Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra ekonomiky

Diplomová práce

Ekonomická analýza Bitcoinu

Bc. Jakub Anděl

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Jakub Anděl

Informatika

Název práce

Ekonomická analýza Bitcoinu

Název anglicky

Economic analysis of Bitcoin

Cíle práce

Hlavním cílem této práce je vyhodnotit míru závislosti mezi cenovou hladinou nejsilnější virtuální měny Bitcoin a vybranými komoditami z finančních odvětví drahých kovů, akciových indexů, dluhopisů, indexů fiat měn a dalších virtuálních měn.

Vedlejším cílem práce je zpracování ekonomické prognózy virtuální měny Bitcoin s délkou prognostického horizontu tří měsíců.

Metodika

Metodika teoretické části práce se zakládá na studiu české i zahraniční literatury. Poznatky, které autor v rámci zpracování teoretické části načerpal, budou vhodně aplikovány při zpracování empirické části práce.

V empirické části této práce se bude autor věnovat vyčíslení míry závislostí mezi vybranými komoditami a cenovou hladinou virtuální měny Bitcoin. Závislost mezi komoditami bude měřena za pomoci statistické metody korelační analýzy, která dokáže statistickou závislost prvků spolehlivě vyhodnotit. Dále bude v rámci empirické části zpracována ekonomická prognóza. Pro účely ekonomické prognózy bude třeba využít metod statistické analýzy dat a ekonometrického modelování.

Doporučený rozsah práce

60 stran

Klíčová slova

Bitcoin,blockchain,virtuální měny, prognoza, decentralizace

Doporučené zdroje informací

ANTONOPOULOS, Andreas M. Mastering bitcoin. Sebastopol CA: O'Reilly, 2015. ISBN 978-1-449-37404-4.

NARAYANAN, Arvind. Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton: Princeton University Press, [2016]. ISBN 978-0691171692.

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

SWAN, Melanie a Alex TAPSCOTT. Blockchain: blueprint for a new economy. Sebastopol, CA: O'Reilly, 2015. ISBN 14-919-2049-1.

SZMIGIELSKI, Albert. Bitcoin Essentials. 1. Birmingham: Packt Publishing, 2016. ISBN 978-1785281976.

Předběžný termín obhajoby

2019/20 ZS – PEF (únor 2020)

Vedoucí práce

Ing. Petr Procházka, Ph.D., MSc

Garantující pracoviště

Katedra ekonomiky

Elektronicky schváleno dne 5. 11. 2019

prof. Ing. Miroslav Svatoš, CSc.

Vedoucí katedry

Elektronicky schváleno dne 7. 11. 2019

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 26. 11. 2019

Čestné prohlášení

Prohlašuji, že svou diplomovou práci Ekonomická analýza Bitcoinu a jiných virtuálních měn jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 28.11.2019 _____

Poděkování

Rád bych touto cestou poděkoval Ing. Petru Procházkovi, MSc, Ph.D. za jeho odborné rady a podporu při psaní této diplomové práce.

Ekonomická analýza Bitcoinu

Abstrakt

Tato diplomová práce řeší vývoj kurzu virtuální měny Bitcoin. Jejím cílem bylo zpracovat ekonomickou prognózu budoucího vývoje této virtuální měny, s délkou prognostického horizontu tří měsíců a vyšetřit míru korelace s dalšími virtuálními měnami, cenou zlata, indexem amerického dolaru, indexem Eura, akciovým indexem S&P500 a výnosem z amerických dluhopisů s délkou splatnosti deset let.

Klíčová slova: Bitcoin, blockchain, virtuální měny, prognóza, decentralizace, peníze, těžba, právo

Economics analysis of Bitcoin

Abstract

This diploma thesis deals with development of virtual currency Bitcoin exchange rate. The objective was to produce an economic forecast for development of this virtual currency, with a forecasting horizon of three months and to detect the degree of correlation with others virtual currencies, price of gold, American dollar index, Euro index, stock index S&P500 and United States ten years bond yield.

Keywords: Bitcoin, blockchain, virtual currencies, prognosis, decentralization, money, mining, law.

Obsah

Seznam obrázků

Seznam tabulek

Seznam použitých zkratek

POW – Proof of work, mechanismus konsenzu
XRP – Ripple, virtuální měna
UTXO – Unspent transaction outputs cache, databáze transakčních výstupů
DDOS – Distributed denial of service, jeden z druhů kyberútoku
SHA – Secure hash algoritm, kryptografický algoritmus
CPU – Procesor
ALU – Aritmeticko logická jednotka
ATH – All time hight, nejvyšší dosažená hranice
EVM – Ethereum virtual machine
LTC – Litecoin, virtuální měna
BTC – Bitcoin, virtuální měna
DF – Dickey-Fuller test, test jednotkového kořene
ADF – Augmented dickey fuller test – rozšířený test jednotkového kořene

1. Úvod

Jedním ze současných trendů, nejen na finančních trzích, ale také v informačních technologiích jsou virtuální měny. Pozornost si virtuální měny získávají především díky vyspělosti technologie, která za nimi stojí a možnosti vysokých výnosů z případných investic do některé z virtuálních měn.

Aktuálnost tématu virtuálních měn podtrhují neustále vznikající nové virtuální měny, jejichž snahou je napodobit úspěch Bitcoinu, nejsilnější soudobé virtuální měny, která svým založením přispěla k rozvoji moderních technologií decentralizovaných platebních sítí, blockchainu a dalším.

Zvyšující se mediální zájem o svět virtuálních měn staví Bitcoin a další virtuální měny do předních pozic zorného pole investorů z řad odborné i laické veřejnosti. Emoce, které virtuální měny ve společností vzbuzují se velmi různí, část společnosti jejich technologii vůbec nevěří. Někteří tyto technologie vnímají kladně, ale rozhodli se své peníze nevkládat a další vidí virtuální měny jako sektor se značným investičním potenciálem a vidinou snadného a rychlého zhodnocení svých vkladů. Prudké pohyby kurzu virtuálních měn směrem nahoru jsou lákavou vidinou pro mnoho investorů. Stinnou stránkou vysoké volatility jsou však i prudké propady cenových hladin virtuálních měn.

Každý, kdo se rozhodne své peníze do virtuálních měn vložit, ať krátkodobě nebo dlouhodobě, řeší otázky, kam se bude kurz zvolené virtuální měny ubírat. Jestli dojde k růstu nebo poklesu, jaký bude budoucí vývoj a podle jakých ukazatelů ho odhadnout. Cílem této práce je nalézt odpověď na tyto otázky, a poskytnout přehled o tom, jakých ukazatelů se před případnou investicí všímat.

2. Cíl práce a metodika

2.1. Cíl práce

Hlavním cílem této práce je vyhodnotit míru závislosti mezi cenovou hladinou nejsilnější virtuální měny Bitcoin a vybranými komoditami z finančních odvětví drahých kovů, akciových indexů, dluhopisů, indexů fiat měn a dalších virtuálních měn.

Vedlejším cílem práce je zpracování ekonomické prognózy virtuální měny Bitcoin s délkou prognostického horizontu tří měsíců.

2.2. Metodika

Metodika teoretické části práce se zakládá na studiu české i zahraniční literatury. Poznatky, které autor v rámci zpracování teoretické části načerpal, budou vhodně aplikovány při zpracování empirické části práce.

V empirické části této práce se bude autor věnovat vyčíslení míry závislostí mezi vybranými komoditami a cenovou hladinou virtuální měny Bitcoin. Závislost mezi komoditami bude měřena za pomoci statistické metody korelační analýzy, která dokáže statistickou závislost prvků spolehlivě vyhodnotit. Dále bude v rámci empirické části zpracována ekonomická prognóza. Pro účely ekonomické prognózy bude třeba využít metod statistické analýzy dat a ekonometrického modelování.

3. Teoretická východiska

V teoretické části této práce je pojednáváno o vzniku, rozvoji a technologii virtuálních měn. Vytvoří ucelený přehled o fungování technologie blockchain, principu těžby a stavbě sítí používaných pro obchodování virtuálních měn. Kapitoly Peníze, Blockchain, Transakce a těžba virtuálních měn pojednávají o principech, které jsou pro všechny virtuální měny společné, zvláštní kapitoly pak tvoří rozsáhlá kapitola Bitcoin, která obsahuje všechna specifika měny, jejíž zkoumání je předmětem této práce. Poslední kapitolou v rámci teoretické částí je kapitola zmiňující další významné virtuální měny, se kterými bude v rámci empirické části Bitcoin porovnáván.

V první části je zmíněn vznik peněž a krátce popsán přechod od jejich počátku po soudobé měny a virtuální měny. V kapitole jsou uvedeny rozdíly mezi virtuální a konvenční měnou. Navazující kapitola pojednává o technologii blockchainu, jejím vzniku, funkci a limitech. Krátce zmiňuje princip funkce mechanismu, za pomocí kterého je v rámci sítě dosahováno konsenzu. Třetí kapitola obsahuje popis struktury transakcí a jejích fungování. Čtvrtá kapitola pojednává o principech rozšiřování blockchainu, historii těžby bloků a její rentabilitě v rámci mechanismu proof of work. Pátá kapitola popisuje vznik, fungování a způsoby uchovávání virtuální měny Bitcoin. Taktéž zmiňuje rozdíly mezi fungováním této virtuální měny a konvenčním platebním systémem, vhodné strategie investování, možnosti a úskalí plateb Bitcoinem. Poslední kapitola v rámci teoretické části pojednává o ostatních velkých virtuálních měnách. Krátce zmiňuje jejich specifika a tržní podíl.

3.1. Literární rešerše

V následujících odstavcích je stručně popsán dosavadní výzkum autorů, věnujících se problematice faktorů, působících na kurz virtuální měny Bitcoin.

Polasik ve své práci z roku 2014 došel k závěru, že cena Bitcoinu je hlavně výsledkem jeho popularity a transakčních potřeb uživatelů sítě. Testoval také počty hledání

klíčových slov spojených s Bitcoinem v internetovém prohlížeči Google. Tato proměnná se podle něj ukázala jako velmi významná, zatímco objem transakcí nikoli. (1)

Bouoiyour & Selmi se ve svém výzkumu z roku 2014 pokusili vysvětlit cenu Bitcoinu regresí jeho tržní hodnoty proti množství různých nezávislých proměnných včetně ceny zlata, počtu hledání slova „Bitcoin“ v internetovém prohlížeči Google, měření rychlosti Bitcoinu, co se týče přenosu transakcí atd. Později zjistili, že většina těchto proměnných nedosahuje větší statistické významnosti nežli 5 %. (2)

Van Alstyne v roce 2014 označil za hlavní zdroj hodnoty Bitcoinu jeho technologický přínos v podobě vyřešení problému tzv. dvojí útraty. I když prolomení tohoto problému umožnilo vznik a rozšíření virtuálních měn, tak se toto řešení za nosič hodnoty Bitcoinu samo o sobě nepovažuje. (3)

3.2. Peníze

Od původních platidel z doby cca 3000 let před naším letopočtem k dnešnímu pojetí peněz a virtuálních měn, kterými se bude tato diplomová práce zabývat, prošlo lidstvo značným vývojem. Původním platidlem pro účely pořízení zboží k osobní spotřebě, nebo za účelem další směny bylo již kolem roku 3000 před naším letopočtem jídlo. Postupem času a dalším vývojem přicházela platidla jako kovy, kovové mince a papírové peníze, jak je známe dnes. (4)

Peníze jsou prostředkem, vyjadřujícím hodnotu věcí. V minulosti bylo možné vyjádřit hodnotu zboží, či služeb v různých komoditách. Předpokladem, který je spojoval byla důvěra lidí v hodnotu a stálost těchto komodit. (5)

Základními předpoklady funkce pěněz jsou podle ekonomických teorií funkce zůčtovací jednotky, prostředku směny a uchovatele hodnoty. Zůčtovací jednotkou je myšleno chápání hodnoty peněž účastníky směnny jednotně tak, aby byly účastníci směny schopni vyjádřit cenu zboží či služby na přibližně stejnou pěněžní hodnotu. Peníze fungující jako prostředek směny znamená, že pokud obchodník dostane za své zboží nebo

služby platidlo, musí být stejné platidlo použitelné bez komplikací při další směně s třetí osobou. Uchování hodnoty je funkcí peněz, která vyjadřuje jejich relativní stálost. To nezmená, že peníze neztratí výrazně na hodnotě od uplynutí nabytí peněž do okamžiku, kdy se majitel rozhodne je utratit. (4)

3.2.1 Konvenční měny

Nejrozšířenějším stávajícím platidlem jsou tzv. fiat měny neboli měny s nuceným oběhem. Slovo „fiat“ je latinského původu a znamená „z nařízení“. Tyto měny bývají vytvořeny státem a jsou zakotvené v zákonech. Některé fiat měny jsou přijímány mimo domovské státy i mezinárodně. Příkladem takové měny může být Euro, které vydává evropská národní banka, nebo Americké dolary, či Britské libry. V České republice je zákonnou měnou s nuceným oběhem Česká koruna. (6) (5)

Zda je měna prijímána mimo domovský stát závisí především na sociální konvencích. Pokud je víra v měnu nízká, může přestat být prijímána, naopak v případě posilující a stabilní měny se mohou oblasti, na kterých je přijímána rozrůstat. Důvěra v měnu a její síla je ovlivňována mimo jiné politikou vlád a dalších istitucí domovských států, jakými jsou například centrální banky. Politická stabilita a silný státní aparát může přilákat do země investory. Zvýšení celkového přísunu zahraničního kapitálu vede k posílení hodnoty domácí měny. Naopak nestálá politická situace, špatná finanční politika a zvyšující se národní dluh, mohou zapříčinit odchod investorů do jiných zemí a tím ztrácí měna na hodnotě. (6)

3.3. Virtuální měny

Virtuální měny jsou digitální měny založené na kryptografii, které vznikly za cílem vytvoření globálně uznávaného platebního systému, který nebude možno regulovat zásahy ze strany státních aparátů. Na rozdíl od standartních měn, jako jsou české koruny, americké dolary nebo britské libry, nemají virtuální měny žádnou centrální autoritu, která by je mohla cenzurovat, nebo jejich šíření omezovat. Chod sítě je tedy od zájmů a rozhodnutí klíčových osob a skupin v rámci státních samospráv oprostěn. (7) (6)

První virtuální měnou, které se podařilo prorazit v globálním měřítku je Bitcoin. Dřívější pokusy o vznik silné virtuální měny většinou zanikly díky nedůvěře a odmítavému přístupu vlád a centrálních úřadů. Hybnými socioekonomickými silami pro další rozvoj virtuálních měn byly technologické a ekologické vlivy, společně s neefektivitou a vysokou cenou provozu klasického finančního systému. Vůbec první virtuální měnou, která se začala pro komeční použití využívat byla virtuální měna eCash založena v roce 1990 společností DigiCash, Inc., ta byla na rozdíl od dnešních virtuálních měn centralizovaná a přestože ji některé banky používaly, v průběhu času zanikla. (7) (6)

3.3.1 Regulace virutálních měn

Přístup státních aparátů hraje v rozvoji virtuálních měn důležitou roli. Snahou některých států jsou regulace, či úplný zákaz virtuálních měn na jejich území. Mezi státy zakazující obchod s virtuálními měnami patří například Bangladéš, Bolívie, Ekvádor, ale i Čína, přestože největší objem směny virtuálních měn má právě čínský Juan. Mezi další státy, které obchod s virtuálním měnami sice přímo nezakazují, ale jejich politika není vůči virtuálním měnám příznivá, se řadí například Francie, Německo, nebo Thajsko. (8)

Potíže centrálním autoritám způsobuje především právní klasifikace virtuálních měn. Některé státy jako je Velká Británie, se snaží přistupovat k virtuálním měnám podobně jako ke klasické formě peněz a aplikovat na ně stejnou finanční a regulační politiku. V jádru věci, se ale virtuální měny od klasických měn značně liší a pokusy o aplikování stávající legislativy na virtuální měny končili nezdarem. Další státy virtuální měny jako peníze neuznávají, příkladem může být Austrálie nebo Spojené státy americké, které k virturálním měnám přistupují jako ke hmotným statkům. Hlavní problémy v regulaci virtutálních měn spočívají v nejasnostech jejich chápání a nedostatečně zpracovaná právní legislativa napříč státy. (8)

3.3.2 Právo a virtuální měny v ČR

Přesto, že virtuální měny zasahují do mnoha oblastí současného práva, nestanovuje dosud český zákon žádné regulace virtuálních měn. S rostoucím zájmem o virtuální měny lze předpokládat, že se situace změní a bude třeba vytvořit ucelená pravidla pro nakládání s virtuálními měnami, podle kterých se bude společnost řídit. Významné by bylo především přesné definování jednotlivých pojmů a termínů, které se virtuálních měn týkají. Předešlo by se tak zaměňování jejich významu a rozdílnému výkladu. Dosud jediná zmínka týkající se virtuálních měn v českém zákoně je umístěna v 2 odst. 1 písm. l) zákona č. 253/2008 Sb. o legalizaci výnosů z trestné činnosti. Mluví se o ni jako o virtuální měně.

„Osoba poskytující služby spojené s virtuální měnou, kterou se pro účely tohoto zákona rozumí elektronicky uchovávaná jednotka bez ohledu na to, zda má nebo nemá emitenta, a která není peněžním prostředkem podle zákona o platebním styku, ale je přijímána jako platba za zboží nebo služby i jinou osobou odlišnou od jejího emitenta.“ (42)

Za současné stanovisko státních orgánů lze považovat sdělení ministerstva financí z roku 2018. Ministerstvo financí se k definici virtuálních měn vyjadřuje takto:

„Pro účely tohoto sdělení se digitální měnou rozumí digitální nositel hodnoty. Jedná se o nehmotné aktivum, které je elektronicky vytvořeno a uloženo. Digitální měny nejsou vydávány či regulovány centrální bankou ani orgánem veřejné moci a nemají právní status měny. Digitální měny jsou však akceptovány některými fyzickými či právnickými osobami jako majetek, který je možné převádět, uchovávat, anebo s ním obchodovat.“ (9)

Pohled ČNB na virtuální měny objasnil její viceguvernér a člen bankovní rady Mojmír Hampl ve svém prohlášení z listopadu roku 2018.

