš mnoho uživatelů pokusí odeslat transakce, jež budou ověřeny pouze lokálně, a tak se jejich ledgery budou lišit.

Další eventualitou v případě výpadku proudu je možný pokus o využití této situace ve prospěch nadpoloviční většiny nodů v síti. Pokud by se mineři v síti, kteří ovládají více než 51 % procesního výkonu v síti, dohodli a pozměnili ledger ve svůj prospěch, například přenesli velké množství kryptoměny na své vlastní účty či spálili určitý počet mincí, nikdo by nebyl schopný tomuto podvodu zamezit. Jelikož blockchain se vždy odvíjí od údaje, který je rozhodnut nadpoloviční většinou, podvodné transakce by byly považovány za platné. Nutno dodat, že tento scénář, ač je plně reálný a možný, je velice nepravděpodobný. První tři mining pooly pro Bitcoin jsou AntPool, BTC.com, a BTC.TOP. Ty dohromady potvrzují až 47,5 % všech bloků v síti. (*Investopedia.com, 2018*) Ani kdyby se tyto tři pooly spojily, nebyly by schopny změnit ledger ve svůj prospěch. Takový útok by vyžadoval vysokou míru organizovanosti. Je však pravdou, že dopad takové akce by byl dozajista fatální. Pravděpodobnější eventualita je však ta, kdy by se několik minerů v síti pokusilo nezávisle na sobě pozměnit ledger ve svůj prospěch, což by vedlo k absolutní desynchronizaci blockchainu a následně k jeho zániku.

Sám blockchain však představuje řešení pro zdokonalení zabezpečení elektrické sítě proti výpadkům, a to díky technologii IoT, která je na něm postavena. Zavedením této technologie

do elektrické sítě je možné zajistit komunikaci jednotkových sloupů vysokého napětí či trafostanic. Vadný sloup by byl v takovém případě sám schopný informovat centrálu o závadě a přivolat údržbářskou jednotku, zatímco by svou funkci převedl na nejbližší funkční sloup a odvedl tak napětí do jiné, funkční části obvodu.

*(Fortune.com, 2018)*

### **1.4.2 Hackerské útoky**

Pokud nepočítáme útoky namířené přímo proti burzám, směnárnám či počítačům jednotlivých uživatelů, které se ve skutečnosti netýkají blockchainu, jediný způsob, jak napadnout DLT, je takzvaný „útok 51 %“. Při tomto útoku se hacker může buď pokusit utratit své coinsy dvakrát nebo narušit důvěryhodnost blockchainu a pokusit se tak sabotovat určitou kryptoměnu. V obou případech útok vypadá stejně.

Aby hacker úspěšně uskutečnil útok, musí své coinsy za něco utratit, např. za luxusní auto. Za účelem dvojité útraty těchto coinů musí vytvořit alternativní verzi blockchainu, která prozatím bude existovat pouze pro něj a nebude sdílena s ostatními nody v síti. Hacker učiní transakci na první verzi blockchainu, kde zakoupí auto, a to mu bude odesláno na jeho adresu. Mezitím vytvoří verzi blockchainu, ve které tuto transakci zvrátí, tudíž podle ní jeho coinsy nikdy neopustí jeho účet. Ostatní mineři v síti tuto verzi nemohou zaznamenat, neboť hacker ji nesdílí veřejně. Miner, jenž se snaží zmanipulovat blockchain, v tento moment stále těží bloky a potvrzuje transakce v síti a připisuje je na svou verzi blockchainu. Aby mohl svůj blockchain učinit veřejně platným, musí tak činit rychleji než zbytek sítě, k čemuž potřebuje alespoň 51 % celkového procesního výkonu v síti, proto název „útok 51%“. Po obdržení zásilky svého luxusního auta hacker odešle svou verzi blockchainu do sítě, přičemž ostatní mineři ji podle blockchain protokolu budou nuceni akceptovat, jelikož bude delší než ověřená verze blockchainu. Tato verze je nyní považována za pravou a všechny transakce, jež neobsahuje, budou okamžitě navráceny. Přestože útočník utratil své coinsy za luxusní auto, je teď schopen je utratit znovu.

Realizace takového útoku by byla velice složitá, jelikož procesní výkon v bitcoin blockchainu představuje stovky tisíc minerů. Útočník by musel utratit enormní částku, aby byl schopen vyvinout nadpoloviční většinu procesního výkonu, tudíž vytvořit delší blockchain nežli zbytek sítě. Dalšími problémy pro takovýto útok jsou náklady na pronájem



prostor pro tolik procesorů, náklady na elektrickou energii a praní získaných peněz. Takovýto útok zkrátka stojí příliš mnoho úsilí na to, aby se ho vyplatilo realizovat.

Existují případy, kdy byl 51% útok skutečně realizován. Jeden z nich proběhl v dubnu roku 2018 na blockchainu kryptoměny XVG, tedy virtuální měna Verge. V tomto případě se útočníkům podařilo najít chybu v kódu blockchain protokolu, kterou využili k extrémně rychlé tvorbě bloků, jež jim umožnila vytvořit delší řetězec ve velmi krátkém časovém úseku. Tento případ dokazuje, že ačkoliv jsou útoky velice málo časté, jsou možné. Terčem takových útoků jsou většinou malé blockchainya, především z důvodu menšího celkového procesního výkonu v síti. Spolehlivý tým vývojářů by podobnou chybu v kódu brzy odhalil a odstranil. Na bitcoin blockchainu takovýto útok nebyl nikdy v minulosti zaznamenán.

Nejlepším způsobem, jak tomuto druhu útoku zabránit, je co největší počet malých minerů v síti, raději než několik málo poolů, které ovládají většinu blockchainu. Vyšší decentralizace těžby v síti zajišťuje vyšší bezpečnost blockchainu.

*(Jimi S., Good Audience, Medium.com 2018)*

### **1.4.3 Podvodné burzy a ICO**

Když člověk vstupuje na trh s virtuálními měnami jako úplný nováček, je velice jednoduché stát se obětí podvodníků. Mnoho lidí se snaží obohatit nečestnými způsoby a fakt, že virtuální měny zatím nepodléhají žádné regulaci zákonem, jim hraje do karet.

Initial Coin offering (dále jen ICO) je název pro společnost, která nabízí ke koupi své vlastní tokeny výměnou za Bitcoin či jinou kryptoměnu. Tyto investované měny pak nadále investují dle vlastního uvážení a svým investorům nabízí určitou část profitu. Ten je udělován ve formě vlastních tokenů dané společnosti. Ty buď narůstají na hodnotě nebo jsou jejich majiteli připisovány dividendy. Tento systém představuje výhodnou investici s poměrně vysokou a rychlou návratností. Má však hned několik rizik, která jsou v podstatě nevyhnutelná. Prvním z nich je šance, že investice ICO společnosti nevyjdou, ta zbankrotuje a utratí všechny peníze svých investorů. V takovém případě osoby, jež zakoupily tokeny u ICO, nemají žádnou možnost odvolání ani kompenzace za své ztracené peníze. Také se může stát, že majitel ICO investované peníze ukradne a zmizí. V takovém případě opět neexistuje žádné odvolání. Známým případem takového podvodu je platforma Falcon Coin,

jejíž majitel zmizel s několika milióny dolarů a nechal odpovědnost za zmizelé investice na svých manažerech a vývojářích.

*(Investopedia.com, 2018)*

Několikrát v historii obchodu s virtuálními měnami se stalo, že z účtů uživatelů se ztratilo určité množství kryptoměny. Některé účty se staly obětmi tzv. phishingu, někdy se jednalo o hackerské útoky přímo na burzy. Některé případy nebyly nikdy objasněny. V březnu roku 2018 byl zaznamenán phishingový útok na burzu Binance, kdy byly bez vědomí majitelů účtů odeslány kryptoměny v hodnotě několika set tisíc dolarů. Tento útok byl včas zachycen a všechny odeslané transakce byly navráceny na účty právoplatných majitelů. Jednalo se o útok, kdy hackeři rozesílali na adresy uživatelů Binance.com podvodné emaily s odkazem na falešnou stránku burzy. Tam se uživatelů dotázali na jejich přihlašovací údaje, které byly následně odeslány přímo hackerům. *(Support.binance.com, 2018)*

Nejznámějším a největším útokem na burzu s virtuálními měnami je společnost MtGox, jež v roce 2014 zbankrotovala. Útočník údajně postupně převáděl bitcoin z účtů uživatelů bez povšimnutí. Tento útok nebyl nikdy zcela vysvětlen a uživatelé burzy se dočkali minimálního, spíše žádného odškodnění za ztrátu svých coinů.