„Nenaplňují žádnou ze tří dobrých charakteristik peněz. Není to ani uchovatel hodnoty, ani nástroj jednoduchého placení ani účetní jednotka,“

3.3.3 Architektura sítě

Jednou z klíčových vlastností virtuálních měn je decentralizovaná sít, která slouží jako prostředí pro výměnu transakcí mezi uživateli. Architektura bez centrálního prvku, na které jsou decentralizované virtuální měny založeny, se nazývá peer-to-peer. Prvky sítě, které se v rámci architektury nazývají uzly, jsou si v síti rovnocenné a navzájem spolu komunikují bez přítomnosti řídícího uzlu. Výhoda sítě peer-to-peer, spočívá v rostoucí přenosové kapacitě sítě společně s rostoucím počtem uzlů a zajištění chodu sítě nezávisle na výpadku některého z uzlů. (7)

Přesto, že jsou si všechny prvky v síti rovnocenné, nemusí mít všechny stejnou funkci. Některé uzly se zaměřují pouze na těžbu nových bloků, další slouží například jako peněženka. Uzly, které zaštitují všechny funkce, se nazývají plné uzly, anglicky full nodes. Jedině plné uzly uchovávají kompletní aktualizovanou kopii distribuované databáze transakcí, tzv. blockchainu.(6) (7)

Plný uzel uchovává kompletní a konzistentní kopii historie blockchainu. Je schopen validovat transakce procházející sítí a spravovat bitcoinové peněženky. Kromě blockchainu plné uzly uchovávají další databázi, která je označována zkratkou UTXO – Unspent transaction outputs cache. UTXO je seznam poskytující informace o výši kont jednotlivých adres. Pokaždé, když dojde k nové transakci je UTXO seznam aktualizován. Obnos z adresy odesílatele, jde připsán na účet adresáta. (6)

Tenký uzel na rozdíl od plného nedokáže samostatně zasílat transakce napříč sítí, ani neuchovává plnou historii blockchainu, neobejde se tedy bez pomoci jiného plného uzlu. Může sloužit například jako peněženka. (10)

Nejsnazší možností přístupu k virtuálním měnám je pomocí webového klienta, ke kterému se přistupuje prostřednictvím prohlížeče. Webový klient umožnuje uživateli manipulovat s peněženkou umístěnou na serveru třetí strany, uživatelské prostředí aplikací webových klientů je podobné tomu, které je známé z používání běžných aplikací online bankingu. (10)

Vysoká technologická úroveň umožuje vyvíjet software, který vytváří velmi nízkou bariéru vstupu nových zájemců o virutální měny na trh. Ke koupi stačí nainstalovat aplikaci na chytrý mobilní telefon, kterým disponuje v dnešní době téměř každý a následně pomocí webového klienta založit peněženku. (10)

Výběr klienta vždy závisí na individuálních potřebách vlastníků peněženek. Volbou plného klienta uživatel získává největší kontrolu a nezávislost, ale zároveň přebírá veškerou odpovědnost za zabezpečení svých fondů. Naopak nejsnazším způsobem přístupu k založení peněženky a nákupu virtuálních měn je webový klient. V případě využívání webových klientů nemá uživatel žádnou kontrolu nad zabezpečením aplikace webového klienta, spravovaného třetí stranou. (10)

3.3.4 Změny protokolu

Jediným možným způsobem ovlivnění chodu sítě je změna iniciovaná ze strany samotných uživatelů sítě. Souhlas pro dosažení změny napříč sítí musí vyslovit nadpoloviční většina uživatelů. Změna, která by rozporovala se zájmy uživatelů sítě tedy nikdy nebude přijata. Přerušení fungování sítě, je možné pouze zamezením chodu všech uzlů v síti. Vypnutí všech prvků v celosvětové síti najednou je praticky nemožné, resistence sítí využívaných pro směnu virtuálních měn je tedy velmi silná. (6)

Po odsouhlasení změny v protoklu a vydání nové verze softwaru je třeba všechny uzly v síti aktualizovat. Změnit verzi software na všech uzlech okamžitě a bez komplikací je v praxi nemožné, vždy budou uzly, které budou mít s včasnou instalací nové verze software problémy. Chod sítě však musí zůstat zachován i s uzly, které nemají nejnovější verzi software. (11)

Změny protokolu se rozlišují na dva typy. Jsou označovány anglickými termíny hard fork a soft fork. Hard fork zapřičinuje rozdělení blockchainu na dvě větve. Pokud nastane v rámci protokolu změna, která nově validuje bloky, které by nebyly validní ve starší verzi softwaru, dojde k větvení spojového seznamu nazývaného blockchain, který bude v rámci této diplomové práce detailněji popsán později. Uzly s nejnovější verzí

software pokračují ve stávající nejdelší větvi blockchainu, zatímco uzly se starším software nové bloky jako validní neuznává. Blockchain se tak rozvětví v bodě posledního bloku validního pro starou verzi software, kde si uzly se starou verzí vytvoří svou „nejdelší“ větev, ve které pokračují do doby, než software aktualizují. (11)

Příkladem soft fork změny je zpřísnění pravidel týkajících se validity transakcí. Uzly se zastaralou verzí software akceptují všechny nové bloky odpovídající starým pravidlům, zatímco uzly s nejnovější verzí software akceptují pouze bloky, které odpovídají novým pravidlům. Pokud uzly se zastaralou verzí software vytěží nové bloky, které nebudou ze strany uzlů s aktualizovaným softwarem akceptovány, založí novou větev. Může tak dojít k více štěpením blockchainu. Většina uzlů v síti na novou verzi softwaru aktualizuje a pokračují v nejdelší větvi. Těžební uzly, které dosud na novou verzi neaktualizovali, budou nacházet nové bloky, které nebudou z pohledu přísnějších pravidel akceptovány, což uzly se starým softwarem upozorní na možnou změnu. Nově vzniklé větve jsou oproti těm, které vzniknou při hard forku kratší. (11)

3.3.5 Pseudoanonymita

U klasických způsobů online plateb (VISA) je identifikace osob reálného světa velmi jednoduchá. Do databází obsahujících historií transakcí jsou zaznamenávány údaje jako číslo karty, jméno držitele a další, které jednoznačně určují identitu vlastníka účtu. Pro virtuální měny neexistuje instituce, která by tyto záznamy shromažďovala, informace o transakcích jsou tedy zapsány do distribuované databáze transakcí, které se říká blockchain. Informacemi o transakcích, které se do blockchainu zaznamenávají, jsou veřejné klíče odesílatele a adresáta, částka a údaje o čase průběhu transakce. O každé transakci, která v rámci sítě proběhla je v blockchainu zaznamenána informace, které jsou veřejně přístupné. V rámci Bitcoin protokolu, tvoří adresa peněženky a údaje o transakcích s ní spojených veřejnou informaci. Tyto informace lze však spojit s identitou konkrétních osob pouze obtížně. Tento stav se nazývá pseudoanonymita. (7)

Adresa peněženky, jejíž technologie bude zmíněna v samostatné kapitole je alfanumerickou kombinací znaků, která jako jediná identifikuje obě strany účastnící se

transakce. Někteří uživatelé se mylně domývají, že jsou v rámci sítě anonymní. Tento omyl může podněcovat ke zneužívání sítě k nelegálním účelům. Protiprávní zneužívání virtuálních měn kriminálmi skupinami, či jednotlivci, vedlo v minulosti k řade skandálů, ve kterých se tyto skupiny snažily legalizovat peníze nabyté z trestné činnosti za pomoci virtuálních měn. Nejčastějším případem zneužití je praní peněz nabytých ilegálních činností nebo platby za prodej drog. Bitcoinové směnárny z tohoto důvodu zavádějí opatření ve formě záznamů o osobních údajích zákazníků. Osoby, které by chtěly bitcoin zneužít pro nelegální aktivity tímto přicházení o svoji anonymitu. (7)

V roce 2013 byl americkou FBI odhalen web Silk road, který tvořil černý trh s mnoha nelegálními aktivitami, jež se na webu daly objednat a následně zaplatit virtuální měnou. Jednalo se například o prodej drog, počítačových virů, falešných dokladů, nebo objednávky nájemních vražd. Za dobu fungování webu od roku 2011 do roku 2013 proběhly na tomto webu platby v celkové výši 9,5 milionu bitcoinu. Obtížné spojení uživatelů sítě s osobani reálného světa vyvolává zdálnlivý pocit bezpečí a tímto podněcuje zneužívání vyrtuální měny k nelegálním účelům. Shanou komunity uživatelů virtuálních měn je se od těchto nelegálních aktivit oprostit. (12)

3.3.6 Burzy virtuálních měn

Pro provedení transakce musí uživatelé nejprve virtuální měnu získat. To lze provést dvěma způsoby, buď směnou za kovenční měnu nebo těžbou. Nákup za konvenční měny je nejjednodušší a nejrychlejší možností pro uživatele, kteří plánují nabytí virtuálních měn pouze pro spekulativní účely. Obzvláště za použití webového klienta, není třeba hlubších znalostí týkajících se uložení a bezpečného skladování virtuálních měn, potažmo privátního klíče k peněžence. Rozhraní webových klientů se podobá běžné aplikaci internetového bankovnicví, které je dnes běžnou součástí života. Navíc není třeba pořizovat žádný speciální hardware. Pro nákup je třeba založit pěneženku a na burze směnit konvenční měnu za měnu virtuální. Ve chvíli připsání virtuální měny na adresu nakupujícího je možné s obnosem operovat a provádět platby a transakce. (7)

Nákup virtuálních měn lze realizovat na specializovaných burzách, které se směně virtuálních měn za konvenční měny věnují. Za svou činnost vybírají burzy poplatky z nákupních transakcí. Všechny převody se v rámci těchto burz odehrávají online. Jejich výhodou je možnost koupě odkudkoli ve kteroukoli denní dobu. Některé z burz či směnáren disponují bankomaty, které dokáží za virtuální měnu vydávat klasické peníze nebo naopak. Nákup virtuální měny na burzách je kromě výměny za konvenční peníze možný i směnou za jinou virtuální měnu. (13)

Mezi největší burzy virtuálních měn patří v listopadu roku 2019: BKEX. LBank, P2PB2B, BitForex a Binance. Velikost burz je v tomto případě určována dle finančního objemu zpracovaných transakcí. Měsíční objem transakcí burzy BKEX za posledních třicet dní (od 20 listopadu) dosahuje 42 miliard dolarů. Zbylé burzy z pětice uvedené na počátku tohoto odstavce stačili za posledních třicet dní zpracovat transakce za přibližně 35 miliard dolarů každá. (14)

3.4. Blockchain

Vynález blockchainu, představený v roce 2008, byl podnětem pro decentralizaci virtuálních měn. Blockchain si lze představit jako otevřenou účetní knihu historie transakcí, do které má každý uživatel sítě možnost nahlédnout Důvěry v informace obsažené v blockchainu, je dosahováno za pomoci hromadného konsenzu, tedy bez centrálních autorit, které za ověřování transakcí v klasické finanční struktuře odpovídají. (15) (16)

Technicky si lze blockchain představit jako spojový seznam bloků stromové struktury, na jehož počátku stojí blok nazývaný genesis. Bloky obsajují distriubovanou databázi transakcí, ke které má každý uživatel v rámci sítě přístup. Kompletní a konzistentní kopii blockchainu si v sobě uchovávají pouze plné uzly, které je na vyžádání zprostředkovaně poskytují i ostatním uzlům v síti. (13) (17)

Všechny bloky v seznamu obsahují jedinečný identifikátor označovaný jako hash. Kromě vlastního hashe obsahuje blok informaci o hashi předchozího bloku a odkazuje tak

na svého předka. Důsledkem je, že z libovolného bloku v jakékoli větvi se lze zpětně pomocí odkazů na předchozí blok dostat až na genesis, který jako jediný blok v seznamu hash předchozího bloku neobsahuje. Kaskádovitost blochchainu je z bezpečnostního hlediska klíčovou vlastností. Jelikož každý z bloků odkazuje na svého předka, není možné obsah bloků měnit, aniž by došlo k přepočítání hashe všech předků. K tomu by bylo potřeba vynaložit enormní množství výpočetního výkonu. K větvení blockchainu dochází pouze při aktualizaci software, kdy uzly, které mají s aktualizací na nejnovější software problémy, vytvářejí nové větve. (10) (16)

Nové bloky jsou do blockchainu přidávány těžbou ve chvíli, kdy se těžařům podaří nalézt správný hash. Rychlost hledání hashe se různí, někdy trvá pouhou minutu a někdy až hodinu, průměrně ale nalezení nového bloku trvá 10 minut. Jakmile dojde k připojení nového bloku do blockchainu, okamžitě začíná hledání dalšího bloku. (13)

Každý blok je složen z hlavičky a těla bloku. Hlavička každého bloku v sobě ukrývá metadata obsahující informaci o jeho hashi, hashi předchozího bloku, souhrnné informace o transakcích obsažených vně bloku a obecné informace o těžbě bloku, tj. doba těžby atd. Tělo bloku v sobě obsahuje transakce, kterých běžný blok pojme zhruba pět set (10)

3.4.1 Mechanismus konsenzu

Proof of work (POW) je mechanismus sloužící k dosažení konsenzu napříč sítí. Dosažením konsenzu je zajištěna důvěra mezi uživateli ve smyslu validity nalezení nového bloku. Těžař, který nalezl nový blok, prokazuje validitu řešení pomocí hashe, jehož správnost si může každý uživatel v síti velmi jednoduše ověřit. Těžaři v rámci protokolu souhlasí s tím, že kdokoli najde validní hash první, rozšíří blockchain o nový blok, který je označen unikátním hashem a za svou práci dostane odměnu. Proof of work není jediný mechanismus, kterým je v rámci virtuálních měn dosahováno hromadného konsenzu. Dalšími mechanismy, které se používají jsou proof of stake, proof of activity, proof of capacity a další. (13)

Odměna pro vítěze těžby je připisována formou transakce, která se je nazývána coin-creator transakce. Coin-creator transakce, musí být stejně jako všechny ostatní transakce validována všemi uzly sítě a pridána mezi ostatní transakce do bloku. Těžař ji získá pouze tehdy, pokud je blok validován ostatními uzly a je zapsán na nejnovější pozici blockchainu. (13) (11)

3.4.2 Neutralita a transparentnost blockchainu

Důležitou vlastností blockchainu je jeho neutralita. Úkolem vývojářů je udržovat blockchain co nejvíce neutrální tak, aby byly platformy na něm založené snadno přístupné a použitelné všemi bez kulturních, národnostních, politických či náboženských rozdílů. Internetoví poskytovatelé se pak musí o neutralitu virtuálních měn založených na principu blockchainu zasloužit ve smyslu neupřednostňování jimi vybraných webů, propagujících virtuální měny, nebo produkty na úkor jiných. Maximální dodržování principu neutrality je z hlediska šíření virtuálních měn napříč společností velmi důležité. (8)

Systémy založené na blockchainu nabízí plně transparentní řešení, které je pro všechny účastníky sítě přístupné. Transakce v těchto systémech není možné po jejich validaci a umístění do bloku přepisovat nebo měnit bez souhlasu uživatelů sítě. V minulosti proběhlo nespočet pokusů o manipulaci, změnu záznamů, nebo jinou formu podvodu v účetních knihách, které nebyly odhaleny díky jejich netransparentnosti. (16)

3.4.3 Nepřítomnost třetích stran

Výměna transakcí v systémech založených na blockchainu probíhá bez zásahů třetích stran, přímo mezi uživateli sítě. Absence prostředníků je výhodou především pro osoby žijící v zemích s vysokou kriminalitou, v chudých regionech nebo v zemích s vysokou mírou korupce, kde se lidé na prostředníky nechtějí spoléhat. Vynechání centrálních autorit, které musí platit lidskou práci a za evidenci či zpracování transakcí vybírají poplatky, může v některých odvětvích podstatně snížit náklady a tím i ceny pro koncové spotřebitele. (11)

3.4.4 Limity blockchainu

Přestože je blockchain velmi přínosnou technologií, v cestě k jeho dalšímu rozvoji stále stojí technické limity, které je třeba odstranit. Jedním z hlavních problémů je propustnost. V případě blockchain platformy, kterou používá Bitcoin a lze ji v rámci virtuálních měn považovat za standart, je propustnost sítě omezena na zpracování cirka 7 transakcí za sekundu. Pro porovnání, jiná sít procesující platby VISA má přenosovou kapacitu v běžném režimu cca 2000 transakcí za sekundu s možností navýšení ve špičce na pětinásobek. Jedním z možných řešení, které vývojáři blockchain platformy nabízí je zvětšení transakční kapacity bloku, které by mělo za důsledek větší propustnost transakcí za sekundu. (8)

Problém dlouhé odezvy úzce souvisí s propustností blockchainu. Bloky mají jasně danou kapacitu počtu přenášených transakcí a dobu těžby. Pokud se by doba těžby uspíšila ze stávajících průměrně 10 minut na kratší časový interval, došlo by ke zvýšení propustnosti. Jak bylo zmíněno výše, potvrzení transakce trvá v průměru deset minut. V některých případech a u některých typů transakcí i déle. V porovnání s VISA platební sítí, kde potvrzení transakce trvá maximálně několik sekund je blockchain v potvrzování transakce velmi pomalý. Jedním z potenciálních řešení urychlení validace transakcí by mohlo být nasazení tzv. Lightning network. Tato technologie operující na imaginární druhé vrstvě nad vrstvou blockchainu má zajistit lepší škálovatelnost blockchainu a umožnit efektivnější práci celého systému. (8)

Za použití mechanismu proof of work vzniká při těžbě nových bloků enormní množství spotřebované energie. Tato energie je využita pouze pro nalezení validního bloku, bez další přidané hodnoty. Odměnu za nalezení bloku, dostane, jak bude zmíněno v kapitole popisující těžbu bloku pouze vítěz těžby. Práce a spotřeba elektrické energie ostatních účastníků těžby tedy přijde vniveč. Odhadovaná cena takto znehodnocené energie byla již v roce 2015 vyčíslena na 15 milionů dolarů denně. S rostoucí náročností a zájmem o těžbu virtuálních měn se množství vyplýtvané energie zvyšuje. Řešením by mohlo být použití jiného ekonomicky a environmentálně výhodnějšího mechanismu dosahování konsensu, jakým je například proof of stake. (8)

Ranou pro životní prostředí není pouze vysoké množství spotřebované elektrická energie, ale také samozný těžební hardware. Čipy, které jsou k těžbě používány mají oproti standartním počítačovým procesorů velmi krátkou životnost. Těžaři, kteří mají ambice být úspěšní, musí svůj hardware velmi často obměnovat za nejvýkonnější dostupné modely. Zastaralých čipů, které obsahují škodlivé látky jako ledek, cadmium a další se pak nevhodným způsobem zbavují a tím zatěžují životní prostředí.(8)

Na obrázku číslo 1 je možné vidět množství tzv. e-waste v kilotunách za rok. E-waste, česky elektronický odpad, je zastarlý, nebo dále nepoužitelný HW, či jiné elektronické zařízení, které nemá další využití a je spojeno s těžbou virtuálních měn. Špičky bylo dosaženo v druhé polovině roku 2018, kdy se roční spotřeba překročila 12,5 kilotun.

Obrázek 1- Množství vyprodukovaného e-odpadu spojeného s těžbou virtuálních měn

(Zdroj: Digicomist.net)

3.5. Transakce

Transakce jsou data, pomocí nichž je zprostředkován přenos virtuálních měn mezi uživateli v rámci sítě. Jsou základním stavebním kamenem a podstatou vzniku decentralizovaných sítí, jejichž snahou je realizace převodů peněž mezi uživateli bez přítomnosti centrálních autorit.

Životní cyklus transakce začíná vytvořením. Transakce může být vytvořena online, nebo offline, v obou případech ale musí být autorizována privátním klíčem vlastníka peněženky, který potvrdí přenos fondů. Autorizovaná transakce následně putuje síti tak dlouho, dokud ji některý z těžebních uzlů nezapíše do nově vytěženého bloku. Ve chvíli vložení do validního bloku je transakce zapsaná v blockchainu a stává se jeho permanentní součástí. Částka převáděná v transakci se připíše na adresu peněženky příjemce a životní cyklus transakce končí. (10)

Odesílatel není ohrožen prozrazením soukromých informací při putování transakce sítí. Informace, které transakce obsahuje se sice dostanou ke všem uzlům sítě, ale jsou veřejné a neposkytují útočníkům možnost k napadení peněženky odesílatele. První uzel na který transakce v rámci sítě narazí ji buď validuje a zašle dalším uzlům, nebo ji v případě že nesplňuje kritéria zamítne a zašle zprávu o zamítnutí uzlu, který transakci vytvořil. Kontrolou, kterou každý uzel v síti vykonává je zajištěna ochrana sítě před DDOS útoky, spamem a dalšími škodlivými vlivy. Validitu transakce ověřují uzly sítě oproti listu kritérií, které musí být splněny. (10)

3.5.1 Struktura transakce

Transakce jsou kódované datové struktury, které slouží k přesunu fondů ze zdroje, ten je označován jako vstup do cíle, který je nazýván výstup. Vstupy ani výstupy není možné nijak spojit s identitami uživatelů v síti, nebo adresami jejich peněženek. Obsah vstupů a výstupů jsou schopni rozluštit pouze jejich původci. Transakce zpravidla obsahuje mezi 300 až 400 byty dat, jejichž struktura je zobrazena v tabulce číslo 1.(10)

Tabulka 1- Struktura transakce

Velikost	Popis
4 byty	Specifikuje, kterými pravidly se transakce řídí
1-9 bytu	Číslo vyjadřující počet vstupů v transakci
Volitelné	Prostor pro transakce
1-9 bytů	Číslo vyjadřující počet výstupů v transakci
Volitelné	Prostor pro transakce
4 byty	Specifikace čísla bloku

(Zdroj: Vlastní práce)

Vytvoření transakce v rámci sítě vzniká transakční výstup. Transakční výstupy, tvořící utratitelné obnosy bitcoinu se nazývají UTXO, anglicky „unspent transaction outputs“. Odesláním obnosu na cílovou adresu, se vytvoří UTXO, které je registrováno na účet přijímatele a opravňuje jej k další manipulaci s obnosem. UTXO jsou zaznamenány v paměti každého plného uzlu. Databáze, kde jsou výstupy uloženy, se nazývá UTXO pool. (10)

Transakční výstup se zpravidla skládá ze dvou částí. První část obsahuje informace o množství přenášeného obnosu a druhá část obsahuje uzamykací skript. Tento skript uzamkne přenášený obnos před manipulací, dokud nejsou splněny podmínky výstupu. (10)

Odesláním obnosu z jedné adresy na druhou je obnos uzamčen podmínkou transakčního výstupu. Odeslaný obnos se stane součástí UTXO a je zaznamenán v blockchainu. Zápisem do UTXO se v peněžence příjemce navýší suma, se kterou může příjemce manipulovat. Naplněním podmínky dojde k odblokování obnosu ve chvíli, kdy chce příjemce nabytou částku utratit a poskytne svůj privátní klíč pro autorizaci transakce. (10)

3.5.2 Priorita transakce a transakční poplatky

Transakční poplatky jsou jednou z motivací těžebních uzlů k rozšiřování blockchainu a zajišťování bezpečnosti sítě. Poplatky jsou k transakcím přidávány povětšinou automaticky. Jejich velikost je určována velikostí transakce v kilobitech, nikoli velikostí, přenášeného obnosu. Výše transakčního poplatku je jedním z kritérií, na základě, kterých těžební uzly určují prioritu zpracování transakce. Ty s vyšší prioritou jsou

ukládány do nových bloků blockchainu přednostně, dalším z kritérií je např. stáří transakce (detailněji popsáno viz Poplatky za transakce a jejich priorita). Na počátku rozvoje sítě byly transakční poplatky povinné a jejich výše byla pro všechny uživatele stejná, v současné době (září 2019) není povinností přikládat transakční poplatek. Výše minimálního poplatku je u Bitcoinu stanovena na 0,0001 bitcoinu. Datová struktura transakce, není pro vkládání transakčních poplatků přímo zařízená, výše poplatků se počítá jako rozdíl sumy transakčních vstupů a výstupů. (10)

Priorita transakce je určována na základě jejího „stáří“, tedy doby, která uplnynula od jejího vzniku. Je počítána jako suma hodnoty a stáří transakce děleno celkovou velikostí transakce.

Priorita = Suma (hodnota transakce * stáří transakce) / velikostí transakce

V této rovnici je hodnota trankce vyjádřena v základní jednotce satoshi. Stáří transakce vyjadřuje počet bloků, které uplynuly od zápisu transakce. Tedy jak hluboko v blockchainu se transakce nachází.Velikost transakce je pak měřena v bytech. (10)

Prvních 50 kilobytů transakčního místa v bloku je vyhrazeno transakcím s vysokou prioritou. Těchto 50 kilobytů je tedy zaplněno první, bez ohledu na velikost poplatku, který z přenosu transakce vznikne. Zbytek transakčního místa je zaplněn trasakcemi, které jsou řazeny podle výše transakčního poplatku. Pokud zbyde volné místo, dojde k doplnění bloku transakcemi, jež neobsahují žádný přenosový poplatek a mají proto nízkou prioritu. Každá transakce, které se do nově vzniklého bloku nevejde, zůstává v transakčním fondu a čeká na místo v dalším bloku. Stáří těchto transakcí se zvyšuje o počet bloků, které byly vytěženy od vzniku transakce a tím se zvyšuje její priorita. (10)

3.6. Těžba virtuálních měn

Těžba virtuálních měn je proces zajišťující přidávání nových bloků do spojového seznamu transakcí. Rozšiřování blockchainu je klíčové pro realizace nových transakcí,

které jsou díky těžbě nových bloků validovány. Validovaná transakce je v novém bloku transparentně zapsána, tak aby ji mohl každý uživatel ověřit. (10) (6)

Oproti nákupu je zisk virtuální měny těžbou daleko složitější a zdlouhavější proces, aby byla těžba úspěšná je nutné investovat značné obnosy peněž do pořízení těžebního HW. Uzly specializuící se pouze na težební účely, jsou označovány jako „mining nodes“, česky těžební uzly. Všechny uzly v síti očekávají zprávu o vzniku nových bloků, avšak pro těžební uzly, má oznámení nového bloku větší význam. Oznámení nově nalezeného bloku znamená vyhlášení vítěze v těžební soutěži, tedy skončení cyklu težby bloku a signál pro počátek těžby nového. Pro těžební uzly znamená nalezení bloku okamžitý start hledání nového bloku. (10)

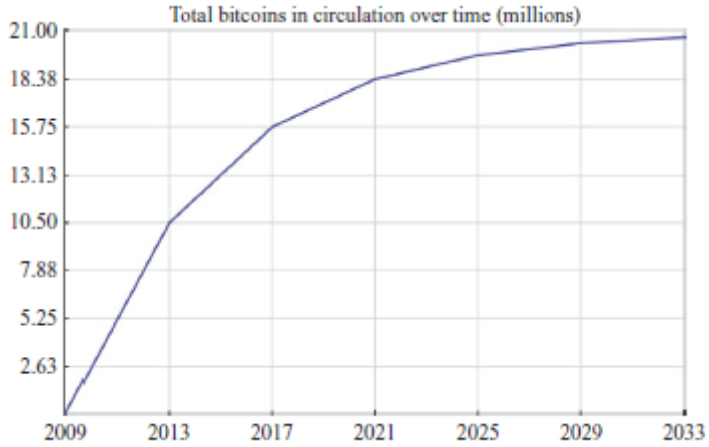
Těžaři za pomoci vysokého vypočetního výkonu hledají validní bloky, prostřednictvím kterých by rozšířili blockchain. Za validní blok je onačován blok, jehož hash je nižší než hash cíle, tkz. „targetu“. Při splnění zmíněné podmínky je stávající blockchain prodloužen o validní blok(hash) a těžba pokračuje. Target nastavuje sama sít a je upravován vždy po nalezení dvou tisíc šestnácti bloků. (19) (13)

Samotná těžba nového bloku probíhá za použití hash funkce SHA-256. Zkratka SHA vyjadřuje anglické slovní spojení Secure Hash Algoritm. SHA-256 patří do skupiny hash funkcí standardizované v roce 2001, při vzniku Bitcoinu byla vybrána jako nejsilnější soudobá hash funkce. Těžaři soutěžící o prvenství v hledání správného hashe musí tuto funkci co nejrychleji opakovaně aplikovat na různé vstupní kombinace. A výstupy, které hash funkce vrátí, se porovnávají s požadovanou kombinací pro vznik nového bloku tzv. targetem, pokud výstup odpovídá kritériím, byl nalezen validní blok. (11)

„Hash je zobrazení množiny dat obecné délky do množiny dat omezené délky (např. soubor libovolné délky zobrazí do množiny 256-bitových čísel). Obecným požadavkem na hashovací funkce je uniformní pokrytí obrazů (aby jednotlivé obrazy příslušely podobnému počtu vzorů). Požadavkem na kryptografickou hashovací funkci je navíc vysoká nelinearita (aby libovolně malá změna vzoru způsobila libovolně velkou změnu obrazu) a především asymetrickou výpočetní složitost“ (19)

Počet bitcoinů byl od počátku protokolu omezený na 21 milionů, předpokládaný datum jejich vytěžení je stanoven na rok 2040. Průběh těžby napříč časem je zobrazen na obrázku číslo 2. (7)

Obrázek 2- Průběh těžby virtuální měny Bitcoin.



(Zdroj: Lee, Dave)

3.6.1 Počátky těžby

Se snižujícím se počtem nevytěžených bloků obtížnost těžby stoupá. Na počátku vzniku virtuálních měn stačil k těžbě běžný kancelářský počítač. Práci při hledání správného hashe tak často vykonával samotný procesor – CPU jednotka. Těžaři, stejně jako dnes aplikovali SHA-256 na vstupy a při každém kroku kontrolovali, zda je výsledkem validní blok. S rostoucí složitostí zadání, které museli pro nalezení bloku řešit, přestala být těžba za pomoci samotné CPU jednotky bez dalších podpůrných čipů rentabilní. V současné době je těžba bloků natolik složitá, že těžit jako jednotlivec se vyplatí pouze specializovaným těžařům, kteří do těžebních center investovali obrovské peníze, menší těžaři se tedy shlukují do tzv. poolů, ve kterých mají šanci na úspěch. (19) (11)

Další generace těžby se vyznačovala využíváním grafických karet. Grafické karty byly v této etapě velmi užitečné, disponovaly vysokým výpočetním výkonem a běžně obsahovaly několik ALU jednotek, které umožnovaly provádět výpočty SHA-256

paralelně a tím značně urychlovaly výpočet správného hashe, navíc jich bylo možné zapojit více najednou. (11)

3.6.2 Průběh těžby

Těžba probíhá tak, že těžaři shromáždí všechny čekající transakce, které v síti najdou a aplikují na ně funkci SHA-256, jejíž výstupem je 32bitová hash hodnota. Pokud je hodnota hashe menší než požadová cílová hodnota, nalezl těžař jako první odpověd na zadaný kryptografický problém a rozšířil blockchain o nový blok. Pokud je hodnota hashe vyšší než hodnota targetu, je třeba upravit vstupní data a opakovat celý proces znovu. Dosažení správného hashe není jednoduchý proces, výpočet za pomoci SHA-256 netrvá dlouhou dobu, ale je nutné ho mnohokrát opakovat. (13)

Kryptografický problém, který je třeba pro nalezení bloku vyřešit, je vždy zadán tak, aby nebylo možno k vyřešení použít jakékoli zkratky. Správného řešení může být dosaženo pouze opakovanou aplikací šifry na SHA-256 na různou kombinaci vstupů. Největší šanci na prvenství má těžař, který dokáže vyvinout nejvyšší výpočetní výkon. Výpočetní výkon těžebních strojů se měří v jednotkách MH/s. Úspěšný těžař je ten, kterému se jako prvnímu podaří nalézt řešení. Po vyřešení problému je hash oznámen ostatním uživatelům sítě, kteří si mohou snadno ověřit jeho správnost, ověření správnosti je velmi jednoduchý a rychlý proces. Tento mechanismus, se nazývá proof of work a je, jak bylo zmíněno v samostatné kapitole pouze jedním z mnoha mechanismů dosahování hromadného konsensu ve světě virtuálních měn. (13) (10) (19)

„Počet bloků mezi blokem zahrnujícím transakci ve svých datech a blokem aktuálně těženým se nazývá počet potvrzení. Jelikož s počtem potvrzení se riziko zvratitelnosti transakce snižuje exponenciálně, je i nízký počet dosačující pro považování transakce za nezvratitelnou. U transakcí větších objemů se v praxi často požaduje počet potvrzení ≥ 6.“ (19)

Odměna, kterou těžaři za svůj přispěvek obdrží, se skládá ze dvou částí. První část je tvořena z poplatků, které uživatelé sítě přidají k transakcím, u kterých požadují prioritní

zpracování. Součet poplatků z těchto transakcí tvoří sumu, kterou obdrží těžař nebo správce poolu, který ji pak těžařům v podle předem stanovených pravidel rozdělí. Druhou částí odměny za nalezení nového bloku je bitcoin. V současné době (srpen 2019) je výše odměny za nalezený blok 25 bitcoinů, opakující se snížení odměny za nalezený blok se nazývá anglickým slovem „halving“, ke kterému dochází vždy po nalezení 210.000 nových bloků. Připsání odměny pro vítěže je provedeno formou speciální transakce, která se nazývá tzv. „coin creator“ transakce, vítězný těžař má právo ji přidat k ostatním transakcím do právě vytěženého bloku a adresovat ji jakémukoli uživateli v síti, typicky ji adresuje sám sobě. Rozdělení odměny mězi těžaře funguje obdobně jako v prvním případě, tedy pokud je těžařem jednotlivec, odměna náleží jemu, v případě že se jedná o pool, dělí odměnu správce. (10) (5) (11)

3.6.2.1 Solo mining

Solo mining je způsob těžby, při kterém těžař jako jednotlivec provádí výpočty za cílem nalezení správného hashe. Jednotlivcům se v dnešní době těžba nevyplácí, rentabilní pro ně bylo pouze období na počátku Bitcoinového protokolu, kdy pro nalezení nového bloku stačil výpočetní výkon poskytující bežný počítač, který v lepším případně obsahoval více současně zapojených grafických karet. Nyní se těžaři jednotlivci zpravidla shlukují do těžebních poolů, kde se o odměnu v podobě bitcoinů, kterou obdrží za vytěžení nového bloku dělí. Těžba bitcoinu vyžaduje kromě výkonného hardwaru znalosti týkající se fungování těžebních poolů, oproti nákupu bitcoinu se tedy jedná o složitější variantu. (7) (20)

Nejefektivnějším, ale zároveň nejnáročnějším způsobem těžby jednotlivců je zakládání tzv. těžebních farem. Jde o velká výpočetní centra s vysokým výkonem. Vystavět dostatečně výkonné výpočetní centrum je finančně velmi nákladné, může si jej tedy dovolit pouze společnost, nebo jednotlivec s velmi vysokým vstupním kapitálem. Podstatnou roli při stavbě takového výpočetního centra hraje množství elektrické energie potřebné k jeho provozu. Ta je položkou, kterou je nutné do nákladů zařadit. Některá centra v důsledku zvýšení cen energií musela v minulosti přerušit svůj provoz, protože se stávala nerentabilní. Pokud chce investor udržovat svoji těžební farmu