*(Ccn.com, 2018)*

Na internetu je také možné setkat se s velkým množstvím podvodných podnikatelů, nabízejících zboží, jež není běžně dostupné. Za účelem ochrany své totožnosti vyžadují platbu bitcoinem. Po odeslání platby však většina těchto podvodníků zmizí a slibované zboží zákazník nikdy neuvidí. Tyto podvody se nedají regulovat jinak než informováním uživatelů o podvodných podnikatelích, neboť transakce Bitcoinu se nedají vystopovat, tudíž identita pachatelů zůstává neznámá.

#### **1.4.4 Limitovaná zásoba bitcoinu**

Tento aspekt Bitcoinu je jeho velkou výhodou, ale zároveň jedním z jeho největších problémů. Díky limitované zásobě bitcoinu měna nepodléhá inflaci, na rozdíl od fiat měn. Ty jsou vydávány centrální bankou podle potřeby daného státu a teoreticky je možné jich natisknout nekonečné množství. V takovém případě však měna ztrácí hodnotu díky zvyšujícímu se objemu peněz v oběhu.

Bitcoin tento problém řeší tak, že od svého zavedení na trh má limitovanou zásobu, kterou nemůže přesáhnout, protože mu to nedovolí jeho zdrojový kód. Momentální objem Bitcoinu v oběhu je 17 357 387 BTC. Jeho maximální zásoba, které je možné dosáhnout je 21 000 000 BTC. (*Coinmarketcap.com, 2018*) Tato částka by teoreticky měla být dosažena v roce 2140. Díky tomuto faktu je cena bitcoinu vždy vázána na jeho reálnou hodnotu, která díky inflaci fiat měn průběžně stoupá, jak jsme mohli v dlouhodobém časovém měřítku vidět před koncem roku 2017.

Vytěžené bitcoiny však slouží jako odměna pro minery, kteří zajišťují chod blockchainu, tudíž bez nich fungování Bitcoinu není možné. Se současným počtem transakcí, v průměru 10,074 za 24 hodin, není možné pokrýt náklady na těžbu z poplatků za transakce. Mineři jsou tudíž placeni pouze z vytěžených bitcoinů. Odměna za vytěžení bloku se periodicky snižuje, vždy na polovinu své hodnoty. Momentální odměna za úspěšně vyřešený blok transakcí je 12,5 BTC. Tato cifra se bude v roce 2020 půlit na 6,25 BTC. Tedy přibližně každých 10-12 minut, což je doba nutná pro uvolnění bloku transakcí, bude mezi všechny minery v síti rozdělena 6,25 BTC. Z toho plyne, že odměna za vytěžený blok bude daleko nižší než náklady na jeho vytěžení. Jedinou šancí Bitcoinu, jak se dostat přes tento problém, je eventualita, že jeho cena ještě před rokem 2020 rapidně stoupne, jinak nebude motivace pro minery dostatečná k tomu, aby pokračovali v těžbě. Jelikož u Bitcoinu nebyl zaznamenán úmysl přechodu na PoS, který tento problém řeší, je to jeho jediná šance k zachování.

Pokud by se negativní prognózy nenaplnily a Bitcoin by přežil půlení odměny za blok v roce 2020, jeho největším problémem do budoucna bude, jak pokrýt náklady minérů, až bude dosažena jeho maximální zásoba. Jediným způsobem, jak v daný moment bude bitcoin blockchain schopný odměňovat minery za tvorbu bloků, budou poplatky za transakce. Jelikož většina procesního výkonu v síti je momentálně využívána k řešení uměle vytvořených problémů z důvodu nízkého počtu transakcí, není částka vybraná na poplatcích ani zdaleka dostačující k pokrytí odměn pro minery. Tento problém má dvě řešení, z nichž alespoň jedno bude nutné pro zachování funkčního bitcoin blockchainu. Těmi jsou za první signifikantní zvýšení poplatků za transakce a za druhé signifikantní zvýšení počtu transakcí. To v praxi znamená, že Bitcoin musí začít být reálně využíván k platbám a pravidelným transakcím, a to dlouho před rokem 2140. Všechny bitcoiny, jež jsou momentálně drženy na účtech velkých investorů, kteří je nechtějí prodat předtím, než cena bitcoinu dosáhne

maxima, budou muset být uvolněny a pravidelně používány. Tím se opět dostáváme k faktu, že cena bitcoinu bude muset být několikanásobně navýšena, a to nejen pro jeho běžné používání, ale hlavně pro zachování jeho blockchainu. V opačném případě se může stát, že bude následovat osud svého sesterského projektu Bitecoin, jenž skončil právě z těchto důvodů.

*(99bitcoins.com, 2018)*

## 2 Průzkum povědomí o kryptoměnách

V rámci bakalářské práce autorka vytvořila dotazník zjišťující povědomí o virtuálních měnách, kterého se zúčastnilo 137 respondentů. Ti odpovídali na otázky ohledně virtuálních měn. Dotazník byl rozdělen do 4 částí, první část se věnovala základním informacím o respondentovi, následovaly 3 sekce otázek. Sekce 1 se týkala obecných otázek o virtuálních měnách, na kterou navazovala sekce 2. Třetí sekce byla zaměřena na Bitcoin.

- Pohlaví

Muž

Žena

- Věk

do 20 let

21-35 let

36-50 let

51-72 let

- Nejvyšší dosažené vzdělání

Základní (ZŠ)

Středoškolské bez maturity (SOU)

Středoškolské s maturitou (SŠ)

Vysokoškolské (VŠ)

### Sekce 1

1. Setkal/(a) jste se někdy s pojmem virtuální měna nebo pojmem kryptoměna?  
(Dokázal/(a) byste nějakou vyjmenovat?)
2. Kolik existuje kryptoměn?
3. Odkud jste informován/(a)?

### Sekce 2

1. Dokázal/(a) byste si virtuální měnu obstarat? Kde?
2. Vlastníte virtuální měnu?
3. Kde se dá virtuálními měnami platit?
4. Myslíte si, že se nějaká z virtuálních měn stane běžným platidlem?
5. Myslíte si, že virtuální měny zcela nahradí současné měny?
6. Myslíte si, že lze virtuální měny zcizit?

7. Myslíte si, že virtuální měny mohou usnadňovat kriminální činnost?

### Sekce 3 - Informovanost o Bitcoinu

1. Kdy Bitcoin vznikl?
2. Kdo je tvůrcem Bitcoinu?
3. Jaký je aktuální kurz bitcoinu vůči dolaru?
4. Je bitcoinů omezené množství?
5. Je Bitcoin spravován některou z centrálních bank?
6. Víte, jak se Bitcoin těží?
7. Víte, co je to blockchain?

Dotazníku se zúčastnilo 137 respondentů, z toho 59 mužů a 78 žen na území České republiky. Pro dotazníkové šetření autorka vybrala určité skupiny respondentů. Hlavní skupinou byli manažeři středního a vyššího managementu, kteří denně ovlivňují a rozhodují o chodu podniků. Další skupinou byli studenti gymnázia. Ze získaných informací lze předpokládat, že by tímto způsobem odpovídalo větší množství lidí v dané věkové kategorii a se stejným stupněm vzdělání.

Věkové skupiny byly rozděleny dle generací, tedy generace Z ve věku do 20 let, generace Y v rozmezí 21 až 35 let, generace X v rozmezí 36 až 50 let a generace Baby Boomers ve věkovém rozmezí 51 až 72 let. Skupinu manažerů zde představuje generace Y, X a Baby Boomers s dokončeným vysokoškolským vzděláním či středoškolským s maturitou a generaci Z zde představují studenti gymnázia s dokončenou základní školou.

**Tabulka 1 Počet respondentů v dané generaci**

Generace	Počet respondentů
Z	21
Y	82
X	27
Baby Boomers	7

*Zdroj: vlastní tvorba*

Poslední část hlavičky dotazníku se týkala nejvyššího dosaženého vzdělání, přičemž 19 respondentů mělo základní vzdělání, 7 respondentů středoškolské bez maturity, 59 dotazovaných mělo dokončené středoškolské vzdělání s maturitou a 52 respondentů mělo vysokoškolské vzdělání.