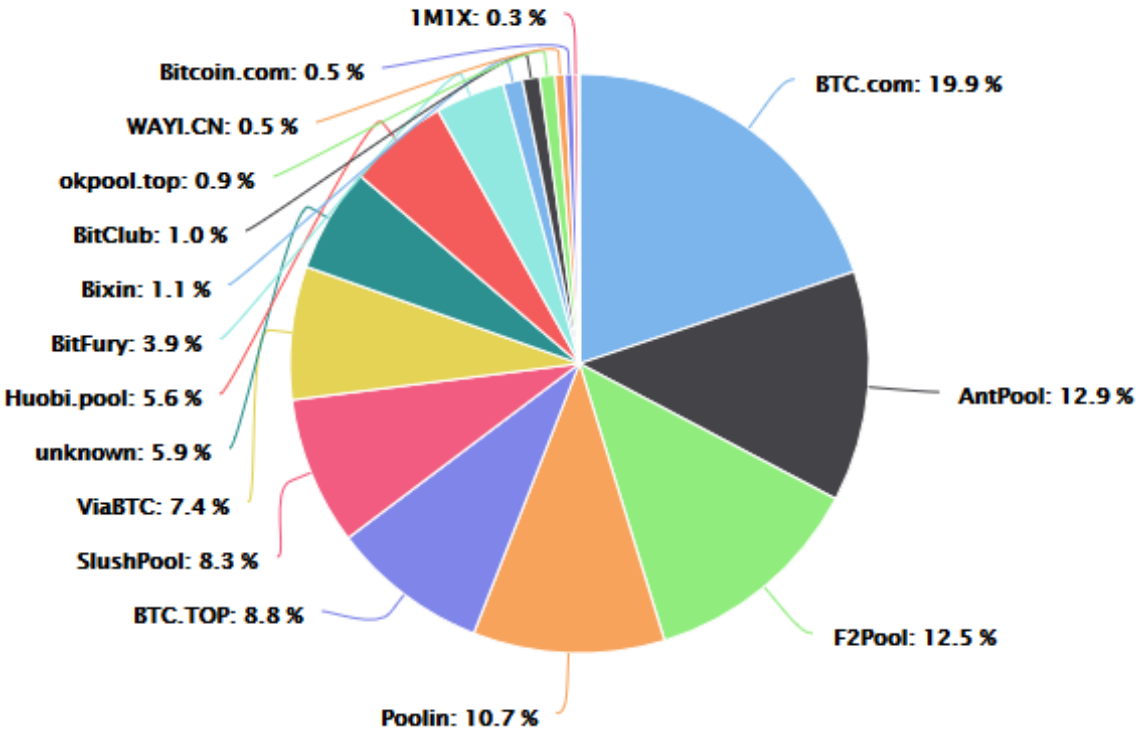
konkurenceschopnou, je třeba pravidelně obměnovat těžební stávající čipy za nejnovější modely. Vyřazený hardware se pak stává zátěží pro životní prostředí. (7) (20)

3.6.2.2 Pool mining

Mining pool je soubor agregovaných těžebních uzlů, které shromažďují společný výpočetní výkon do tzv. poolu. Docílí tím vyšší efektivity při řešení kryptografických úkolů, které je třeba pro nalezení nového bloku rozluštit. Pro dělbu odměny v poolu se používá mnoho pravidel, nejznáměnší z nich je tzv. proporční pool. V proporčním poolu je rozdělena odměna mezi těžare podle míry přispění k vyřešení hashe. Těžaři v poolu odesílají operátorovi poolu téměř dořešené bloky, tyto bloky se označují názvem kandidátní bloky. Složitost nalezení hashe kandidátního bloku je o něco nižší než nalezení validního bloku. Těžaři operátorovi poolu dokazují, že pracují na řešení prostřednictím odesílání kandidátních bloků, které se nazývají příspěvky, anglicky shares. Odměna pro těžaře je pak závislá na tom, kolik kandidátních bloků dokázal najít, (20) (6)

Na obrázku číslo 3 je zobrazeno rozvrzení hash kapacity napříč ming pooly v měsíci červenci roku 2019

Obrázek 3- Rozložení těžebních poolů



(Zdroj: Bitcoin.com)

3.6.2.3 ASIC mining

Současným trendem v těžbě je ASIC mining. ASIC je výraz vyjadřující anglickou zkratku application-specific integrated circouts. Jde o speciálně navržené a optimalizované čipy pro účely těžby virtuálních měn, které na trh začala uvádět již kolem roku 2013 společnost Butterfly Labs. Výpočetní rychlosti, kterých jsou ASIC čipy schopné dosáhnout, se pohybují v řádech stovek GH/s až jednotek TH/s, kdy je spotřeba elektrické energie přepočtená na GH/s u ASIC čipů výrazně nižší, než u CPU jednotek, které takových výkonů nedosahují. Silné konkurenční prostředí tlačí výrobce čipů k neustálému zrychlování těžebního hardwaru, předním výrobcem v roce je 2019 společnost Bitmain, která u svých výpočetních jednotek deklaruje rychlost až 14TH/s. (16) (5)

3.6.3 Rentabilita těžby

Nejrentabilnější období těžby virtuálních měn bylo na samotném počátku jejich vzniku. Za jejich vznikem nestála žádná silná korporace, která by rozvoj virtuálních měn marketingově podporovala. V počátcích tedy úspěch sítě závisel na důvěře těžařů v růst projektu. (6)

Úspěšnost těžby se odvýjí především podle množství výpočetního výkonu, který je těžar schopen vyvynout. Výpočetní výkon je v tomto případě nazýván Hash rate. Ten je jedním z klíčových atributů ovlivňujících efektivitu a rentabilitu těžby, může být definován jako množství výpočetních operací, které hardware provede za jednu sekundu. Pro dosažení prvenství v hledání správného hashe je třeba aplikovat hash šifru s různými vstupy opakovaně a co nejrychleji. Čím vyšší je hash rate, tím vyšší je šance na úspěšné nalezení správného hashe a získání odměny. Hash rate je měřen v jednotkách MH/s (megahashe za sekundu), GH/s (gigahashe za sekundu), nebo TH/s (terahashe za sekundu). (5)

Spotřeba elektrické energie je v problematice rentability těžby virtuálních měn atributem, který je třeba ještě před nákupem těžebního hardwaru pečlivě zvážit. Základem úspěšné těžby je dostatečný hash rate, ten dokáže poskytnout pouze výkonný hardware, který, ale spotřebuje značné množství elektrické energie. Před případnou investicí do koupi těžebního hardware je třeba propočítat, zda bude těžba rentabilní a obnos vynaložený na zaplacení spotřebované energie nižší nežli odměna. (5)

Při současné výpočetní složitosti zadání je třeba pro nalezení správného hashe vypočítat 10^{20} kombinací, s odměnou rovnající se 25 bitcoinům za každý nalezený blok. Odměna, jak již bylo uvedeno, se skládá z bitconu, který za nově nazelený blok těžař získá a transakčních poplatků, které jsou pridány k prioritním transakcím. Náklady na těžbu jsou dány pořizovací cenou těžěbního hardwaru a provozními výdaji (elektřina, chlazení atd.) Náklady obsahují fixní a variabilní složku. Koupě hardware tvoří fixní nákladovou položku, zatímco náklady na provoz těžebního hardwaru se mohou v závislosti na čase

měnit, rentabilita těžby je přitom ovlivněna především variabilními náklady. Cena elektřiny potřebné k napájení a chlazení těžebního hardwaru se mění, někdy i vícekrát v roce. Její růst jednoznačně zapříčiní snížení profitu. Dalším výrazným faktorem, kvůli kterému některé farmy pozastavily svoji činnost je propad kruzu bitcoinu. Výše odměny je v rámci jednoho cyklu (halvu) vždy stejná, poklesem kurzu bitcoinu se však při vysokých cenách energií může stát těžba nerentabilní. Faktorů, které je třeba brát v potaz je celá řada, nutností je rentabilitu průběžně s nejvyšší pečlivostí propočítávat. (11)

3.7. Bitcoin

Bitcoin je počítačový open source software fungující na síti architektury peer-to-peer založený roku 2008 osobu, či skupinou pod pseudonymem Satoshi Nakamoto, jehož identita je dodnes nejasná. Bitcoin vytváří svojí vlastní virtuální měnu, která se nazývá bitcoin. (7)

Bitcoin je v současné době nejznámější a nejrozšířenější virtuální měnou s nejvyšší tržní kapitalizací a nejvyšší cenou za jednu minci. Tržní kapitalizace bitcoinu v současné době (24. 11. 2019) dosahuje 129 miliardy dolarů, přičemž celková tržní kapitalizace všech virtuálních měn dohromady dosahuje 195 miliard dolarů. Bitcoin tedy dosahuje téměř 70 procent celkové kapitalizace. Situace se vzhledem k vysoké volatilitě virtuálních měn mění každý den. Bitcoinu však takto vysoká čísla v poměru k menším altcoinům zůstávají. Virtuální měnou s druhou nejvyšší tržní kapitalizací je Ethereum s 15 miliardami dolarů (24. 11. 2019), následováno XRP s 9,8 miliardami dolarů (24. 11. 2019). Vývoj ceny bitcoinu za poslední rok je zachycen na obrázku číslo 4. Celková křivka vývoje cenové hladiny Bitcoinu je zobrazena na obrázku číslo 4. (14)

Obrázek 4- Vývoj ceny virtuální měny bitcoin za poslední rok

(Zdroj: Investing.com)

Na obrázku číslo 4, který zachycuje změny cenové hladiny virtuální měny Bitcoin za poslední rok je možné pozorovat nárůst v první polovině letošního roku z původních hodnot pod hranicí 5000 dolarů za minci na letošní maximum nad hranicí 12500 dolarů, kterou Bitcoin překonal v letošním roce dvakrát, jednou v červnu a poté znovu v červenci. Od té doby cena mince pozvolně klesala k hranici 7500 dolarů.

Obrázek 5- Historický vývoj ceny virtuální měny Bitcoin

(Zdroj: Investing.com)

Na obrázku číslo 5 je zachycen vývoj cenové hladiny Bitcoinu od jeho počátku po listopad roku 2019. Mince bitcoinu se na počátku tohoto grafu, tj. roku 2013, obchodovala za 65 dolarů. S mírným výkyvem v roce 2014 spojuje první čtyři roky stagnace, kterou přerušuje prudký nárůst mezi roky 2017 a 2018, kdy Bitcoin dosáhl ATH ve výši 20000 dolarů.

3.7.1 Příčiny úspěchu Bitcoinu

Hlavním technologickým průlomem Bitcoinu bylo vyřešení problému tzv. dvojí útraty. Ten nastává, když se uživatel pokusí utratit stejný obnos dvakrát. Centralizované systémy umí poměrně jednoduše tento stav ošetřit. Transakce jsou zaznamenány v centrální databázi a další nové tranaskce jsou s původní databází porovnávány. Dvojí útrata je tak snadno identifikována a zamítnuta. V decentralizovaném systému neexistuje instituce, která by za kontrolu transakcí převzala odpovědnost. Tento problém byl vyřešen vznikem blockchainu. (6)

Dalšími faktory, které dělí Bitcoin od svých neúspěšných předchůdců jsou Open-source software, decentralizace, globálnost, rychlost přenosu a potvrzování transakcí, bezpečnost, flexibilita, spolehlivost a škálovatelnost. Dosažení kvalit v těchto oblastech zapříčinilo úspěšnost Bitcoinu oproti předchozím neůspěšných pokusů o vytvoření silné virtuální měny. (7)

3.7.2 Bitcoin vs klasický fin. systém

Vznik a následný rozvoj nové technologie virtuálních měn s sebou přináší mnoho výhod, např. ušetření lidské práce, snížení nákladů na provoz stávajícího finančního systému, ale i nástrah v podobě zneužívání virtuálních měn pro nelegální účely.

Bitcoin byl navržen tak, aby docházelo k co nejrychlejšímu zpracování a potvrzování transakcí za nízké nebo žádné poplatky. Odesílatel sám rozhoduje o tom, zda ke své transakci připojí transakční poplatek či nikoli. V případě, že poplatek přidá, priorita transakce roste a je zpracována rychleji. Někteří internetoví obchodníci neumožnují u plateb menších obnosů či mikrotransakcí provádět online platby kreditní kartou. Poplatek za platbu kartou je u mikroplateb pro obchodníky přílíš vysoký a online platba kartou se pro ně stává nerentabilní. Nabízí se využití virtuálních měn, u kterých není nutno za transakce platit poplatky. Zákazníkům by tedy díky technologii virtuálních měn bylo umožněno platit komfortně online. (7)

Bitcoin a další virtuální měny mohou v případě finančních krizí sloužit jako bezpečná volba pro uložení kapitálu. Při realizaci transakcí virtuálních měn nedochází ke kontrole výše přenášeného obnosu ze strany bank a státní správy. V síti nevystupuje třetí strana, která by svým chováním narušovala nebo kontrolovala finanční toky mezi uživateli a vybírala za jejich zpracování poplatky. V zemích, kde lidé nedůvěřují státní správě či bankovním institucím, mohou být virtuální měny východiskem k bezpečnému uložení finančních prostředků. (7)

Samotný provoz stávajících finančních institucí je velmi nákladný a množství lidské práce, kterou je třeba zaplatit, se s rostoucí mírou byrokracie neustále zvyšuje. Virtuální měny žádné nároky na lidskou práci nemají, náklady na provoz by se jejich rozšířením snížily. (7)

3.7.3 Platba Bitcoinem

Současný denní počet transakcí bitcoinu se v listopadu roku 2019 pohybuje mezi 250tis. a 350tis. transakcemi denně. Denní maximum počtu transakcí bitcoin zažil 14. 12. 2017, kdy se počet uskutečněných transakcí vyšplhal na 498 tisíc. Většina těchto transakcí je prováděna za spekulativním účelem, nikoli pro potřeby plateb za služby, nebo zboží. Procento spekulativních přesunů je v porměru k platbám nízké především z důvodu neochoty obchodníků zařazovat virutální měny mezi možnosti platby. Přestože někteří velcí obchodníci začali bitcoin jako měnu přijímat, např. Microsoft, Overstock nebo nepřímo Amazon je množství obchodníků, kteří bitcoin přijímají stále nízké. Z předních českých prodejců je možno jmenovat prodejce IT vybavení Alza.cz a.s., která bitcoin akceptuje. (7) (21)

Důvodů, proč obchodníci platby virtuálními měnami neakceptují je více. Proces verifikace transakce při platbě bitcoinem zabere v průměru 10 minut, to je v poměru k platebnímu systému VISA, u kterému zabere potvrzení transakce maximálně pár sekund dlouhá doba. Interval verifikace transakce je určen dobou vytěžení nového bloku, do kterého jsou transakce vloženy. (7)

Další překážkou je vysoká volatilita kurzu bitcoinu a virtuálních měn obecně . Kurzy virtuálních měn se mění často a někdy velmi razantně. Pro obchodníky to znamená komplikaci v podobě častého přepočítávání cen zboží či služeb v závislosti na změnách kurzu. Usilí, které by museli obchodníci pro udržování konzistentních cen zboží vzhledem ke změnám kurzu vynaložit, by pro ně znamenalo další finanční zátěž. Časté razatní změny kurzu navíc nutí prodejce nenechávat příchozí platby uložené ve virtuálních měnách, risk spojený s náhlým poklesem kurzu a následné ztráty tlačí obchodníky k okamžité směně virtuálních měn na klasické peníze. (7)

Vysoká cena za minci virtuální měny, obzvláště v případě bitcoinu může být pro zákazníka nakupujícího drobné statky nekomfortní. Cena jedné bitcoinové mince je zhruba 7000 dolarů (24.11.2019). Při nákupu zboží bežné denní spotřeby by byla výše částky potřebné pro platbu uvedena v řádu jednotek tisícin bitcoinu. Takové řády nejsou pro spotřebitele uživatelsky přívětivé. Přepočítání tak malé částky na dolary, nebo jinou měnu by mohlo spotřebitelům činit obtíže a odradit je tak od koupě. (7)

3.7.4 Investice a investiční strategie

Častým důvodem nákupu virtuálních měn jsou spekulace. Bitcoin je po prudkém růstu z konce roku 2017 a následném razantním propadu v počátku roku 2018 zajímavým tématem pro větší či menší investory a mainstreamová média. Zprávy, které média populaci poskytují, mohou přilákat nové potenciální investory, kteří uvěří přínosu a ideologii virtuálních měn a rozhodnou se investovat. (7)

Veřejnost, která vstupuje do světa virtuálních měn, se v mnohých případech rozhoduje o investicích právě na základě zpráv médií, která nejsou vždy seriózní, nebo se v problematice nedostatečně orientují. Technologie neznalí uživatelé, mohou snadno podlehnout vlivům těchto médií a nevhodně investovat. V reakci na ztráty investorů právě z přelomu roku 2017/2018 některá média omezila, nebo přímo zakázala reklamy na virtuální měny, příkladem může být sociální sít Facebook.(7)

Investovat do virtuálních měn lze v krátkodobém horizontu řádu několika hodin, nejvýše několika týdnů, nebo v dlouhodobém horizontu. Investice v dlouhodobém horizontu je nazývána anglickým slovem „hodl“ a bývá plánována na alespoň jeden rok. (5)

Krátkodobé investice jsou náročné na správně načasovaný nákup i prodej. Vzhledem k vysoké volitalitě virturálních měn je třeba věnovat pohybu kurzů neustálou pozornost a být připraven na změny reagovat s minimální odezvou. Správné nastavení Stop-lossu je jedním z klíčových bodů krátkodobých investic. Stop-lossem se rozumí nastavení krajní hranice poklesu kurzu, při které investor své fondy, nebo jejich část odprodá a akceptuje menší ztrátu jako prevenci, před jejím nárůstem. (5)