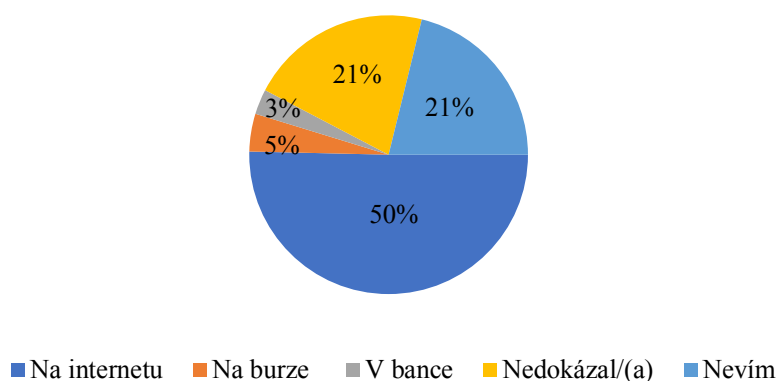
**Tabulka 2 Nejvyšší dosažené vzdělání**

Nejvyšší dosažené vzdělání	Počet respondentů
Základní	19
Středoškolské bez maturity	7
Středoškolské s maturitou	59
Vysokoškolské	52

*Zdroj: vlastní tvorba*

Na první otázku odpovědělo 117 respondentů, že se někdy s pojmem virtuální měna či kryptoměna setkalo, dalších 20 respondentů se s tímto pojmem nikdy neseťkalo. V porovnání s bakalářskou prací z roku 2017 autora Ladislava Lásky se s tímto pojmem setkalo o 20 % více lidí, což autorka vyhodnotila v rámci dotazníkových šetření, můžeme tedy říci, že se tento pojem rozšířil. Následující otázka se týkala pořízení virtuální měny. 69 respondentů by si virtuální měny pořídilo přes internet, což činí 50 %, 29 respondentů by si virtuální měnu nedokázalo pořídit, dalších 29 respondentů by nevědělo, jak virtuální měnu pořídit, 6 dotazovaných by nakoupilo virtuální měnu na burze a pouze 4 respondenti by si šli virtuální měnu pořídit do banky, což činí právě 3 %.

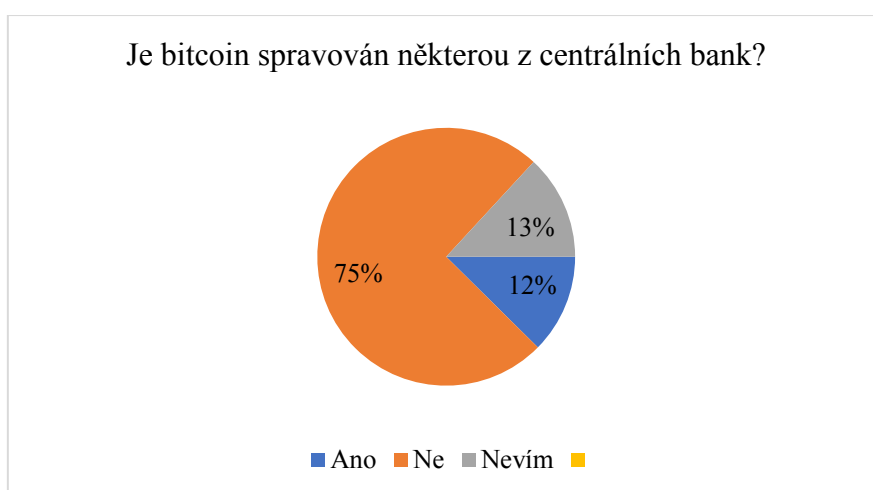
Dokázal/(a) byste si pořídit virtuální měnu? Kde?



Graf 2 Kde by si respondenti nakoupili virtuální měny

Zdroj: vlastní tvorba

91 dotazovaných, tedy 66 % si myslí, že virtuální měny mohou usnadňovat kriminální činnost, 34 respondentů odpovědělo, že virtuální měny neusnadňují kriminální činnost a 12 respondentů nevědělo. Dále by autorka ráda zmínila odpovědi respondentů týkající se decentralizace, jelikož 17 respondentů odpovědělo, že Bitcoin je spravován centrální bankou, dokonce zmínili Českou národní banku. Tedy 12 % respondentů si myslí, že Bitcoin je měna centralizovaná. 102 dotazovaných však vědělo, že tato měna centrálně řízená není a zbylých 18 respondentů nevědělo.



Graf 3 Decentralizovanost Bitcoinu

Zdroj: vlastní tvorba



Při vyhodnocování autorka zjistila, že žádná žena z dotazovaných nevlastní virtuální měnu a ani se o virtuální měny nijak více nezajímá, dotazované ženy mnohdy odpovídaly, že jsou informované o virtuálních měnách od svých manželů či partnerů, kteří o tomto tématu vědí více. Pouze 16 respondentů z dotazovaných vlastní virtuální měnu, což činí necelých 12 %, tedy velmi malé procento v porovnání s medializací kryptoměn v současné době. Respondenti, kteří vlastní virtuální měny, byli muži z generace X a Y, kteří byli dobře informováni a v dotazníku dokázali jednoznačně a správně odpovědět na všechny otázky. Nejmladší věkovou skupinu představovala generace Z, tuto skupinu zastupovalo 21 respondentů, přičemž 3 muži dokázali odpovědět správně na všechny otázky, ač žádnou virtuální měnu nevlastní. Důvodem toho, že virtuální měnu nevlastní, bude zřejmě to, že jsou ve věku do 20 let, čili studenti a nemají finance na investice do virtuálních měn. Na otevřené otázky týkající se Bitcoinu byla většina odpovědí nesprávná, pouhých 19 respondentů odpovědělo na všechny otázky správně, což činí necelých 14 %. Autorka při vyhodnocování uznávala více odpovědí jako správných, tedy např. u otázky: „Kdo je tvůrcem Bitcoinu?“ to byly odpovědi: Satoshi Nakamoto, autor není známý, osoba či skupina osob vystupující pod pseudonymem. Jednou ze skupin respondentů byli manažeři středního a vyššího managementu a jejich povědomí o virtuálních měnách nebylo příliš valné. Z toho autorka vydedukovala, že je v současné době velice nepravděpodobné zavedení používání virtuálních měn pro nákup či prodej komponent, konečných výrobků či služeb v běžném podnikatelském prostředí. K důvodům, proč nepoužívat virtuální měny v podnikatelském prostředí, patří dlouhodobé kontrakty mezi podniky s pevně stanovenými cenami. Hovoříme-li o nejznámější virtuální měně Bitcoin, jeho cena je velice nestabilní, a tak by podnikům přinášela mnoho starostí vzhledem k velkým výkyvům jeho hodnoty. Podniky potřebují obchodovat ve stabilní měně a Bitcoin se chová jako spekulativní komodita. Dále je bitcoinů omezené množství. Dalším důvodem jsou finanční úřady, pojišťovny a ostatní instituce, u kterých je třeba, aby měly přehled o pohybu peněz týkajících se daného podniku. Občas jsou také virtuální měny spojovány s nelegálním obchodováním a oblastí šedé ekonomiky. V rámci obchodování s Bitcoinem je nejznámější Daarknet či Deepweb. Celkově tedy autorka musí podotknout, že povědomí o virtuálních měnách a jejich využití existuje, ale společnost se bude muset ještě mnohé naučit, aby bylo fungování kryptoměn reálné.

### 3 Stanovení hodnotících kritérií

Autorka se rozhodla pro stanovení hodnotících kritérií z důvodu, aby analyzovala, která kryptoměna by mohla být pro podnikatelské prostředí nejvhodnější.

V této části se autorka práce zabývá třemi hodnotícími kritérii, které si sama určila. Následně stanovila váhy a vyhodnotila. Prvním hodnotícím kritériem je počet transakcí za sekundu. Druhým kritériem je rozvoj technologie a třetím kritériem je průměrný objem obchodování za posledních 30 dní. Průměrný objem obchodování za posledních 30 dní je počítán z dat od 10.11.2018 do 10.12.2018 a jednotkou je americký dolar.

Autorka stanovila kritéria na základě předchozího studia kryptoměn. U každého kritéria stanovila váhu dle svého úsudku. Váhy jsou stanoveny čísly 0–5, přičemž 0 je nejnižší hodnocení a 5 značí nejvyšší hodnocení.

*Tabulka 3 Stanovení hodnotících kritérií*

Název měny	TPS	Rozvoj technologie	Průměrný objem obchodování za posledních 30 dní (USD)	Suma
Bitcoin	1 (7 tps)	0	5 (5452676472,67)	6
Ethereum	2 (25 tps)	5	4 (2096767693,40)	11
Ripple	5 (1 500 tps)	2	3 (674975307,03)	10
Neo	3 (35 tps)	3	2 (156996024,30)	8
Iota	5 (1 500 tps)	5	1 (11921816,47)	11

*Zdroj: vlastní zpracování dat z coinmarketcap.com*

Z rozboru v tabulce autorka zjistila, že nejlepší výsledky získala Iota a Ethereum. Iota se z hodnocených měn nejrychleji technologicky rozvíjí a je schopna zajistit 1500 transakcí za sekundu, je rychlá a má nulové poplatky. V současné době na ni není přizpůsobený platební systém, do budoucna má však velký potenciál. Hodnota průměrného obchodování za

posledních 30 dní je v porovnání s ostatními virtuálními měnami nejnižší. Můžeme tedy předpokládat, že se nejméně používá.