U dlouhodobých investic jsou krátkodobé fluktuace cen očekávaným jevem. Investor s nimi v případě dlouhodobých investic musí počítat a věnovat jim pozornost, zároveň by ho ale neměli od předem plánované strategie nijak odchýlit. Krátkodobé výkyvy nejsou v dlouhodobém horizontu významné, přesto je vhodné mít pro případ velmi prudkého propadu stop-loss nastaven. Kritické je u dlouhodobých investic správné načasování nákupu a zachování klidu při momentálním nepříznivém vývoji cen. (5)

Vhodnou stategií pro dlouhodobé investice je diverzifikovat fondy do více virtuálních měn najednou. I když se jedná o jeden komoditní sektor a virtuální měny, co se týče vývoje kurzu často reagují stejně. Je možné nalézt vyjímky, které na růst ostatních virtuálních měn nereagují, nebo jejich cena začně klesat. Pro zvýšení šance na úspěšnou investici je vhodné diversifikovat minimálně do dvou virtuálních měn zároveň. (5)

3.7.5 Možnosti uložení Bitcoinu

Možné způsoby uchování Bitcoinu se různí především ve formách uložení privátních klíčů. Zodpovědnost za jejich zabezpečení je v některých případech delegována na zprostředkovatele, v jiných si za bezpečné uložení klíče ručí vlastník peněženky sám. Další pojem, který s uložením Bitcoinu úzce souvisí je adresa peněženky.(6) (10)

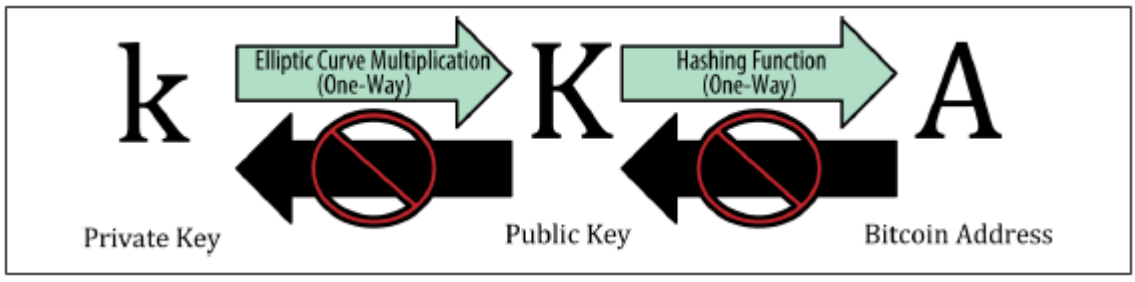
3.7.5.1 Adresa peněženky

Pro identifikaci uživatelů v rámci sítě slouží adresa peněženky, neboli Bitcoinová adresa. Jedná se o jedinečný řetězec znaků, který identifikuje uživatele pro účely odesílání, nebo příjmu bitcoinu. Je generována z veřejného klíče pomocí jednocestné hash funkce a skládá se z čísel a znaků abecedy, vždy však začíná číslem 1. Svou bitcoinovou adresu nemusí uživatel držet v tajnosti, při odeslání tranaskce do sítě je adresa součástí transakce a všechny uzly, které ji validují, adresu uvidí. Jedinečnost adresy zaručuje, že v síti nebudou vystupovat dva uzly se stejnou bitcoinovou adresou. (6) (10)

3.7.5.2 Bitcoinové peněženky

Software, který umožnuje uživateli hospodařit s virtuální měnou se nazývá peněženka. Termín peněženka je v tomto kontextu poněkud zavádějící, ve skutečnosti se totiž přímo v peněžence žádný bitcoin nenachází, je uložen v blockchainu. Peněženka pouze umožnuje realizaci transakcí. Bitcoinové peněženky kromě bitcoinu uchovávají dva druhy klíčů, privátní a veřejný klíč. Privátní klíč je řetězec sloužící pro ověření identity vlastníka peněženky před odesláním transakce do sítě, je jedinečný a vlastník peněženky se jeho vyzrazením vystavuje riziku odcizení peněženky. Vztahy mezi privátním klíčem, veřejným klíčem a bitcoinovou adresou je možno vidět na obrázku číslo 6. (10) (6) (20)

Obrázek 6- Bitcoinová adresa, privátní a veřejný klíč



(Zdroj: Antonopulos)

Privátní klíč je generované náhodné číslo, které by měl uživatel uchovávat v tajnosti. Na privátní klíč je aplikována jednocestná kryptografická metoda šifrování klíčů

elliptic curve multiplication, pomocí níž je vygenerován klíč veřejný. Z veřejného klíče je pak možné pomocí hash funkce vygenerovat adresu peněženky. (10)

Privátní klíč, opravňující vlastníka peněženky k realizaci transakcí, musí zůstat tajný. Vyzrazením, nebo ztrátou privátního klíče se vlasník peněženky vystavuje riziku zcizení fondů, nebo zamezení přístupu k nim. V případě odhalení privátního klíče je majitel vystaven neoprávěnému nakládání s jeho peněženkou třetí stranou, která získá neomezeou kontrolu nad peněženkou poškozeného uživatele a může převést fondy do peněženky, kterou sama vlastní. Ztrátou privátního klíče se vlastník peněženky vystavuje riziku zamezení přístupu ke své peněžence. Obnos sice zůstává stále uložen v blockchainu, ale bez privátního klíče s ním nebude možné provést žádnou operaci a považuje se tak za ztracený. (6) (10)

Pro uchování privátního klíče lze využít fyzické médium – např. flashdisk.Výhoda uchovávání klíčů na fyzických médiích je zamezení přístupu k privátnímu klíči z vnějšího internetu. Tento způsob uložení privátnho klíče se nazývá cold storage. Klíč takto uložený sice není ohrožen online útoky z vnější sítě, zato je vystaven riziku fyzického odcizení média na kterém je uložen. Takto uchovávaný klíč je třeba proti fyzickému odcizení řádně a pečlive zapezpečit. (6)

Média, která lze jako cold storage použít jsou například flash disky, optické disky, nebo paměťové karty. Na médium je uložen privátní klíč, který je vyžadován pouze v případě realizace transakce. Offline uložený privátní klíč se naimportuje do online klienta, tím vlastník peněženky autorizuje transakci, která je vyslána do sítě. Slabé místo nastává ve chvíli importu klíče do online klienta, kdy by mohl online útočník privátní klíč odhalit a následně zneužít. (6)

Dalším způsobem uložení privátního klíče na cold storage je tisk na papír. Takto vzniklé peněženky se nazývají paper-wallers. Na papíru je vytištěn privátní klíč, veřejný klíč a adresa schránky. Tyto údaje se tisknou pomocí generovaného QR kodu. Bezpečnost uložení takto zaznamenaného privátního klíče závasí především na fyzickém zabezpečení a uskladnění papírové peněženky. Stejně jako u flash disků a dalších offline médií, se

vlastník vystavuje riziku odcizení ve chvilí importu privátního klíče do online klienta při autorizaci platby. (6)

3.7.5.3 Hardwarové peněženky

Hardwarové peněženky jsou speciální zařízení pro cold storage uložení privátních klíčů, které jsou schopné autorizovat transakce offline. Nedochází tedy k importu privátního klíče do online klienta. Odpadá tak riziko napadení škodlivým malwarem během importu. (6) (17)

Online klient v tomto případě vystupuje pouze jako prostředník při komunikaci mezi blockchainem a peněženkou. Transakce jsou zasílány z online klienta do hardwarové peněženky, která je připojena k počítači nejčasteji pomocí USB portu. Hardwarová peněženka pak navrací potvrzenou transakci stejnou cestou, jako žádost o potvrzení transakce přišla. Hardwarové peněženky běžne obsahují malý displej, zobrazující uživateli podrobnosti o transakci a tlačítka umožnující potvrzení nebo zamítnutí transakce. Běžně je pro potvrzení transakce také nutné do HW pěneženky vyplnit přednastavený PIN kod. (6)

3.7.5.4 Webové peněženky

Webové peněženky, nebo také hosted wallets, případně cloud wallets, umožnují uživatelům uložit svoje fondy prostřednictvím zprostředkovatele. Peněženka vzniká na straně zprostředkovatele, který přebírá odpovědnost za její zabezpečení. Uživatelé k webovým peněženkám přistupují pomocí webového prohlížeče, nebo aplikací na svých mobilních telefonech. (6)

Mezi hlavní výhody webové peněženky patří především velmi rychlé a snadné zřízení peněženky. Vstupní bariéra pro začínající uživatele je díky tomuto způsobu uložení bitcoinu značně snížena. Výhodou, ale zároveň možným rizikem je správa privátního klíče zprostředkovatelem. Vlastníkům peněženek odpadá starost o bezpečné uložení privátního klíče, což může být pro některé nezkušené uživatele žádoucí. Ve výběru způsobu zabezpečení privátních klíčů důvěřují metodě, kterou zvolil zprostředkovatel. Kvalita

zabezpečení privátních klíčů ze strany zprostředkovatelů se různí a je třeba pečlivě vybírat. Webová peneženka je vhodná zejména pro zprostředkování každodenních transakcí. Pro zadržování většího obnosu je vhodné zřídit cold storage tak, jak bylo popsáno v předchozích kapitolách. (6)

Z uživatelského hlediska se prostředí webové peněženky velmi často podobá aplikacím internetového bankovnictví. Jedná se však pouze o podobnost, na rozdíl od bankovnictví, není bezpečná manipulace s účtem nijak pojištěna. Zprostředkovatelem webových peněženek se může stát kdokoli, vstup na trh tedy není nijak regulován a je třeba dobře rozmyslet, který zprostředkovatel je dostatečně důvěryhodný. (6)

3.7.5.5 Hybridní peněženky

Hybridní webové peněženky jsou takové, u kterých je privátní klíč uložen v počítači uživatele, ale jeho obsluha je spravována softwarem zprostředkovatele. Výhodou je částečné zatajení dat před zprostředkovatelem. Nevýhodou pak, že na uživatele přechází veškerá zodpovědnost za zabezpečení privátního klíče. (6)

3.8. Další významné virtuální měny

Nové virtuální měny, tzv. altcoiny díky oblíbenosti Bitcoinu a dalších velkých virtuálních měn vznikají díky neexistenci regulací každý den, jejich celkový počet je odhadován na zhruba dva tisíce. Větší úspěchy však zažívá jen velmi malé procento z nich. Jak bylo zmíněno, úspěch, či neúspěch virtuální měny závisí především na důvěře investorů v technologii, na které je měna založená. Mezi hlavní konkurenty Bitcoinu, co se týče celkové tržní kapitalizace lze v současné době (Září 2019) zařadit Ethereum, XPR a Litecoin.

3.8.1 Ethereum

Ethereum je poměrně mladá virtuální měna, která vznikla v roce 2015 a od počátku se těšila značné přízni ze strany uživatelů. Token Etherea se nazývá Ether. Vznikla na

open-source platformě, která je stejně jako Bitcoin založena na distribuované databázi blockchainu. V době psaní této práce (Listopad 2019) zaujímá druhou příčku v pořadí tržní kapitalizace virtuálních měn za Bitcoinem s celkovou tržní kapitalizací 15,9 miliard dolarů. Technologie Etherea se v mnohém podobá technologii Bitcoinu, některé vylepšení přesto přináší. Nejvýznamnější z nich je smart contracts. Ethereum jako první přineslo kompletní skriptovací jazykovou sadu a koncept virtuálního stroje Ethereum virtual machine (EVM). Konsenzu je v současné době dosahováno podobně jako u Bitcoinu pomocí mechanismu proof of work, vizí blízké budoucnosti je však změna na mechanismus proof of stake. Důvodem, je zefektivnění současného modelu rozšiřování blockchainu. Vývoj kurzu Etherea za poslední rok od 19. listopadu je možné vidět na obrázku číslo 7 převzatého z webu Investing.com. Cena Etherea se v posledním roce pohybuje okolo hranice 200 dolarů za minci s maximem ve výši 360 dolarů. Nejvyšší cena (tzv. ATH) za minci Etherea od jeho vzniku byla 1 432 dolarů z ledna roku 2018. (14)

Obrázek 7- Vývoj ceny virtuální měny Ethereum za poslední rok

(Zdroj: Investing.com)

Z obrázku číslo 7 je patrný znatelný nárůst v polovině letošního roku z původních zhruba 120 dolarů na hodnoty v okoli 370 dolarů, kde se však Ethereum udrželo pouze krátkou dobu. Jedná se o podobný průběh jako ten co byl pozorován na obrázku číslo 4, který zachycoval roční vývoj ceny Bitcoinu.

3.8.1.1 Ethereum Virtual machine

Ethereum virtuál machine si lze představit jako decentralizovaný kompletní turingovský stroj, který je v rámci platformy využíván pro zpracování smart contracts. Při jednoduché výměně transakcí mezi dvěma uživateli není EVM nijak využíváno. V ostatních případech, kdy komunikuje účet externího vlastníka se smart contractem je zpracování pomocí EVM vyžadováno. Z velmi abstraktního pohledu si lze EVM představit jako globální decentralizovaný počítač obsahující velké množství zpracovatelných objektů s vlastním trvalým datovým úložištěm. (5)

3.8.1.2 Smart contracts

Každý uživatel v sítí může za malý poplatek vytvořit smart contract vložením programového kódu v bytecodu do speciální transakce. Smart contract je posléze zpracován EVM a připojí se do blockchainu. Smart contract nemají žádný privátní klíč určený k autorizaci transakce, řídí se sami na základě predeterminovaného chování, které je určeno kódem, který je i s datovým uložištěm obsahem smart contracts. (10) (11)

3.8.1.3 GAS

Každou výpočetní operaci je před jejím zpracovávaním prostřednictvím Ethereum virtual machine třeba nejprve vykrýt jednotkou zvanou Gas, nebo také crypto fuel. Některé smart contracts mohou vzhledem k možnému využití smyček vytěžovat EVM příliš dlouho. Aby bylo možné takový smart contract ve využívání EVM omezit, je za každou funkci v rámci platformy placeno Gas. Každou transakci, musí uživatel, který ji vytvořil uhradit předem. Základní operace v rámci smart contract jako přičítání, nebo porovnání stojí 1 Gas, se složitostí operace potřebné množství GAS stoupá. Pokud v průběhu zpracování dojde předplacený GAS, je zpracování přerušeno a operace vykonávající transakcí se vrací na začátek. Případný nadbytečný GAS po zpracování všech operací umístěných v transakci je navrácen uživateli, který transakci vytvořil. (5)

3.8.2 Ripple

Virtuální měnou s třetí nejvyšší tržní kapitalizací na počátku listopadu 2019 je Ripple (XPR) s 9,8 miliardy dolarů. Ripple byl založen v roce 2012 firmou Ripple lab, jejíž záměrem bylo vytvořit velmi rychlou platební sít, na které by bylo možné provádět platby a přenášet transakce mezi uživateli bez poplatků. Pro účely výměny transakcí mezi uživateli byla vytvořena sít RippleNet a distribuovaný spojový seznam Ledger, který funguje podobně jako výše zmíněný blockchain. Vývoj kurzu Ripple za poslední rok je možné vidět na obrázku číslo 8. Nejvyšší hodnoty v uplynulém roce (4. 11. 2018-4. 11. 2019) dosáhl ripple počátkem listopadu loňského roku, kdy cena jedné mince ripple dosahovala 0,56 dolaru. Dosavadní ATH ripple je 3.84 dolaru za minci. (14)

Obrázek 8- Vývoj ceny virtuální měny Ripple za poslední rok

(Zdroj: Investing.com)

Průběh vývoje cenové hladiny XPR zachycený na obrázku číslo 8 podobně jako v případě Etherea a Bitcoinu dosahoval letošní maximální hranice v červenci. Ke konci roku stejně jako Ethereum a Bitcoin pomalu klesá.

3.8.3 Litecoin

Další významnou virtuální měnou, s rokem vzniku 2011 je Litecoin. Za vznikem této virtuální měny založené na open source software stojí bývalý zaměstnanec společnosti Google Charles Lee. Litecoin zabírá v žebříčku tržní kapitalizace v listopadu 2019 šestou příčku s celkovou hodnotou 3,1 miliardy dolarů. Stejně jako ostatní hlavní virtuální měny

je Litecoin založen na principu decentralizovaného blockchainu. Někdy je považován za mladšího bratra Bitcoinu z důvodu podobnosti těchto virtuálních měn. Litecoin totiž vznikl ze zdrojového kódu Bitcoinu. (22)

Výhody, které sebou Litecoin na oproti většímu Bitcoinu přináší je vícero. Celkové množství mincí Litecoinů je rovno 84 milionům, tedy zhruba čtyřikrát více nežli Bitconu. Doba těžby jedné mince je oproti staršímu Bitcoinu kratší také zhruba čtyřikrát. Průměrná doba těžby bloku Litecoinu je stanovena na dvě a půl minuty. (22) (23)

Nejvyšší hodnota za jednu minci dosáhl Litecoin devatenáctého prosince roku 2017, kdy byla její cena ustálila na 375,29 dolarech. Průběh vývoje kurzu Litecoinu za poslední rok je zobrazen na obrázku číslo 9. (23)

Obrázek 9- Vývoj ceny virtuální měny Litecoin za poslední rok

(Zdroj: Investing.com)

Průběh vývoje ceny Litecoin na obrázku číslo 9 opakuje vzorec vypozorovaný z předchozích ročních průběhů virtuálních měn Bitcoin, Ethereum a Ripple. Maxima bylo dosaženo postupným nárůstem na přelomu června a července letošního roku s následným postupným klesáním stejně, jako tomu bylo u ostatních virtuálních měn.

Z průběhů jednotlivých cenových hladin virtuálních měn za poslední rok lze usoudit, že virtuální měny jako sektor v případě cenových výkyvů reagují stejně, tedy navzájem korelují. Přesná míra korelace mezi virtuálními měnami vzájemně a korelací s komoditami jiných sektorů bude předmětem korelační analýzy v praktické části této diplomové práce.