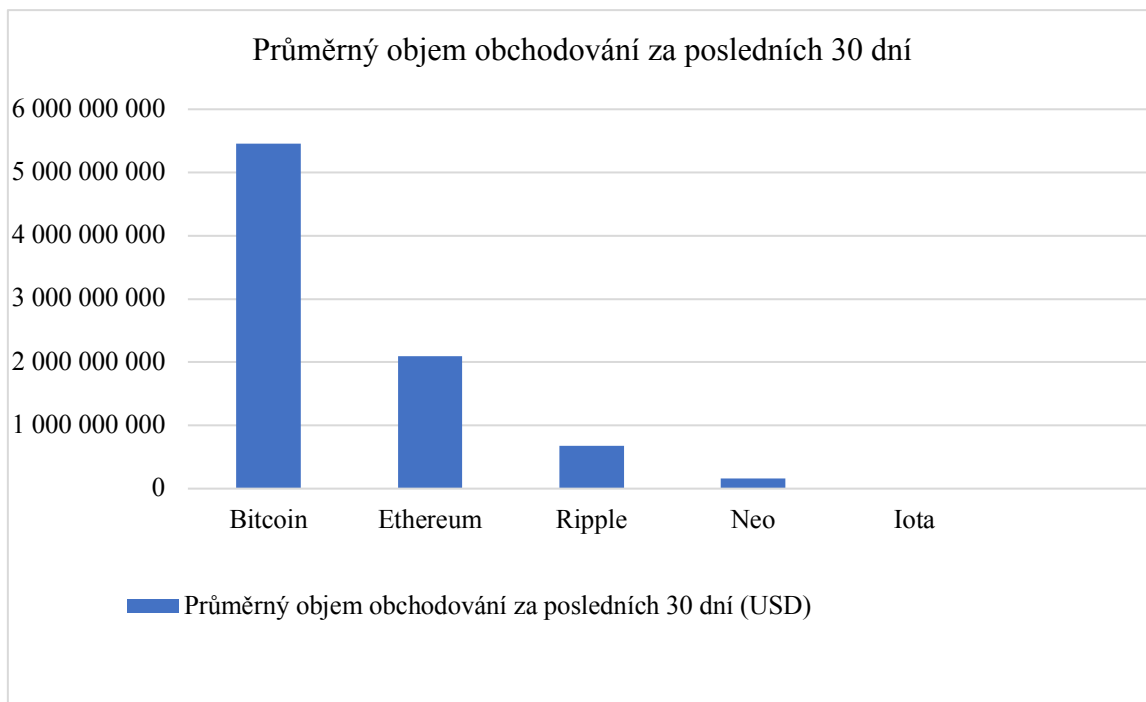
Stejný počet bodů má také Ethereum, které má druhý největší průměrný objem obchodování za posledních 30 dní s hodnotou 2 096 767 693,40 USD, dále se rychle vyvíjí technologie smart contractů a Dapp, proto autorka zvolila váhu 5 u rozvoje technologie. Ethereum je přístupné uživatelům a využití v praxi, například v některých počítačových hrách.

Na další příčce s 10 body se umístil Ripple, který zajistí 1500 transakcí za sekundu, rozvoj technologií je pomalejší, avšak Ripple má dosažitelné cíle. Vyvíjí se dle stanovených představ vývojářů.

Neo zajistí pouze 35 transakcí za sekundu, což je z hlediska současných požadavků velmi nízká rychlost. Rozvoj technologie není tak rychlý, jelikož Neo pochází z Číny, kde jsou kryptoměny zakázané. V současné době je v rámci porovnávaných virtuálních měn druhou nejméně používanou.

Jako poslední v tabulce se umístil Bitcoin, který zajistí nejméně transakcí za sekundu a jeho technologie se již nerozvíjí. V současné době je ale nejvyužívanější virtuální měnou, přičemž průměrný objem obchodování v období od 10. listopadu do 10. prosince dosáhl hodnoty 5 452 676 472,67 USD. Bitcoin se tedy nejvíce využívá, ale jelikož se nevyvíjí, nemá velké vyhlídky do budoucna.

Na základě výsledků z tabulky číslo 4 by autorka do podnikatelského prostředí doporučila virtuální měnu Ethereum, jako perspektivní. Jeho předností jsou především možnosti smart contractů a decentralizovaných aplikací, které by se v budoucnu mohly pro běžné podnikatelské prostředí aktivně využívat. V současné době by k plné implementaci v cestě stála nízká transakční rychlost.



Graf 4 Průměrný objem obchodování za posledních 30 dní

*Zdroj:* vlastní tvorba

Graf 4 znázorňuje průměrný objem obchodování za posledních 30 dní. Na ose x se nacházejí názvy jednotlivých kryptoměn a na ose y hodnoty v USD. Z grafu můžeme vidět, že Bitcoin je jednoznačně nejvíce obchodovatelnou kryptoměnou.

## 4 Problematika využití kryptoměn v ČR

Kryptoměny, stejně jako ostatní přední světové technologie, s sebou nesou potenciál zlepšit život každého z nás a usnadnit nám každodenní činnosti. K dosažení plné implementace kryptoměn bude však třeba radikálních změn fungování společnosti. Edukace v oboru je nezbytná, a to nejen u lidí, kteří se kryptoměnami přímo zabývají, jako jsou vývojáři a programátoři, ale primárně u široké veřejnosti.

Co se týče technické stránky kryptoměn, je Česko velice silným hráčem na Bitcoinové mapě světa. Významný mining pool Bitcoinu, Slush pool, byl založen českým vývojářem Markem Slush Palatinusem, hardwarová peněženka s názvem Trezor, jež je jedním z nejbezpečnějších způsobů pro uložení kryptoměn, byla vytvořena českým inovátorským týmem SatoshiLabs. Co se týče bitcoinmatů, můžete u nás nalézt české General Bytes nebo bitcoinmaty společnosti WBTBC, kterých je po České republice 8. V Praze má tato společnost i zákaznické centrum. Ve prospěch kryptoměn hovoří i fakt, že Praha v minulosti hostila několik kryptokonferencí, v Praze také vznikla první kryptokavárna na světě – Paralelní Polis. Česká republika je s počtem něco přes 100 podniků akceptujících kryptoměny výrazně v popředí světové kryptokomunity. I přesto, že máme hned několik informačních kanálů zaměřených na kryptoměny (Cointelegraph, Kryptomagazin, BTCTip), je však u nás povědomí o virtuálních měnách poměrně nízké. Pokud se pak zaměříme na implementaci a vývoj kryptoměn v podnikání, v porovnání s některými státy východní Asie či Ameriky má Česká republika výrazné mezery.

Zatímco země jako je Rusko či Venezuela po dlouhodobém plánování již zakládají vlastní blockchayny s národní kryptoměnou, vláda České republiky se teprve nedávno vyjádřila k záležitosti kryptoměn. Zástupci České fintech asociace a Svazu průmyslu ČR se na memorandu o spolupráci v používání blockchain technologie pro Českou republiku vyjádřili, že mají v plánu přitáhnout více zahraničních investorů a podpořit aplikaci kryptoměn v podnikání. Tento krok české vlády, ač velice progresivní, je značně opožděn oproti zahraničním státům. Většina zemí již započala pokusy o využití nebo regulaci kryptoměn, či dokonce v případě Číny úplný zakáz kryptoměny. Fakt, že vládní instituce daného státu mají potřebu se vyjádřit k tématu kryptoměn znamená, že kryptoměny ve státě hrají podstatnou roli a mají konkrétní dopady na jeho obyvatelstvo. To se nedá tak docela

řít o České republice. Například Jižní Korea v srpnu roku 2018 investovala 4.4 miliard dolarů do podpory inovativního růstu technologie blockchainu. Tento krok byl rozhodnut přímo korejským finančním úřadem (*Cryptoslate.cz, 2018*). Takovýto krok je těžko možné očekávat od české vlády. Zatímco konglomeráty jako LG, Samsung nebo Hyundai se v Koreji aktivně podílí na těžbě kryptoměn a zároveň implementují technologie jako IoT či inteligentní domácnosti, u nás takové kroky k rozvoji blockchain technologie není možné realizovat. Důvodů k této situaci v České republice je možné uvést hned několik. Ať už se budeme bavit o ekonomickém či hospodářském statusu země, celkové vzdělanosti populace či počtu firem se srovnatelným profitem jako společnosti LG nebo Samsung, všechno mluví v neprospěch České republiky. S přihlédnutím k současné informovanosti české společnosti by se dalo říci, že zdejší prostředí není na implementaci kryptoměn v současné době připraveno.

## **4.1 Charakter českého podnikání**

Největší překážkou reálného využití kryptoměn v českém podnikatelském prostředí je nízký počet firem zabývajících se souvisejícími odvětvími. Vzhledem k naší legislativě, která není k podnikatelům vyloženě vstřícná, je zakládání nových firem poměrně obtížné. Zaběhlé firmy se mnohdy drží tradičních postupů a inovace v nich nemá takový prostor jako v zahraničních firmách.

Většina českých firem se spíše snaží zdokonalovat v procesech výroby, které mají již zaběhlé a do nových odvětví tolik neexpandují. To je však velice důležitý aspekt pro plné využití kryptoměn, neboť jejich potenciál neleží v současném ekonomickém a obchodním systému a běžných transakcích, ale v ekonomickém systému budoucnosti, jehož zavádění je závislé na ostatních technologiích, mimo technologie blockchainu. Virtuální měny jsou v každém případě přínosem k současnému platebnímu systému, jejich využití však sahá mnohem dál a k plnému pochopení jejich možného využití je třeba zabývat se pokrokovými metodami a ty aplikovat v praxi.

K řešení této situace je tedy potřeba, aby společnosti zabývající se technologickým, automobilovým či strojním průmyslem začaly expandovat do nových odvětví a učit se pokrokové postupy a ty aplikovat v praxi. Vliv společností z okolních zemí je zde v každém případě na místě. V dnešní době již není prostor pro tradice, alespoň ne tolik, jako tomu bylo

dříve. Mnohem důležitější je držet krok s konkurencí a investovat do nových směrů vývoje. Zahraniční firmy využívající kryptoměny jsou vysoce diverzifikované a mají široké spektrum odvětví, jimiž se zabývají. V českém prostředí jsou obvyklejší firmy, které se zabývají pouze jedním odvětvím. Tato skutečnost úzce souvisí s ekonomickou stránkou věci. V České republice není dostatečná kupní síla pro zavádění tohoto typu nových produktů a služeb. Většina firem investuje do inovací spojených s výrobou, logistikou, kvalitou a zdokonalováním zaběhlých procesů, a tudíž investice do diverzifikace nejsou primárním cílem. Pokud si ale například budete pořizovat cenově dostupné auto, patrně nebudete očekávat, že bude vybaveno počítačem, jenž dokáže pomocí IoT komunikovat s ostatními inteligentními spotřebiči.

Valná většina předních českých firem nemá majitele v České republice, ale je ve vlastnictví některé z velkých světových firem. V České republice nejsou podniky, jichž by se kryptoměny přímo týkaly při své současné úrovni implementace. Kryptoměny se nachází v rozvojové fázi a k jejich využívání je třeba se zároveň podílet na jejich vývoji. K tomu ze své současné pozice v globální ekonomice a průmyslu nemá Česká republika jak výrazně přispět. Jediným způsobem, jakým se české podniky mohou aktivně podílet na rozšíření kryptoměn je participace na projektech iniciovaných zahraničními podniky. Většina projektů souvisejících s kryptoměnami hledá partnery pro ještě větší diverzifikaci.

Předtím, než se kryptoměny budou moci plně zavést na běžný trh se zbožím a reálně se využívat v běžném podnikatelském prostředí u nás, bude muset být jejich finanční stránka vysoce zdokonalena. Jak je zmíněno v teoretické části, kryptoměny trpí oproti konvenčním způsobům plateb velkými problémy s rychlostí, škálovatelností a celkovou standardizací systému pro lidi s menší technickou zdatností. Transakcemi a finanční stránkou DLT se zabývají měny jako Litecoin, Dash, Stellar, Ripple nebo Bitcoin Cash, zatímco měny jako Ethereum nebo Neo plně rozvíjí nefinanční stránku technologie. Tedy zavádění zmíněných dvou měn do běžné ekonomiky, jak ji známe, není jejich primárním záměrem. Způsob, jakým se bude implementace kryptoměn projevovat v našich každodenních životech a v podnikatelských záměrech firem a živnostníků v českém podnikatelském prostředí, je v současnosti velkou neznámou a je závislý na tom, jaké měny zaujmou vedoucí pozici na kryptotrhu a jak bude probíhat aplikace jejich funkcí. To úzce souvisí s množstvím investorů, které jednotlivé měny budou mít jako podporu za svými projekty. Tudíž nejlepším způsobem, jak zavést kryptoměny do českého prostředí, jsou investice do projektů, jimž

věříme a vidíme v nich budoucnost či pro ně nalézáme konkrétní využití. Zda budou fungovat různé coiny pro jednotlivá prostředí nebo bude všechno sjednoceno pod jedním dominantním coinem, popřípadě který to bude, je asi největší otázka v současné fázi zavádění kryptoměn do podnikatelského prostředí.

Například osoba, která podniká v leteckém průmyslu, může projevit zájem o investici do měny s názvem Aeron, jenž svůj zdrojový kód koncipuje jako decentralizovaný systém databází, ve kterém je možné najít data o letadlech, letových školách a pilotech. Tento elektronický systém záznamu by měl přispět k bezpečnosti letecké dopravy. Stejnou aplikaci je však možné napsat i na Ethereum platformě či na Neo main net jako Dapp. Otázkou je, čemu dají investoři přednost a které řešení získá větší podporu. Vzhledem k současnému propadu trhu je velice těžké dělat v tomto směru jakékoliv předpovědi.

## **4.2 Informovanost veřejnosti**

Dalším velkým problémem při využívání kryptoměn v praxi je nízké povědomí společnosti o jejich významu a fungování. Aby lidé skutečně začali rozumět kryptoměnám na úrovni, kdy je budou chtít sami nakoupit, využít nebo dokonce rozšířit jejich využití o nové nápady, musí dojít ke změně u každého zvlášť. Neexistuje způsob, jak někoho vzdělávat v něčem, o co postrádá zájem. Existují však způsoby, jak lidi zaujmout a zainteresovat v předmětu kryptoměn.

Největším vlivem jsou především běžná média. Počet zpráv o kryptoobchodu v komerční televizi a novinách je minimální, ačkoli to je místo, odkud většina lidí získává informace. Kdyby, čistě hypoteticky, existoval pravidelný televizní pořad o kryptoinvestorech, všichni by se o kryptoměny zajímali mnohem více. V případě, že se zprávy o kryptoměnách začnou objevovat ve zprávách běžných televizních kanálů, bude to mít dozajista dobrý vliv na informovanost o kryptoměnách v České republice, tudíž i na rozšíření jejich využití. Dále veřejné přednášky o kryptoměnách pro lidi, kteří chtějí o kryptoměnách vědět více, ale neví, kde konkrétní informace hledat, články v časopisech či na internetových informačních portálech, to vše jsou způsoby jak veřejnost blíže seznámit s principem a potenciálem kryptoměn a jejich dopadem na životy nás všech.



### 4.3 Nedůvěra k novým technologiím

Většina podnikatelů by při otázce, proč nevyužívají ve své firmě některou z nových technologií, patrně odpověděla, že jí nedůvěřují. A není divu, není možné věřit něčemu, co nikdy neviděli v praxi fungovat. Důvěra v nové technologie a inovativní praktiky je dozajista velkou překážkou v případě využití kryptoměn v podnikání. Málokdo se odhodlá investovat do něčeho, co nemá žádnou fyzickou formu a není možné to zvážit nebo změřit. Klasické peníze jako by pro většinu lidí stále měly alespoň nějakou „reálnou“ hodnotu, ačkoliv samotné bankovky ani mince nemají hodnotu, kterou představují, ani už nejsou kryté drahými kovy jako tomu bylo v minulosti. Způsobem, jak překonat tuto počáteční nedůvěru lidí ke kryptoměnám, je uvedení konkrétních případů jejich využití. Pokud by například podnik jako ČEZ zavedl blockchain technologii do své sítě, nebo snad dokonce umožnil svým zákazníkům platit bitcoinem či některými altcoiny, rozhodně by to zvedlo důvěru v kryptoměny. Velký krok pro Českou republiku v tomto ohledu udělal obchodník s elektronikou Alza.cz. Jako jeden z největších prodejců elektroniky u nás zavedl na svůj obchod možnost platby bitcoinem. Tato možnost je výhodou například pro minery nebo obchodníky s kryptoměnami. Fakt, že při nákupu elektroniky z tohoto obchodu není nutné bitcoin směňovat za fiat měnu, což se neobejde bez poplatků směnárně, ale je možné nakoupit produkty přímo výměnou za kryptoměnu, je pro ně motivací nakupovat právě na Alza.cz. Pro ostatní obchodníky je to dobrý příklad toho, že platby v kryptoměnách jsou možné a mají své výhody. Pro běžné občany, kteří o kryptoměnách nejsou informováni, to však markantní význam nemá.