4. Empirická část

Časovou řadu lze definovat jako posloupnost hodnot ukazatelů, měřených v rovnoměrných časových intervalech. V rámci praktické části této práce bude analyzován dosavadní průběh vývoje ceny virtuální měny Bitcoin. Pro zachycení dynamických pohybů je třeba zajistit dostatečně dlouhou časovou řadu. Ekonomické časové řady je možno dělit z hlediska intervalu na dlouhodobé a krátkodobé. Toto dělení je důležité především kvůli jejich členění. Dlouhodobé časové řady jsou sledovány v ročních či delších časových úsecích. Krátkodobé časové řady se pak sledují v kratších úsecích, nežli je jeden rok. Dalším možným dělením časových řad je dělení dle charakteru ukazatele na okamžité, nebo intervalové a podle druhů ukazatele na absolutní a odvozené. (24)

Okamžikové měření ukazatele se vztahují ke konkrétnímu okamžiku, kdežto intervalové měření poskytuje například informace o tom, jak vysoké byly náklady na provoz automobilu minulý měsíc. Jedná se tedy o souhrnnou hodnotu za určité období. Absolutní ukazatelé reprezentují konečné očištěné hodnoty, zatímco odvozené ukazatele mohou být vyjádřeny součtem jiných ukazatelů, nebo jejich poměrem. (25)

Časová řada vývoje kurzu virtuální měny Bitcoin, která bude použita pro vypracování ekonomické prognózy je dlouhodobého charakteru s denním pozorováním v okamžitých hodnotách. Jedná se o denní pozorování za poslední rok a půl, tj. od 1. 5. 2018 do 1. 11. 2019. Data byla čerpána z webu Investing.com, který denní data kurzu virtuální měny Bitcoin poskytuje. Pro účely modelování prognózy je třeba otestovat časovou řadu na stacionaritu. Sestavení modelu ARMA je možné pouze za předpokladu stacionarity časové řady, pokud by tedy výchozí časová řada stacionární nebyla, bude třeba data upravit. (26)

4.1. ARMA model

Před odhadem samotné prognózy je nejprve třeba upravit podkladová data ve formě časových řad do podoby vhodné pro ekonometrické modelování. Jednotlivé fáze úprav časové řady budou popsány v následujících odstavcích.

Časovou řadu lze dle ekonomické analýzy dekomponovat na čtyři složky, tj. trendová, cyklická, sezonní a náhodná složka. Trendová složka udává směr časové řady v dlouhodobém horizontu, je výsledkem působení faktorů v dlouhodobém hledisku. Cyklická složka naopak vyjadřuje kolísání okolo trendů, které je zapříčiněno ekonomickými i neekonomickými faktory. Cykly mají obvykle nepravidelný charakter a lze je zpravidla na období delších nežli jeden rok. Sezonní složka časové řady má na rozdíl od cyklické pravidelný charakter, kolísání se objevuje opakovaně každý rok v určitém období. Sezonní vlivy jsou určovány především ročním obdobím, národnostními zvyklostmi, svátky atd. Náhodná složka obsahuje všechny nesystematické a nahodilé jevy. (24)

4.1.1 Box-Jenkinsnova metodologie

Lineární stochastické modely jsou nejjednodušší modely vystihující chování finančních časových řad. Pro tvorbu těchto modelů se využívá tzv. Box-Jenkinsnovi metodologie, která považuje za základní prvek konstrukce modelu reziduální složku časové řady. Časová řada je v rámci využití této metodologie analyzována podle předem jasně stanového postupu. Jako první je třeba model identifikovat, následně odhadnout parametry modelu a na závěr model verifikovat. Klíčovou vlastností časové řady pro potřeby její analýzy je stacionarita. (27)

4.1.2 Vyhlazení a Stacionarizace časové řady

Stacionarita časové řady vystihuje, zda je její průběh v stochasticky ustálený. Stacionaritu je možné rozdělovat na slabou, a striktní. Striktní stacionaritu lze jednoznačně určit tak, že její rozdělení pravděpodobnosti je v čase neměnné. Slabá stacionarita má průměr a rozptyl konstantní, přičemž kovariance libovolných dvou pozorování časové řady závisí pouze na velikosti zpoždění. (27) (28)

„Chování časové řady může ze statistického hlediska buď podléhat změnám v průměru či variabilitě (řada nestacionární), nebo být stále stejná (řada stacionární). Zhruba

řečeno to znamená, že u stacionární řady nejsme schopni na základě zjištěných statistických parametrů, jako jsou aritmetický průměr hodnot nebo jejich rozptyl, schopni odlišit jeden úsek řady od druhého. Nestacionární řada naopak vykazuje změny v chování: například aritmetický průměr hodnot ze začátku řady je signifikantně jiný než průměr členů na konci (o takové řadě říkáme, že vykazuje trend).“ (25)

Pro potřeby sestavení ekonometrického modelu dle Box-Jenkinsovi metodologie je nejprve třeba vstupní časovou řadu upravit. Jelikož se jedná o časovou řadu s délkou přesahující jeden rok, je třeba ji očistit od sezonních a dalších cyklických faktorů. Pro vyhlazení původní časové řady byl použit statistický počítačový software Statistica. Konkrétní metoda, která byla na data aplikována, se nazývá exponenciální vyhlazování. Rozdíl mezi vyhlazenými daty a původní časovou řadu je zachycen na obrázku číslo 10, kde křivka vyobrazená modrou barvou představuje původní časovou řadu a červená barva časovou řadu zbavenou sezonních vlivů.

Obrázek 10- Průběh původní a vyhlazené časové řady

(Zdroj: Vlastní práce)

Před sestavením samotného modelu je nutné u vyhlazených dat testovat jejich stacionaritu. Nejspolehlivější prognózu získáme právě tehdy, pokud budou data stacionární. Testování stacionarity časové řady se provádí za pomoci testů jednotkových kořenů. Pro testování jednotkových kořenů v této práci bude využita rozšířená verze Dickey-Fullerova testu.

Nejprve byla na stacionaritu testována vyhlazená vstupní data. Pro potřeby testování stacionarity byl rozšířen vstupní soubor dat o vyjádření očištěné časové řady v prvních diferencích. Rozšířený Dickey-fullerův test jednotkového kořene byl nejprve aplikován na nediferencovanou časovou řadu. Nulová hypotéza v případě rozšířeného ADF testu zní, že časová řada je nestacionární. Kritická testovací hladina je v případě tohoto testu 0,05.

$$p - hodnota \geq 0{,}05 \; = nestacionarita$$

Výsledky ADF testu jsou znázorněné na obrázku číslo 11.

Obrázek 11- Test jednotkového kořene nedif. čas. řady

```
Rozšířený Dickey-Fullerův test pro KurzBTCocisteno
testing down from 1 lags, criterion AIC
počet pozorování 536
nulová hypotéza jednotkového kořenu: a = 1

  s konstantou a trendem
  s použitím jedné zpožděné proměnné (1-L)KurzBTCocisteno
  model: (1-L)y = b0 + b1*t + (a-1)*y(-1) + ... + e
  odhadovaná hodnota (a - 1): -0,00169032
  testovací statistika: tau_ct(1) = -2,73395
  asymptotická p-hodnota 0,2227
  autokorelační koeficient 1. řádu pro e: -0,004
```

(Zdroj: Vlastní práce)

Výsledná p hodnota tohoto testu se rovná 0,227. Kritická testovací hranice p hodnoty je rovna 0,05. Z testu je patrné, že p hodnota překračuje povolenou mez. Nulovou hypotézu, tj. že testovaná data jsou nestacionární v tomto případě přijímáme. Data v této podobě nejsou stacionární a neposkytly by kvalitní podklady pro tvorbu ekonometrického modelu. Časovou řadu je tedy nutno převést do prvních diferencí a znovu testovat za pomoci ADF testu. Výsledky ADF testu s časovou řadou v prvních diferencích je možné vidět na obrázku číslo 12.

Obrázek 12-Test jednotkového kořene diff.. čas. řady

```
Rozšířený Dickey-Fullerův test pro d_KurzBTCocisteno
testing down from 1 lags, criterion AIC
počet pozorování 536
nulová hypotéza jednotkového kořenu: a = 1

  s konstantou a trendem
  s použitím 0 zpožděných proměnných (1-L)d_KurzBTCocisteno
  model: (1-L)y = b0 + b1*t + (a-1)*y(-1) + e
  odhadovaná hodnota (a - 1): -0,068473
  testovací statistika: tau_ct(1) = -4,30085
  p-hodnota 0,003349
  autokorelační koeficient 1. řádu pro e: 0,006
```

(Zdroj: Vlastní práce)

Na základě výsledků plynoucích z dat na obrázku číslo 12 lze v tomto případě nulovou hypotézu zamítnout. P-hodnota je v tomto případě rovna 0,00339, což je nižší hodnota, než je kritická testovací mez 0,05. Přehledné výsledky obou testů jsou uvedeny v tabulce číslo 2.

Tabulka 2- Výsledky ADF testu

	p-hodnota	Kritická hodnota	Stacionarita
Vyhlazená časová řada	0,227	0,05	Ne
Vyhlazená časová řada v prvních diferencích	0,03349	0,05	Ano

(Zdroj: Vlastní práce)

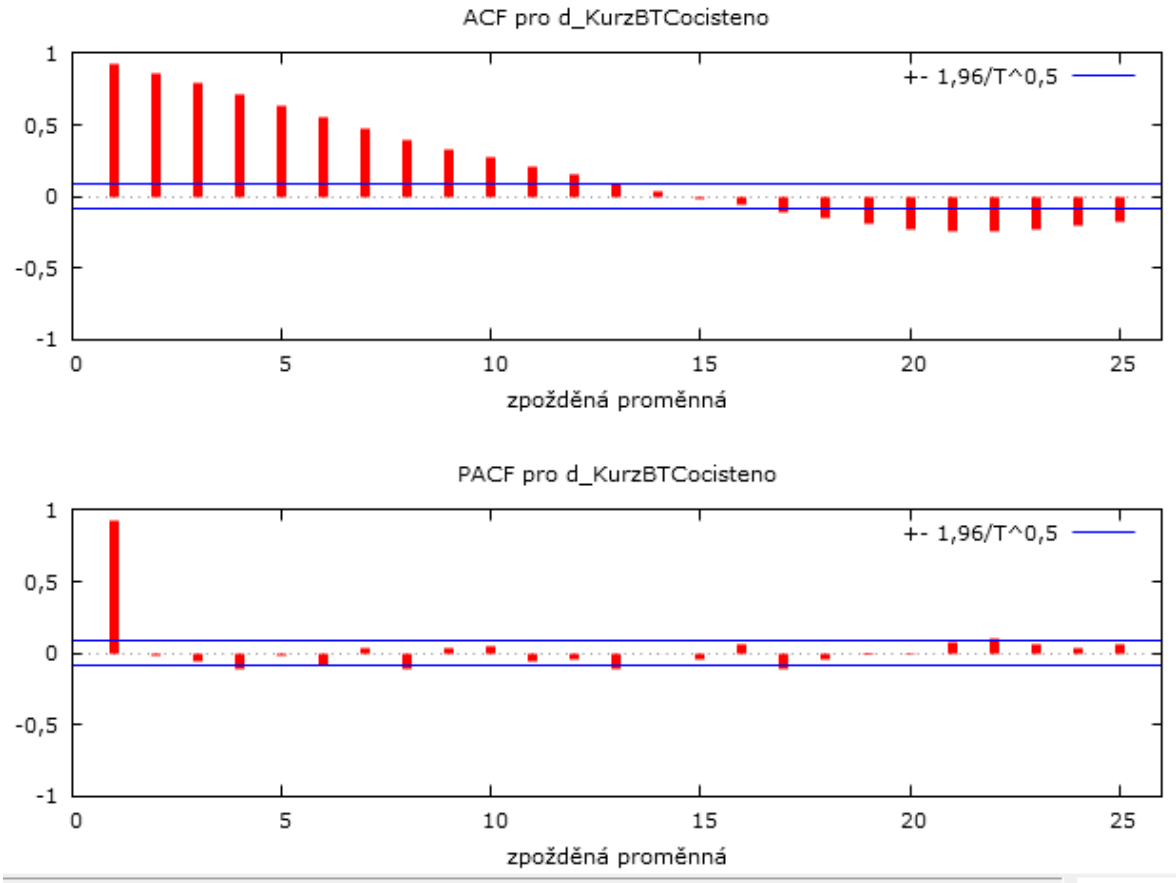
Data jsou dle výsledků rozšířeného Dickey-Fullerova testu stacionární po převedení do prvních diferencí. Pro potřeby určení řádu zpoždění ARMA modelu budou využita v této stacionární podobě.

4.1.3 Identifikace a odhad modelu ARMA

Dle Box-Jenkinsovi metodologie je nejprve třeba model identifikovat. Identifikace modelu bude v této práci provedena za pomoci korelogramu, který vykresluje průběh autokorelační (AFC) a parciálně autokorelační funkce (PAFC). Tyto korelogramy mohou být nápomocné pro identifikaci případné korelace mezi jednotlivými pozorováními časové řady. Pokud nebudou data předem uvedena do stacionární formy, bude z průběhu

korelogramu patrná silná korelace mezi pozorováními. Průběh a číselné hodnoty autokorelační a parciálně korelační funkce je vyobrazen na obrázcích 13 a 14.

Obrázek 13- Průběh AFC a PAFC



(Zdroj: Vlastní práce)

Obrázek 14- Číselné vyjádření AFC a PAFC

```
Autokorelační funkce pro d_KurzBTCocisteno
***, **, * indicate significance at the 1%, 5%, 10% levels
using standard error 1/T^0,5

  zpoždění      ACF           PACF          Q-stat. [p-hodnota]

    1    0,9296  ***   0,9296 ***     466,6076  [0,000]
    2    0,8620  ***  -0,0152         868,6220  [0,000]
    3    0,7906  ***  -0,0644        1207,4166  [0,000]
    4    0,7096  ***  -0,1116 ***    1480,8783  [0,000]
    5    0,6319  ***  -0,0255        1698,1566  [0,000]
    6    0,5484  ***  -0,0869 **     1862,1076  [0,000]
    7    0,4762  ***   0,0323        1985,9407  [0,000]
    8    0,3948  ***  -0,1157 ***    2071,2074  [0,000]
    9    0,3251  ***   0,0315        2129,1544  [0,000]
   10    0,2701  ***   0,0510        2169,2267  [0,000]
   11    0,2108  ***  -0,0634        2193,6770  [0,000]
   12    0,1547  ***  -0,0517        2206,8745  [0,000]
   13    0,0902  **   -0,1144 ***    2211,3652  [0,000]
   14    0,0349       -0,0007        2212,0373  [0,000]
   15   -0,0200       -0,0419        2212,2580  [0,000]
   16   -0,0617        0,0565        2214,3746  [0,000]
   17   -0,1085  **   -0,1108 **     2220,9224  [0,000]
   18   -0,1560  ***  -0,0415        2234,4993  [0,000]
   19   -0,1941  ***  -0,0092        2255,5550  [0,000]
   20   -0,2291  ***  -0,0066        2284,9345  [0,000]
   21   -0,2449  ***   0,0691        2318,5752  [0,000]
   22   -0,2439  ***   0,0945 **     2352,0116  [0,000]
   23   -0,2308  ***   0,0594        2382,0001  [0,000]
   24   -0,2098  ***   0,0343        2406,8273  [0,000]
   25   -0,1797  ***   0,0655        2425,0880  [0,000]
```

(Zdroj: Vlastni práce)

Z průběhu autokorelační a parciálně autokorelační funkce je zřejmé, že data nejsou nijak významně korelována. Na základě grafického průběhu a číselného výstupu AFC a PAFC je třeba zvolit zpoždění AR a MA procesů s co nejvyšší statistickou signifikancí. Výběrem správných zpoždění bude dosaženo nejpřesnějšího možného modelu. Z výstupu je zřejmé, že lze odvodit hned několik vhodných kombinací AR a MA procesů. Po simulaci jednotlivých zpoždění ve statistickém software Gretl byly zvoleny procesy se zpožděním AR (8) a MA (8), jelikož je jejich statistická signifikance největší.

V tomto kroku byla provedena identifikace modelu dle Box-Jenkinskovi metodologie. Data byla očištěna od sezonní složky a stacionarizována způsobem převedení na postupné diference prvního řádu. Identifikace modelu byla provedena v prostředí

statistického software Gretl na základě korelogramů dat upravených dle zmíněných postupů. Jako nejvhodnější byl zvolen model s řádem zpoždění AR (8) MA (8).

Odhad modelu je druhým krokem, který Box-Jenkinsova metodologie specifikuje. Byl proveden taktéž v prostředí Gretl. Výsledný model je zobrazen na obrázku číslo 15.