## 5 Simulace využití kryptoměn

V současné době existuje hned několik reálných využití pro kryptoměny v podnikatelském prostředí. Ty jsou dostupné každému a jejich výhod je možné využít prakticky kdykoliv. Nutná je však edukace v oboru, rozhodně není dobré obchodovat s něčím, čemu člověk nerozumí. Po důkladném studiu dostupných kryptoměn se tedy autorka práce rozhodla rozebrat tři následující potenciální využití virtuálních měn v praxi. Ty bude aplikovat na smyšlenou firmu, která se bude zabývat obchodem s elektronikou.

### 5.1 Transakce

První, ale zdaleka ne jediné využití kryptoměn, které se samo nabízí, je jejich finanční využití. Ač je v současnosti finanční stránka většiny blockchainů stále v plenkách a v porovnání s konvenčními metodami placení jsou velice pomalé a nepraktické, i tak mají několik nepopíratelných výhod oproti bankovním převodům a platbám kartou.

Majitel firmy má možnost nabídnout svým zákazníkům možnost platby bitcoinem. Tuto možnost již zavedlo mnoho firem, konkrétně restaurací či kaváren, ale i obchodů s produkty různého druhu. V naší firmě bude možné platit přímo převodem do peněženky majitele firmy. Zavedení takovéto funkce, oproti online platbě kartou, nevyžaduje registraci u žádné finanční instituce. Majitel firmy nemusí být přihlášen u banky jako živnostník, a tudíž neodvádí měsíční poplatek za tuto službu jako je tomu u platby kartou. Dále je také možné platit kryptoměnami v kamenných prodejnách pomocí jednoduché aplikace do mobilu. Těch existuje celá řada. V podstatě jsou to jen softwarové peněženky, jež obsahují funkci převedení částky v dané kryptoměně na peněženku příjemce pomocí privátního klíče či vygenerováním specifického klíče pro danou transakci. Tyto platby jsou pomalejší než platby kartou, ale rychlejší než převody z účtu většiny českých bank (v případě převodu na účet u jiné banky). Výhodou těchto plateb je velice vysoká úroveň zabezpečení, anonymita a univerzální měna.

Dalším potenciálním využitím, které je již také aplikováno některými obchody, je bitcoinat přímo na prodejně. Některé společnosti provozující bitcoinmaty umožňují nákup bitcoinu přímo z automatu za různé měny. Pokud například na prodejnu přijde zákazník, který nebude

mít české koruny a bude si chtít koupit notebook, bude mít možnost zakoupit si bitcoin přímo z bitcoinmatu a následně jím zaplatit. Zatímco většina bank si účtuje poplatek za výběr v cizí měně stejně jako za platbu kartou v cizině, poplatek za nákup bitcoinu, stejně jako za transakci, je zcela minimální. Tento proces sice vyžaduje založení Bitcoin peněženky, to je však v bitcoinmatu záležitostí několika vteřin a nejsou k tomu potřeba žádné osobní údaje. Tento proces, ač se může zdát zbytečně složitý, je stále výhodnější než zakoupení korun ve směnárně nebo výběr z bankomatu.

Majitel firmy má také možnost platit za zboží, jež nakupuje na prodejnu, kryptoměnou. Samozřejmě je potřeba se domluvit s dodavatelem, který prvně musí alternativní způsob platby akceptovat. V takovém případě je pak například možné objednat zásilku elektroniky přímo od dodavatele a uhradit ji v kryptoměně. Obchodník se tak vyhne provizi pro směnárnu při nákupu cizí měny či poplatku za převod na zahraniční účet. Pro tento účel je navrhnut Ripple, zmíněný v teoretické části. Při pravidelném nákupu zboží ze zahraničí může majitel firmy na této službě ušetřit nezanedbatelnou částku.

## **5.2 Smart contracty**

Pokud zajdeme s nápadem pravidelného nákupu zboží ze zahraničí ještě dál, přímo se nám nabízí možnost využití smart contractů neboli inteligentních smluv. Ty představují technologii, jež umožňuje dvěma stranám obchodovat se zbožím na základě předem domluvených podmínek. Jejich dodržení je však na rozdíl od běžné smlouvy zajištěno automaticky, bez potřeby zásahu lidského faktoru.

Dejme tomu, že majitel firmy bude chtít sepsat smart contract s dodavatelem z Číny. Může k tomu využít například platformy Ethera. V inteligentní smlouvě bude programovacím jazykem zapsána cena produktů v katalogu, cena dopravy pro různé množství zboží, množstevní slevy, příplatky za nadstandardní služby apod. Majitel firmy už pak jen odešle objednávku a nestará se o platbu ani doručení, vše zařídí smart contract automaticky. Dodavatel pak už jen obdrží seznam zboží, které si obchodník objednal a odešle ho na jeho adresu.

Ač se na první pohled může zdát, že tento automatizovaný systém už existuje a není k němu potřeba technologie blockchainu, tento systém není tak autonomní, jak by se mohlo zdát. Pokud by tato stejná objednávka byla provedena pomocí současného systému, musí být

provedena přes elektronický katalog či e-shop, spravovaný firmou, jejíž službu dodavatel využívá. To je instituce #1. Dále pak při platbě objednávky musí obě strany využít svůj bankovní účet, každá u své vlastní banky. To jsou instituce #2 a #3. Pak zde také hraje roli zásilková společnost, #4, která se musí postarat o bezpečné doručení objednávky od odesílatele k příjemci. Výše zmíněné instituce spolu navzájem přímo nespolupracují, komunikují jen v rámci dané objednávky. To vede k prodlevám a zvýšeným poplatkům za služby.

Při využití technologie blockchainu nejen že odpadá problém převodu platby mezi dvěma bankami, ale elektronický katalog má přímý přístup k peněžence obou stran. Instituce #1, #2 a #3 jsou tak sloučeny pod jednu. Zásilková společnost pak může pomocí nefinanční strany blockchainu komunikovat přímo s peněženkami obou stran stejně jako s elektronickým katalogem. To značně ulehčí nadstandardní služby jako expresní doručení či sledování zásilky.

Takováto standardizace značně zjednoduší a zrychlí celý proces, což ušetří finance jak dodavateli, tak maloobchodníkovi. Objednávka nemusí být manuálně potvrzována dodavatelem jako je tomu u běžného e-shopu, platba v bance nemusí být potvrzena zaměstnancem banky a sledování zásilky nemusí být manuálně kontrolováno zaměstnancem zásilkové společnosti. Při jakémkoliv sporu mezi participanty jsou detaily transakce jednoduše vyhledatelné a ověřitelné ve veřejné účetní knize blockchainu (Distributed Ledger). Tento systém je plně transparentní a není v něm prakticky žádná mezera, kterou by bylo možné využít k případnému podvodu. Obě strany na začátku souhlasí s pravidly smlouvy, jež jsou pro oba výhodné a v případě, že je jedna ze stran poruší (například dodavatel, který by nedeslal objednávku), všechny údaje je možné dohledat a velice snadno odhalit případný podvod.

V tomto případě zároveň úplně odpadají problémy spojené se směnou. Ani jedna ze stran nemusí sledovat směnné kurzy a podle toho plánovat nákup či prodej a nemusí platit provizi směnárně.

### 5.3 Nefinanční využití blockchainu

Nefinanční stránka blockchain technologie může být velkým přínosem pro firmy všech podnikatelských odvětví. Na rozdíl od finanční stránky není limitován nedostatečnou úrovní vývoje a standardizace a je možné ji zavést do jakékoliv firmy bez větších obtíží. Distribuovaná síť databází, přístupná z jakéhokoliv místa na světě, může značně usnadnit aspekty jako je administrativa, personalistika, účetnictví, marketing či hodnocení jednotlivých prodejů.

Majitel naší firmy, který má uzavřenou inteligentní smlouvu s dodavatelem, může například několika kliknutími zkontrolovat množství zboží objednané jednotlivými prodejny. Pokud pak blockchain aplikaci dá přístup i k datům týkajícím se prodeje, kontrola profitu jednotlivých prodejů se stane jednoduchým procesem, který je možný udělat třeba i na telefonu. Aplikace, která bude mít přístup ke všem datům prodejny, může sama spočítat její zisk, porovnat ho s ostatními a zhodnotit je. Podobný proces je možný i v případě jednotlivých zaměstnanců. Systém hodnocení je jedna z blockchain aplikací s nejširším záběrem využití.

Další technologií, kterou je možné zavést jak do smart contractu, tak do plně decentralizované databáze firmy, je umělá inteligence. Ta může vyhodnocovat data hodnocení či profitů prodejů a navrhnout způsoby vylepšení marketingové strategie, obchodních postupů či náborem zaměstnanců. Potenciál této technologie je limitován pouze tím, jaká data je jí uživatel ochoten poskytnout.

Podnik může také využívat technologie decentralizované databáze k záznamům o zaměstnancích. Aplikace použije jako zdrojová data docházku, výkonnost, zkušenosti a schopnosti jednotlivých zaměstnanců společně s jejich osobními údaji jako je bydliště, věk, vzdělání apod. a usnadní tak pověřené osobě rozdělování směn a charakteru práce jednotlivým zaměstnancům. Blockchain značně usnadňuje programování takových aplikací díky svému decentralizovanému systému. Systém odměn a prémie, soutěž o zaměstnance měsíce či zaměstnanecké ankety a návrhy jsou mnohem jednodušší, spravedlivější a efektivnější.

## 5.4 Decentralizované aplikace

Na vývojářské platformě, jakou je například Ethereum nebo Neo, je také možné napsat decentralizované aplikace využívající vlastní tokeny, které plní roli kryptoměny konkrétní společnosti. Podnik obchodující s elektronikou má například možnost vytvořit věrnostní program pro své zákazníky. Těm budou pomocí aplikace přiřazovány tokeny naší firmy, které mohou být nadále využívány. Například jim může být připsána funkce slevových tokenů, takže čím víc jich bude zákazník mít, tím větší slevu dostane. Tokeny mohou zákazníci směňovat mezi sebou, prodávat, nakupovat nebo vyměňovat za jiné kryptoměny. Odměna v podobě tokenů může být také udělována uživatelům za psaní recenzí na produkty. Recenze zvýší prodej zboží a tokeny rozdělené mezi uživatele je motivují k dalším nákupům. Je to způsob, jakým se může odlišit od konkurentů, přitáhnout více nových zákazníků a udržet si ty staré.

Jednotlivé Dapps se také mohou navzájem provazovat, tudíž můžeme zákazníkům nabídnout možnost využití tokenů partnerské firmy v našem věrnostním programu a naopak. Pokud například bude podnik prodávat telefony, může uzavřít partnerství s mobilním operátorem. Zákazník, jenž si zakoupí mobilní telefon se SIM kartou, získá určitý počet tokenů, který může nadále využívat na slevy či nadstandardní služby u partnerské firmy – mobilního operátora. Naopak pokud zákazník bude hojně využívat služeb mobilního operátora, ten ho pak může odměnit věrnostními tokeny, které je možné využít při nákupu ve firmě s elektronikou. Z tohoto vztahu těží jak obě firmy, které si navzájem předávají zákazníky, tak samotný zákazník, který je za využívání služeb a nákup produktů odměněn. V momentě, kdy chce přestat využívat služby dané firmy, může tokeny prodat, což přitáhne nového zákazníka. Tato aplikace může využít takzvaný Proof of purchase (PoP) neboli průkaz o zakoupení.

## 5.5 Zhodnocení

Všechny výše zmíněné aplikace virtuálních měn do prostředí podnikání jsou z technického hlediska plně reálné a je možné je uskutečnit prakticky ihned. Jediné, co je pro to třeba, je napsání aplikace programátorem. Druhou stránkou věci je však využití těchto aplikací v praxi. Kvůli nízkému povědomí o kryptoměnách ve společnosti se dá očekávat, že zákazníci by nové službě nedůvěřovali nebo dokonce nerozuměli jejímu praktickému využití

a neviděli v ní přínos. V tomto ohledu je třeba bližšího seznámení společnosti s kryptoměnami a jejich aplikací.

## Závěr:

Cílem této bakalářské práce bylo především najít možná řešení problémů, jež stojí v cestě procesu implementace virtuálních měn v českém podnikatelském prostředí. Zatímco v zemích jako je Jižní Korea, Japonsko či Kalifornie jsou kryptoměny aktivně využívány desítkami firem, jež je zároveň rozvíjejí, Česká republika v tomto ohledu značně zaostává za zbytkem světa. Nutno dodat, že tento fakt úzce souvisí s celkovou ekonomickou, politickou a hospodářskou situací země a jejím postavením v globálním obchodu a průmyslu.

K tomu, aby tato práce mohla klást otázky související s praktickým využitím kryptoměn, bylo třeba v její první části popsat technickou stránku této technologie neboli princip fungování blockchainu a těžby a vysvětlit, jakým způsobem jsou transakce na blockchainu současných kryptoměn zpracovávány. Dále autorka práce vybrala pět z prvních dvaceti kryptoměn podle tržové kapitalizace, detailně popsala jejich funkce, výhody, nevýhody, technické aspekty a porovnála je s ohledem na jejich koncept a záměry jejich vývojářů do budoucna. Dále se zde autorka zbývala obecnou problematikou kryptoměn a riziky s nimi spojenými.

Druhá část práce už byla zaměřena přímo na aplikaci zmíněných postupů v praxi, tedy jejich využití v podnikatelském prostředí. Praktická část byla uvedena průzkumem, který vypověděl o informovanosti veřejnosti ohledně kryptoměn. Předmětem praktické části bylo vytyčit body střetu podnikatelského prostředí s prostředím virtuálních měn, nalézt problémy, jež stojí v cestě jejich propojení a následně zamyslet se nad případným řešením.

Výsledek této práce vypovídá především o tom, že česká společnost je o kryptoměnách málo informovaná, tudíž jejich vývoj a implementace u nás značně zaostává. Na druhou stranu je však pravdou, že k využití potenciálu kryptoměn je potřeba radikálního zdokonalení přímo ze strany jejich vývojářů. Problematika škálovatelnosti a rychlosti většiny virtuálních měn je staví daleko za běžné platební způsoby a brzdí jejich zavádění do podnikatelského prostředí.



Bitcoin a ostatní kryptoměny dost možná přinesou revoluci do finančního systému a převrat do každodenního života všech lidí, bude to však trvat ještě přinejmenším 5-10 let, než se stanou běžně používanými a ani pak jejich vývoj nebude ještě zdaleka u konce.

Odpovědí na výzkumnou otázku, která byla položena v úvodu této práce je, že Bitcoin není nejhodnější virtuální měnou pro podnikatelské prostředí, transakční rychlost je velice nízká. Poplatky za transakce jsou vysoké, což je nevyhodné u mikrotransakcí, kde poplatek za transakci převyšuje samotnou částku. Příkladem je koupě kávy. Má také problém se škálovatelností. V současné době má sice nejvíce uživatelů, avšak tento počet se bude snižovat dle názoru autorky. Perspektivněji do podnikatelského prostředí autorka vyhodnotila virtuální měnu Ethereum, jejíž potenciál je veliký. V rámci této bakalářské práce byly splněny všechny stanovené cíle.

## Bibliografie

ATHANASSIOU, Phoebus L. *ECB Legal Working Paper Series No 16* [pdf]. European Central Bank, 2017 [cit. 2018-10-10]. ISBN: 978-92-899-3015-4. Dostupné z: <https://www.ecb.europa.eu/pub/pdf/scplps/ecb.lwp16.en.pdf>

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

STROUKAL, Dominik a Jan SKALICKÝ. *Bitcoin: peníze budoucnosti : historie a ekonomie kryptoměn, stručná příručka pro úplné začátečníky*. Praha: Ludwig von Mises Institut CZ&SK, 2015. ISBN 978-80-87733-26-4.

LEE, Howard. *Whitepaper On Distributed Ledger Technology* [pdf]. Hong Kong monetary authority. 2016 [cit 2018-18-10].

Dostupné z: <https://www.scribd.com/document/330783398/Whitepaper-on-Distributed-Ledger-Technology>

NAKAMOTO, Satoshi. *Bitcoin Whitepaper* [pdf]. Bitcoin.org, 2009 [cit 2018-18-10] Dostupné z: <https://bitcoin.org/bitcoin.pdf>

BUTERIN, Vitalik. *Ethereum Whitepaper* [pdf]. Ethereum.org, 2015 [cit 2018-19-10] Dostupné z:

[http://blockchainlab.com/pdf/Ethereum\\_white\\_paper-a\\_next\\_generation\\_smart\\_contract\\_and\\_decentralized\\_application\\_platform-vitalik-buterin.pdf](http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf)

BRITTO, Arthur a SCHWARTZ, David. *Ripple whitepaper* [pdf]. Ripple.com, 2018 [cit 2018-19-10] Dostupné z:

<https://whitepaperdatabase.com/wp-content/uploads/2017/09/Ripple-XRP-Whitepaper.pdf>

POPOV, Serguei. *Tangle Whitepaper* [pdf]. Version 1.4.3, Iota.org, 2018 [cit 2018-23-10] Dostupné z: [https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvsIqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1\\_4\\_3.pdf](https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvsIqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1_4_3.pdf)

## Citace

Bitcoin market capitalisation graph. In: *Coinmarketcap.com*. 2018. [online]. [cit 2018-12-10] Dostupné z: <https://coinmarketcap.com/currencies/bitcoin/>

DAS, Samburaj. Hedge Funds are Buying Customer Claims of Mt Gox Bitcoin Payout. In: *Crypto Coin News* 2017. [online]. [cit 2018-12-10] Dostupné z: <https://www.ccn.com/report-hedge-funds-buying-customer-claims-mt-gox-bitcoin-payout/>