Obrázek 15- Model ARMA

```
Vyhodnocování funkce: 254
Vyhodnocování gradientu: 64

Model 3: ARMA, za použití pozorování 2018-05-02:2019-10-20 (T = 537)
Estimated using AS 197 (přesné ML)
Závisle proměnná: d_KurzBTCocisteno
Směrodatné chyby založené na Hessiánu

             koeficient   směr. chyba       z       p-hodnota
  ------------------------------------------------------------
  const      -0,263710    11,6941        -0,02255   0,9820
  phi_1       1,92882      0,0758576     25,43      1,27e-142 ***
  phi_2      -1,40502      0,154895      -9,071     1,18e-019 ***
  phi_3      -0,333606     0,171412      -1,946     0,0516    *
  phi_4       1,39166      0,145556       9,561     1,17e-021 ***
  phi_5      -0,229681     0,164633      -1,395     0,1630
  phi_6      -1,30062      0,178784      -7,275     3,47e-013 ***
  phi_7       1,62398      0,141355      11,49      1,50e-030 ***
  phi_8      -0,732361     0,0616406    -11,88      1,48e-032 ***
  theta_1    -1,01399      0,0889178    -11,40      4,01e-030 ***
  theta_2     0,563024     0,112402       5,009     5,47e-07  ***
  theta_3     0,803507     0,104809       7,666     1,77e-014 ***
  theta_4    -0,760004     0,128274      -5,925     3,13e-09  ***
  theta_5    -0,202946     0,150517      -1,348     0,1776
  theta_6     0,875618     0,129678       6,752     1,46e-011 ***
  theta_7    -0,792862     0,0997241     -7,951     1,86e-015 ***
  theta_8     0,0238062    0,0593744      0,4010    0,6885

  Střední hodnota závisle proměnné    -1,544877
  Sm. odchylka závisle proměnné        89,60893
  Střední hodnota inovací             -0,031500
  Sm. odchylka inovací                 31,08565
  Koeficient determinace               0,879437
  Adjustovaný koeficient determinace   0,875966
  Logaritmus věrohodnosti             -2610,280
  Akaikovo kritérium                   5256,559
  Schwarzovo kritérium                 5333,707
  Hannan-Quinnovo kritétium            5286,739
```

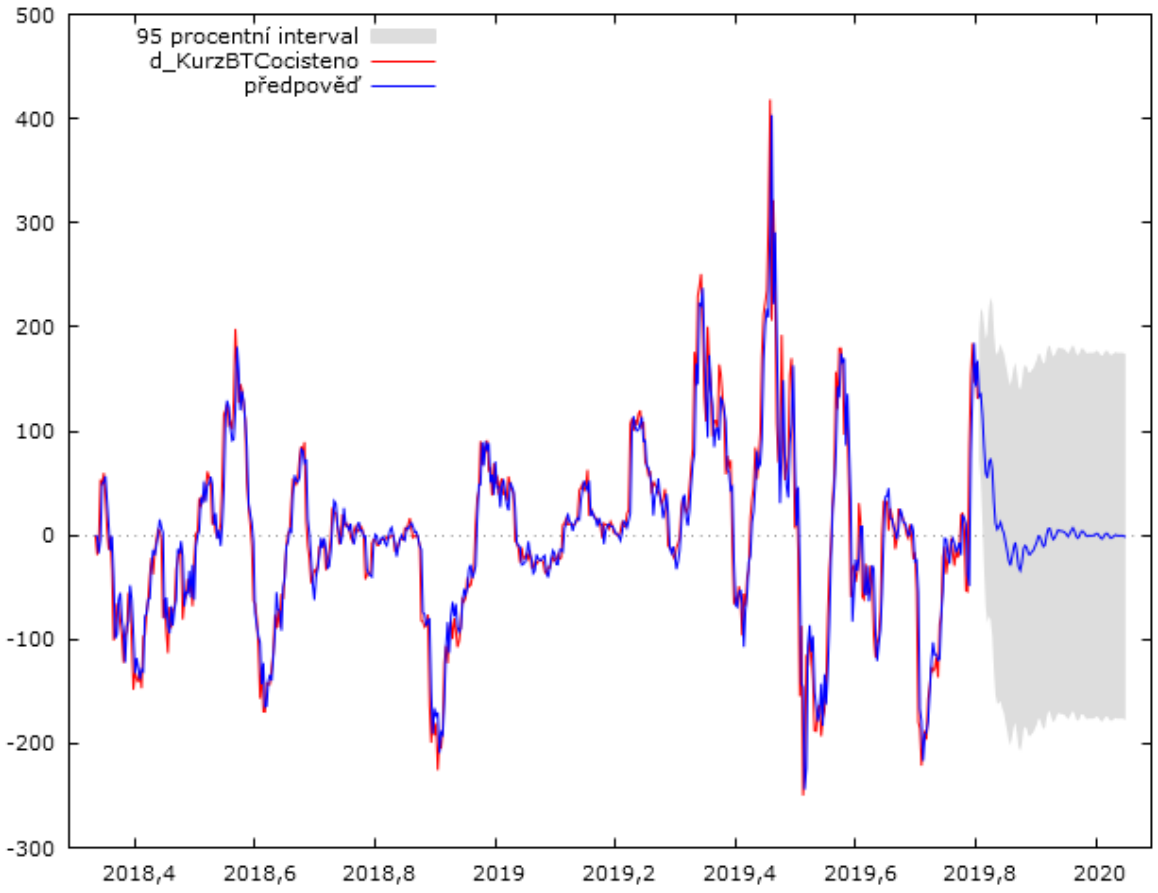
(Zdroj: Vlastní práce)

Odhadnutý model obsahuje nejvyšší počet statisticky významných parametrů, proto byl tento řád zpoždění pro jeho vytvoření zvolen. Rovnice odhadnutého modelu v konkrétním číselném vyjádření se zaokrouhlením parametrů na tři desetinná místa by tedy vypadala takto:

$$\Delta y_t = -0{,}264 + 1{,}926\Delta y_{t-1} - 1{,}405\Delta y_{t-2} - 0{,}334\Delta y_{t-3} + 1{,}392\Delta y_{t-4} - 0{,}230\Delta y_{t-5} - 1{,}301\Delta y_{t-6} + 1{,}624\Delta y_{t-7} - 0{,}732\Delta y_{t-8} + 0{,}563\varepsilon_{t-1} + 0{,}804\varepsilon_{t-2} - 0{,}760\varepsilon_{t-3} - 0{,}203\varepsilon_{t-4} + 0{,}876\varepsilon_{t-5} - 0{,}793\varepsilon_{t-6} + 0{,}024\varepsilon_{t-7} + \varepsilon_t$$

Za pomoci sestaveného ARMA modelu byla v prostředí Gretl vypracována ekonomická prognóza, s délkou prognostického horizontu tří měsíců. Na obrázku číslo 16 je zachycena celé časová řada, včetně odhadnuté prognózy, která je v obrázku zaznačena v šedém poli na konci časové řady. Data jsou vyobrazena v diferencích prvního řádu.

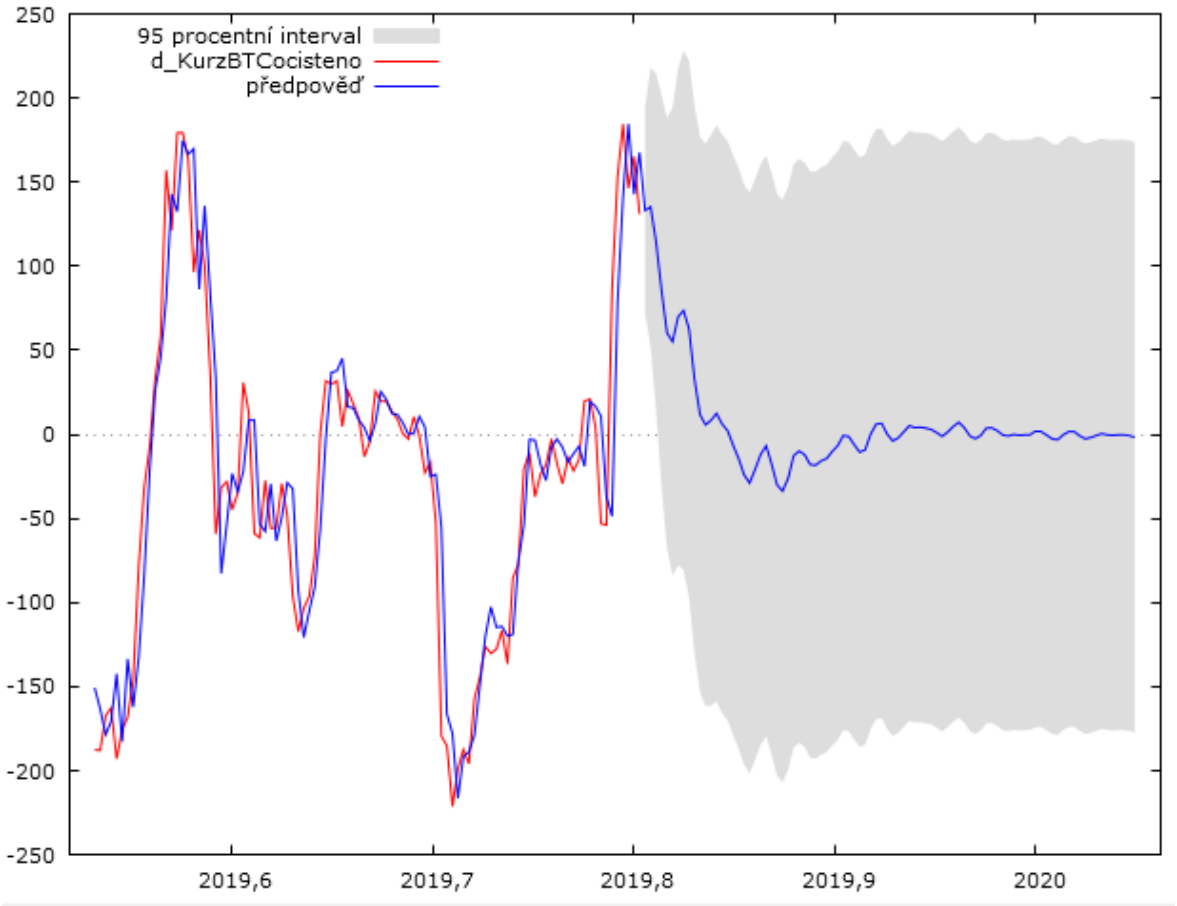
Obrázek 16- Průběh prognózy



(Zdroj: Vlastní práce)

Na následujícím obrázku číslo 17 je pro lepší přehlednost vyobrazen detail průběhu prognózy bez předchozích pozorování časové řady. Data jsou vyobrazena v diferencích řádu jedna.

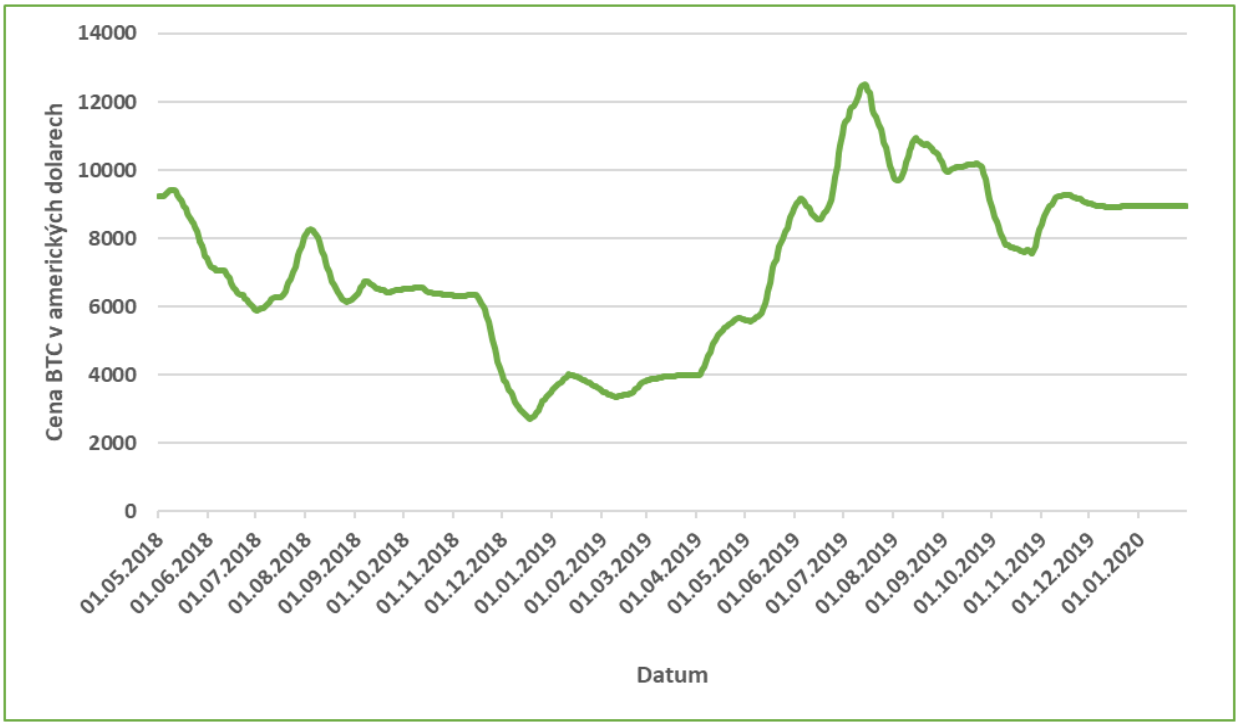
Obrázek 17- Detail zpracované prognózy



(Zdroj: Vlastní práce)

Průběh časové řady a vypracované prognózy převedené z postupných diferencí prvního řádu na původní hodnoty je zobrazen na obrázku číslo 18.

Obrázek 18- Průběh časové řady cenové hladiny virtuální měny Bitcoin



(Zdroj: Vlastní práce)

Konkrétnější představu o odhadnutém vývoji kurzu virtuální měny Bitcoin poskytne číselné vyjádření ekonomické prognózy. Výstupní data jsou zachycena v tabulce číslo 3.

Tabulka 3 – Průběh vypracované prognózy

Listopad	Kurz BTC	Prosinec	Kurz BTC	Leden	Kurz BTC
01.11.2019	8413,3226	01.12.2019	9026,777	01.01.2020	8956,573
02.11.2019	8546,4189	02.12.2019	9008,81	02.01.2020	8955,886
03.11.2019	8681,6849	03.12.2019	8990,466	03.01.2020	8959,489
04.11.2019	8796,5176	04.12.2019	8974,665	04.01.2020	8963,357
05.11.2019	8882,2923	05.12.2019	8960,332	05.01.2020	8965,509
06.11.2019	8942,5363	06.12.2019	8950,07	06.01.2020	8965,101
07.11.2019	8997,6071	07.12.2019	8943,216	07.01.2020	8964,156
08.11.2019	9067,4224	08.12.2019	8942,407	08.01.2020	8964,032
09.11.2019	9141,0563	09.12.2019	8941,106	09.01.2020	8963,475
10.11.2019	9203,5831	10.12.2019	8934,933	10.01.2020	8963,137
11.11.2019	9236,0883	11.12.2019	8924,344	11.01.2020	8962,913
12.11.2019	9247,7071	12.12.2019	8915,104	12.01.2020	8964,367
13.11.2019	9253,4018	13.12.2019	8915,324	13.01.2020	8965,828
14.11.2019	9261,8164	14.12.2019	8921,393	14.01.2020	8965,243
15.11.2019	9274,3062	15.12.2019	8927,938	15.01.2020	8962,545
16.11.2019	9280,4891	16.12.2019	8928,028	16.01.2020	8959,362
17.11.2019	9282,6393	17.12.2019	8924,094	17.01.2020	8959,041
18.11.2019	9276,2042	18.12.2019	8921,92	18.01.2020	8960,623
19.11.2019	9261,7987	19.12.2019	8923,386	19.01.2020	8962,179
20.11.2019	9237,8527	20.12.2019	8928,419	20.01.2020	8961,305
21.11.2019	9208,8592	21.12.2019	8932,464	21.01.2020	8958,665
22.11.2019	9188,0012	22.12.2019	8936,635	22.01.2020	8956,731
23.11.2019	9176,0072	23.12.2019	8940,312	23.01.2020	8956,009
24.11.2019	9169,1536	24.12.2019	8943,222	24.01.2020	8956,38
25.11.2019	9151,5913	25.12.2019	8944,176	25.01.2020	8956,049
26.11.2019	9121,4276	26.12.2019	8942,99	26.01.2020	8955,532
27.11.2019	9087,6649	27.12.2019	8944,375	27.01.2020	8955,176
28.11.2019	9061,565	28.12.2019	8949,042	28.01.2020	8954,865
29.11.2019	9048,8016	29.12.2019	8956,165	29.01.2020	8954,104
30.11.2019	9038,87	30.12.2019	8960,135	30.01.2020	8952,296
-		31.12.2019	8959,203	-	

(Zdroj: Vlastní práce)

Výstupní data prognózy vygenerované procesem ARMA jsou poměrně ustálená. Významnější změnu v řádech stovek dolarů za minci lze pozorovat především v úplném

počátku prognostického horizontu. Další vývoj odhadnuté cenové hladiny je utlumen na změny v řádech desítek až jednotek dolarů za minci.

4.2. Faktory ovlivňující kurz Bitcoinu

Dalším z cílů této diplomové práce je posoudit, zda má vývoj kurzu dalších vybraných komodit vliv na vývoj cenové hladiny virtuální měny Bitcoin. Míra ovlivnění bude posuzována metodou korelační a analýzy. Mezi komodity, se kterými bude míra korelace hodnocena, patří cena zlata, index amerického dolaru, index Eura, akciový index S&P 500, výnosy z amerických dluhopisů a další tři velké virtuální měny Ethereum, Litecoin a Ripple.

Cena zlata byla pro potřeby korelační analýzy vybrána jako zástupce ukazatele hodnoty napříč historií. Dodnes je zlato jedním z předních investičních nástrojů. Zlato coby měna přestalo ztrácet na významu po zrušení Brettonwoodského měnového systému z roku 1971. Podstatou dohody uzavřené během jednání mezi 44 zněměni v roce 1944, kdy byl systém zaveden, bylo napojení amerického dolaru na zlato. Ostatní měny byly napojeny na dolar a tak, byly všechny měny kryté zlatem. Tyto skutečnosti vedly k výběru zlata pro účely korelační analýzy.

Index amerického dolaru byl pro potřeby korelační analýzy vybrán z důvodu vyjádření síly amerického dolaru jako takového. Index porovnává sílu dolaru s šesti dalšími důležitými měnami obchodních partnerů Spojený státu amerických. Výchozí hodnota indexu, založeného v roce 1973 je 100. Hodnota indexu fluktuuje v závislosti na síle amerického dolaru vůči dalším měnám, čím je hodnota vyšší, tím je americký dolar silnější. (29)

Index Eura představuje podobně jako index amerického dolaru porovnání Eura s dalšími měnami. Nepřímo tedy vyjadřuje aktuální sílu Eura. Měny, se kterými se Euro porovnává, jsou americký dolar, Britské libra, Švýcarský frank a Japonský yen. Stejně jako v případě indexu amerického dolaru je výchozí hladinou hodnota 100.