YOUNG, Joseph. 8,200 BTC Moved From Mt. Gox Wallet, Possible Sell-Off Affects Bitcoin Price. In: *Crypto Coin News* 2018. [online]. [cit 2018-12-10] Dostupné z: <https://www.ccn.com/report-hedge-funds-buying-customer-claims-mt-gox-bitcoin-payout/>

BROWN, Casper. Is “Upbit” Up For Serious Legal Actions By South Korean Officials? Full Analysis. In: *Coingape.com* 2018. [online]. [cit 2018-13-10] Dostupné z: <https://coingape.com/upbit-up-for-serious-legal-actions/>

WILMOTH, Josiah. Bitcoin ETF Applicants to SEC. In: *Crypto Coin News* 2018 [online]. [cit 2018-13-10] Dostupné z: <https://www.ccn.com/bitcoin-etf-applicants-to-sec-stop-moving-the-goal-posts-eliminate-ico-double-standard/>

YASHU, Gola. Bitcoin Price Intraday Analysis. In: *Crypto Coin News* 2018 [online]. [cit 2018-13-10] Dostupné z: <https://www.ccn.com/bitcoin-price-intraday-analysis-btc-usd-in-tether-linked-breakout-action/>

S., Jimi. Blockchain: how mining works and transactions are processed. In: *Medium* 2018 [online]. [cit 2018-18-10] Dostupné z: <https://medium.com/coinmonks/how-a-miner-adds-transactions-to-the-blockchain-in-seven-steps-856053271476>

ALTUCHER, James. Everything you need to know about bitcoin. In: *Medium* 2018 [online]. [cit 2018-18-10] Dostupné z: <https://medium.com/the-mission/everything-you-need-to-know-about-bitcoin-f2a3be247a5b>

O'KEEFFE, Daniel. Understanding Cryptocurrency Transaction Speeds. In: *Medium* 2018 [online]. [cit 2018-18-10] Dostupné z: <https://medium.com/coinmonks/understanding-cryptocurrency-transaction-speeds-f9731fd93cb3>

DOSSMAN, Jack. Top 10 Cryptos Explained. In: *Medium* 2018 [online]. Altcoin Magazine. [cit 2018-18-10] Dostupné z: <https://medium.com/altcoin-magazine/the-top-10-cryptos-explained-2bd116c6a68c>

POLYSWARM. Companies Already Brilliantly Using Smart Contracts. In: *Medium* 2018 [online]. Polyswarm. [cit 2018-18-10] Dostupné z: <https://medium.com/polyswarm/5-companies-already-brilliantly-using-smart-contracts-ac49f3d5c431>

H., Alexandra. Problémy s Ethereum Constantinopole. In: *kryptomagazin.cz* 2018 [online]. [cit 2018-18-10] Dostupné z: <https://kryptomagazin.cz/update-nejjistota-problemy-s-ethereum-constantinopole-v-2018-se-ho-asi-nedockame/>

DIRAR, Ahmed. Santander and HSBC Part Ways in Choosing between Ripple and Swift for Global Money Transfers. In: *Ripple News*. ripplecoinnews.com 2018 [online]. [cit 2018-18-10] Dostupné z: <https://ripplecoinnews.com/santander-and-hsbc-part-ways-in-choosing-between-ripple-and-swift-for-global-money-transfers>

LEVENSON, Noam. NEO versus Ethereum. In: *Hackernoon.com* 2018 [online]. [cit 2018-19-10] Dostupné z: <https://hackernoon.com/neo-versus-ethereum-why-neo-might-be-2018s-strongest-cryptocurrency-79956138bea3>

GRABOWSKI, Dylan. NEO News: Week in Review. In: *Neonews.com* 2018 [online]. [cit 2018-19-10] Dostupné z: <https://neonewstoday.com/general/neo-news-week-in-review-november-5th-to-november-11th/>

AKOLKAR, Bhushan. China officially bans all crypto-related commercial activities. In: *Bitcoinist.com* [online]. [cit 2018-19-10] Dostupné z: <https://bitcoinist.com/china-officially-bans-crypto-activities/>

POPOV, Serguei. Introduction to Iota. In: *IOTA Developers Hub 2018* [online]. [cit 2018-20-10] Dostupné z: <https://docs.iota.org/introduction>

TREICHL, Carolin. DXC Technology Teams with Blockchain Specialist IOTA at Hannover-Messe- Industrie. In: *DXC.Technology 2018* [online]. [cit 2018-20-10] Dostupné z: [http://www.dxc.technology/nce/press\\_releases/144635-dxc\\_technology\\_teams\\_with\\_blockchain\\_specialist\\_iota\\_at\\_hannover\\_messe\\_industrie\\_making\\_industry\\_4\\_0\\_safe](http://www.dxc.technology/nce/press_releases/144635-dxc_technology_teams_with_blockchain_specialist_iota_at_hannover_messe_industrie_making_industry_4_0_safe)

HUILLET, Marie. Japanese IT Giant Fujitsu Launches Blockchain-Based Rewards System for Retail. In: *Cointelegraph.com* 2018 [online]. [cit 2018-20-10] Dostupné z: <https://cointelegraph.com/news/japanese-it-giant-fujitsu-launches-blockchain-based-rewards-system-for-retail>

MUELLER, Chris. IOTA: #2 of real world use cases. In: *Medium* 2018 [online]. [cit 2018-20-10] Dostupné z: <https://medium.com/@iotasupporter/iota-2-of-real-world-use-cases-6355ab5cc1ed>

KHAN, Faisal. IOTA's Smart city stride. In: *DataDrivenInvestor.com* 2018 [online]. [cit 2018-20-10] Dostupné z: <https://www.datadriveninvestor.com/2018/07/11/iotas-smart-city-strides/>

VÍTOVÁ, Nela. V Holandsku vznikne město budoucnosti. In: *Czechcrunch.cz* 2018 [online]. [cit 2018-20-10] Dostupné z: <https://www.czechcrunch.cz/2018/07/v-holandsku-vznikne-mesto-budoucnosti-ktere-bude-pestovat-vlastni-jidlo-i-zpracovavat-odpad/>

MUNRO, Andrew. Taiwan to use IOTA Tangle-based citizen ID cards, data marketplace. In: Finder.com 2018 [online]. [cit 2018-20-10] Dostupné z: <https://www.finder.com.au/taiwan-to-use-iota-tangle-based-citizen-id-cards-data-marketplace>

SETH, Shobhit. Top 5 Bitcoin Mining Pools. In: Investopedia [online]. [cit 2018-31-10] Dostupné z: <https://www.investopedia.com/news/top-bitcoin-mining-pools/>

TAPSCOTT, Don a TAPSCOTT Alex. How Blockchain Technology Can Reinvent The Power Grid. In: *Fortune.com*, 2018 [online]. [cit 2018-31-10] Dostupné z: <http://fortune.com/2016/05/15/blockchain-reinvents-power-grid/>

S., Jimi. Blockchain: how a 51% attack works. In: *Medium*, 2018 [online]. Coinmonks, Good Audience. [cit 2018-31-10] Dostupné z: <https://medium.com/coinmonks/what-is-a-51-attack-or-double-spend-attack-aa108db63474>

INVESTOPEDIA. Initial Coin Offering (ICO) Definition. In: *Investopedia*, 2018 [online]. [cit 2018-31-10] Dostupné z: <https://www.investopedia.com/terms/i/initial-coin-offering-ico.asp>

BINANCE Team. Summary of the Phishing and Attempted Stealing Incident on Binance. In: *Binance News*, 2018 [online]. [cit 2018-01-11] Dostupné z: <https://support.binance.com/hc/en-us/articles/360001547431-Summary-of-the-Phishing-and-Attempted-Stealing-Incident-on-Binance>

BIEGEL, Ofir. What Will Happen When All Bitcoins Are Mined?. In: *99Bitcoins*, 2018 [online]. [cit 2018-01-11] Dostupné z: <https://99bitcoins.com/what-will-happen-when-all-bitcoins-are-mined/>

YOUNG, Joseph. South Korea's Crypto Market Overview: How Largest Banks and Conglomerates Back Exchanges. In: *Cointelegraph*, 2018 [online]. [cit 2018-29-11] Dostupné z: <https://cointelegraph.com/news/south-koreas-crypto-market-overview-how-largest-banks-and-conglomerates-back-exchanges>

Bitcoin, *Historický vývoj ceny bitcoinu* [online]. In: . 2018 [cit. 2018-12-03]. Dostupné z: <https://coinmarketcap.com/currencies/bitcoin/>

Grafické znázornění, *Blockchain technologie*: [online]. In: . [cit. 2018-12-04]. Dostupné z: <https://idevji.com/what-is-blockchain-technology/>