Ze sektoru dalších virtuálních měn bylo pro vyšetření míry korelace s cenovou hladinou Bitcoinu vybrány Ethereum, Litecoin a Ripple. Tyto tři virtuální měny mají v listopadu roku 2019 po Bitcoinu nejvyšší tržní kapitalizaci v rámci sektoru. Technické detaily, které se těchto virtuálních měny týkají, byly uvedeny v samostatné kapitole této práce. Časové řady vývoje cenových hladin těchto virtuálních měn byly na rozdíl od ostatních porovnávaných veličin vstupujících do korelační analýzy zkráceny, z důvodu rozdílného data vzniku těchto virtuálních měn a neexistence dat některých virtuálních měn pro roky 2014 a 2015. Jako počátek byl tedy zvolen listopad roku 2016. Všechny tyto časové řady mají délku tří let a jsou zachyceny v týdenních pozorováních. Hodnoty časové řady jsou vyjádřeny v amerických dolarech za minci. (14)

Akciový index S&P 500 patří dlouhodobě mezi nejsledovanější indexy. Tento souhrnný index amerických akciových trhů je jedním z předních ukazatelů vypovídajícím o stavu americké ekonomiky. Je založen na tržní kapitalizaci pěti set největších amerických společností. (30)

Jako poslední byl zařazen výnos z desetiletého dluhopisu Americké vlády. Dluhopisy vydávané americkou vládou často korelují se situací americké ekonomiky, která je jedna z nejsilnějších. Proto byly americké dluhopisy vybrány pro korelační analýzu.

4.2.1 Korelační analýza

Zdrojem dat pro korelační analýzu byl server investing.com. Použita byla týdenní data s délkou časové řady pět let. Pro potřeby korelační analýzy byl využit software MS Excel s instalovaným doplňkem umožňujícím datovou analýzu.

Úkolem korelační analýzy je odpovědět na otázku, jak silná je závislost mezi proměnnými. V rámci korelační analýzy je sestavována korelační matice, která určí sílu lineární závislosti mezi veličinami. Tato matice obsahuje párové korelační koeficienty jednotlivých proměnných, z kterých lze určit sílu závislosti neboli korelace. Korelace vyjadřuje vliv změny úrovně jedné veličiny, na změnu úrovně druhé. Kladná korelace vyjadřuje růstovou tendenci obou proměnných, záporná pokles a nulová korelace stagnaci

obou proměnných. V tomto případě bude v korelační matici zkoumán vliv výše zmíněných faktorů na růst cenové hladiny virtuální měny Bitcoin. Párové korelační koeficienty budou tedy vždy tvořeny cenou Bitcoinu a jednou další z vybraných veličin. (31)

Míra korelace je posuzována dle výše Pearsonova korelačního koeficientu, který je ve statistice běžně označován písmenem r. Tento statistický ukazatel míry korelace mezi veličinami může nabývat hodnot od -1 do 1. Čím je hodnota korelačního koeficientu blíže mezním hranicím -1 a 1, tím je míra závislosti silnější. Pokud korelační párový koeficient dosahuje přímo hodnoty -1, nebo 1, pak je korelace mezi proměnnými označovaná za dokonalou. V případě dokonalé korelace by grafické znázornění obou veličin představovalo jednu dokonale rovnou přímku. (31)

Vyhodnocení míry korelace bylo v této práci provedeno za pomoci stupnice, kterou roku 1996 publikoval J. D. Evans. Stupnice je zobrazena v tabulce číslo 4.

Tabulka 4 - Evansova stupnice

Síla korelace	r
Velmi slabá	0-0,19
Slabá	0,20 - 0,39
Střední	0,40 - 0,59
Silná	0,60 - 0,79
Velmi silná	0,80 - 1,00

(Zdroj: Vlastní práce)

Korelační matice budou z důvodu neexistence podkladových dat pro virtuální měnu Ethereum v rocích 2015 a 2014 zpracovány dvě. Jedna bude obsahovat akciový index S&P500, Zlato, ETH, Index amerického dolaru, index Eura, výnos z amerických dluhopisů a Bitcoin. Druhá matice pak bude obsahovat pouze Bitcoin a Ethereum se stejnou délkou časové řady.

Výsledky první korelační matice, sestavené na podkladových datech, která byla zmíněna výše, si lze prohlédnout v tabulce číslo 5.

Tabulka 5- Korelační matice č. 1

	SP500	*Zlato*	*BTC*	*Index dolaru*	*US dluhopisy*	*Index Eura*
SP500	**1,000**					
Zlato	0,587	**1,000**				
BTC	0,844	0,586	**1,000**			
Index dolaru	-0,152	-0,277	-0,342	**1,000**		
US dluhopisy	0,477	-0,199	0,349	-0,211	**1,000**	
Index Eura	0,767	0,582	0,806	-0,675	0,369	**1,000**

(Zdroj: Vlastní práce).

Prvky korelační matice nad diagonálou, vyznačené v tomto případě oranžovou barvou jsou z korelační matice vynechány z důvodu jejich nadbytečnosti. Data nad diagonálou jsou u korelační matice stejná jako pod ní. Pro vyhodnocení míry korelace byla tedy duplicitní data vynechána. Koeficienty, které jsou v tabulce zaznačeny žlutou barvou, jsou z hodnocení vynechány. Jde o párové koeficienty stejných proměnných, které mezi sebou dokonale korelují. V následující tabulce číslo 6. jsou vyhodnoceny párové korelační koeficienty první korelační matice.

Tabulka 6 - Vyhodnocení korelačních koeficientů č. 1

	Proměnná	**R**	**Síla závislosti dle Evanse**
BTC	**SP500**	**0,844**	**Velmi silná**
	Zlato	**0,586**	**Střední**
	Index eura	**0,806**	**Velmi silná**
	Index dolaru	**-0,342**	**Slabá**
	US Dluhopisy	**0,349**	**Slabá**

(Zdroj: Vlastní práce)

Z korelační matice je zřejmé, že cenová hladina Bitcoinu koreluje slabě s indexem dolaru a výnosem z amerických dluhopisů. Středně silnou korelaci lze pozorovat mezi

cenou zlata a cenovou hladinou Bitcoinu. Nejsilnější korelace s cenou Bitcoinu v rámci komodit vstupujících do korelační analýzy vykazuje akciový index S&P500. Hodnota párového korelačního koeficientu v tomto případě dosahuje 0,844, což je dle Evansovy stupnice velmi silná korelace. Další velmi silná korelace se nachází mezi indexem eura a Bitcoinem.

Druhá korelační matice obsahuje pouze sektor virtuálních měn. Jsou to cenová hladina virtuální měny Ethereum, Bitcoin, Litecoin a Ripple. Podkladová data pro druhou matici jsou v délce tří let, od listopadu roku 2016 do listopadu roku 2019. Korelační matice je zobrazena v tabulce číslo 7.

Tabulka 7- Korelační matice č. 2

	BTC	ETH	LTC	XRP
BTC	**1,000**			
ETH	0,698	**1,000**		
LTC	0,840	0,826	**1,000**	
XRP	0,694	0,788	0,839	**1,000**

(Zdroj: Vlastní práce)

Stejně jako u první matice jsou duplicity prvků vynechány a párový korelační koeficient je uveden pouze pod diagonálou. Dokonalá korelace mezi stejnými prvky bude z hodnocení síly korelace vynechána. Vyhodnocení síly korelace dle Evansovy stupnice mezi cenovou hladinou Bitcoinu a cenovou hladinou Etherea je zobrazeno v tabulce číslo 8.

Tabulka 8- Vyhodnocení korelačních koeficientů matice č. 2

	Proměnná	r	Síla závislosti dle Evanse
BTC	**ETH**	**0,698**	**Silná**
	LTC	**0,840**	**Velmi silná**
	XPR	**0,694**	**Silná**

(Zdroj: Vlastní práce)

Z hodnot párových korelačních koeficientů odečtených z korelační tabulky číslo dvě lze zhodnotit, že míra závislosti je mezi jednotlivými virtuálními měnami poměrně značná. Velmi silná korelace byla zjištěna mezi cenou virtuálních měn Litecoin a Bitcoin.

Hodnota korelace mezi těmito dvěma virtuálními měnami dosahuje výše 0,84. Dle odečtených hodnot jsou však i ostatní míry závislosti v rámci testovaných veličin velmi silné. Například míra korelace mezi Litecoinem a Ethereem dosahuje velmi silné úrovně s hodnotou 0,826, podobně vysoká je míra závislosti i v případě Ripple a Litecoinu. Silné úrovně závislosti dosahuje cenová hladina Bitcoinu i s cenou Etherea a Ripple, zde jsou hodnoty párových korelačních koeficientů podobné a liší se pouze o čtyři setiny.

Z výstupů obou korelačních matic lze stanovit několik velmi silných a silných funkčních závislostí mezi Bitcoinem a dalšími veličinami, především mezi indexem eura, akciovým indexem S&P500 a virtuální měnou Litecoin je vykazovaná míra korelace dle Evansovy stupnice velmi silná. Silná míra korelace se nachází mezi cenovou hladinou virtuálních měn Etherea, Ripple a Bitcoinu. Z výstupu je zřejmé, že ostatní virtuální měny poměrně často kopírují změny a výkyvy kurzu nejsilnější virtuální měny Bitcoinu, nalezená míra korelace mezi zkoumanými virtuálními měnami tento předpoklad potvrzuje. Středně silná funkční závislost byla nalezena mezi cenou zlata a cenovou hladinou Bitcoinu. Slabé míry závislosti je dosaženo v případě indexu dolaru a výnosu z amerických dluhopisů.

5 Výsledky a diskuse

Hlavním cílem této práce bylo stanovit, zda vybrané finanční komodity ovlivňují cenovou hladinu virtuální měny Bitcoin a jak v jaké výši ji ovlivňují. Pro účely stanovení míry závislosti byla zvolena metoda korelační analýzy, která poskytuje hodnocení o vzájemných závislostech mezi proměnnými.

Mezi proměnné, které byly pro korelační analýzu využity, byly zařazeny zástupci několika finančních sektorů tzv. tvrdých měn, a to konkrétně index amerického dolaru a eura. Za sektor cenných papírů byly jako zástupci vybráni americký akciový index S&P500 a výnos z amerických dluhopisů s délkou splatnosti 10 let. Zástupcem komoditního odvětví drahých kovů byla zvolena cena zlata. Zvláštní skupinu v korelační analýze utvořily další virtuální měny. Do korelační analýzy byly zařazeny tři z nich, tj. Ethereum, Litecoin a Ripple.

Korelační analýza byla provedena ve dvou částech. První část s délkou časové řady pět let, od listopadu roku 2014 do listopadu roku 2019 zahrnovala porovnání ceny Bitcoinu se zlatem, indexem amerického dolaru, indexem eura, výnosy z amerických dluhopisů a akciovým indexem S&P500.

Druhá část korelační analýzy obsáhla vyjádření míry korelace mezi Bitcoinem a virtuálními měnami Ethereum, Ripple a Litecoin. Délka časových řad byla v tomto případě díky rozdílným datům vzniku, a tedy neexistenci historických dat zkrácena na tři roky, od listopadu 2016 do listopadu 2019.

V první části korelační analýzy byla zjištěna velmi silná míra závislosti mezi cenou Bitcoinu a vývojem akciového indexu S&P500 a indexu eura. Naopak slabá korelace byla zjištěna mezi cenou Bitcoinu, výnosy z amerických dluhopisů a indexem amerického dolaru.

V druhé části byla zjištěna velmi silná korelace mezi cenou Bitcoinu a Litecoinu. Korelace mezi Bitcoinem, cenou Etherea a Ripple byla vyhodnocena jako silná. Korelace ceny Litecoinu s dalšími veličinami sice není hlavním předmětem zkoumání této práce,

přesto si nelze nevšimnout nejen velmi silné korelace mezi cenou Litecoinu a zkoumaného Bitcoinu, ale také mezi Litecoinem a ostatními zkoumanými virtuálními měnami. Toto zjištění ukazuje, že odvětví virtuálních měn často reaguje na změny kurzu stejně.

Vedlejším cílem této diplomové práce bylo zpracování ekonomické prognózy cenové hladiny virtuální měny Bitcoin s délkou prognostického horizontu tří měsíců. Ekonomická prognóza byla zpracována za pomoci metod ekonometrického modelování. Nejprve byla za pomoci standartních statistických operací provedena úprava vstupních dat, tak aby bylo dosaženo vyhlazení a stacionarity časové řady vstupující do modelu.

Pro sestavení ekonometrického modelu byl zvolen smíšený proces ARMA s řádem zpoždění AR (8) MA (8). Tyto řády zpoždění byly zvoleny na základě zkoumání signifikance jednotlivých řádů zpoždění pro stacionární časovou řadu, přičemž zvolený proces obsahoval nejvíce statisticky významných proměnných.

Za pomoci procesu ARMA (8,8) byla sestavena ekonomická prognóza. Tato prognóza předpověděla mírný propad a následně ustálený vývoj kurzu virtuální měny Bitcoin na následující tři měsíce. Hodnoty se od sebe, mimo počátečního propadu o zhruba tisíc dolarů, žádným směrem příliš nevychylují. Změny cenové hladiny se pohybují v řádech několika stovek dolarů za minci s postupným útlumem na změny v řádech desítek dolarů. Podrobné číselné výsledky byly uvedeny v tabulce číslo 2.

Gajdorusová ve své případové studii Bitcoinu z roku 2019 vytvořila prognózu vývoje kurzu Bitcoinu v srpnu roku 2018. Tato prognóza byla sestavena s výrazně kratším časovým horizontem než prognóza vytvořená v rámci této práce, přesto se výsledky shodovaly ve stálosti průběhu prognóz.

Rozdíly s prognózami jiných autorů lze připsat na vrub rozdílům ve vstupních datech, například délky časových řad, nebo jejich kvality. Dále mohou být rozdíly způsobeny nevhodným výběrem ekonometrického modelu. V rámci této práce bylo využito procesu ARMA, lze však využít i modely VAR, VECM a jiné.

6 Závěr

Hlavním cílem této práce bylo nalézt odpověď na otázku týkající se spojitosti vývoje cenové hladiny virtuální měny Bitcoin s dalšími finančními komoditami. V rámci empirické části této práce, byly vybrané komodity z různých finančních odvětví porovnávány a zkoumány za pomoci statistické metody korelační analýzy.

Výsledky ukázaly na silnou závislost mezi růstem cenových hladin zkoumaných virtuálních měn. Na základě těchto výsledků lze předpokládat, že budou virtuální měny jako sektor reagovat na pokles i růst kurzu společně. V porovnání s komoditami mimo sektor virtuálních měn byla nalezena velmi silná míra závislosti mezi akciovým indexem S&P500 a indexem eura. Dle těchto výsledků lze tedy předpokládat, že kurz S&P500, index Eura a kurz Bitcoinu budou taktéž navzájem kopírovat aktuální trendy ve vývoji cen.

Vedlejším cílem bylo zpracování odhadu vývoje cenové hladiny virtuální měny Bitcoin v délce tří měsíců. Tento odhad byl realizován za použití statistických metod a metod ekonometrického modelování.

Dále byl zpracován ekonometrický model ARMA s odpovídajícím řádem zpoždění, který byl stanoven vzhledem k předchozímu zkoumání časové řady historického cenového vývoje Bitcoinu. Jeho výstupem byla prognóza vývoje cenové hladiny této virtuální měny s délkou prognostického horizontu tří měsíců, která pro tento časový úsek naznačila mírný propad a následnou stagnaci kurzu Bitcoinu.

7 Seznam použitých zdrojů

Knižní publikace

4. HALABURDA, Hanna a M. SARVARY. *Beyond bitcoin: the economics of digital currencies*. New York City, NY: Palgrave Macmillan, 2016. ISBN 978-113-7506-412.

5. QUEST, Martin. *Cryptocurrency Master*. 1. CreateSpace Independent Publishing Platform, 2018. ISBN 9781721961634.

6. FRANCO, Pedro. *Understanding Bitcoin*. John Wiley, 2014. ISBN 1119019168.

7. LEE, David. *Handbook of digital currency: bitcoin, innovation, financial instruments, and big data*. Amsterdam: Elsevier/ AP, [2015]. ISBN 978-012-8021-170.

8. SWAN, Melanie. *Blockchain: blueprint for a new economy*. O´Reilly: Sebastopol, 2015. ISBN 978-1-491-92049-7.

10. ANTONOPOULOS, Andreas M. a Gavin WOOD. *Mastering Ethereum: building smart contracts and DApps*. Sebastopol, CA: O'Reilly, 2019. ISBN 14-919-7194-0.

11. NARAYANAN, Arvind. *Bitcoin and cryptocurrency technologies: a comprehensive introduction*. Princeton: Princeton University Press, [2016]. ISBN 978-069-1171-692.

12. NISHIBE, Makoto. *The enigma of money: gold, central banknotes, and bitcoin*. New York, NY: Springer Berlin Heidelberg, 2016. ISBN 978-981-1018-183.

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

15. BASHIR, Imran. *Mastering Blockchain*. Packt Publishing Limited, 2018. ISBN 9781788839044.

16. GATES, Mark. *Blockchain*. Createspace, 2017. ISBN 9781547090686.

17. ANTONOPOULOS, Andreas M. *Mastering bitcoin*. Sebastopol CA: O'Reilly, 2015. ISBN 978-149-1902-608.

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

20. SZMIGIELSKI, Albert. *Bitcoin Essentials*. Packt Publishing Limited, 2016. ISBN 9781785281976.

22. REED, Jeff. *Litecoin: An Introduction to Litecoin Cryptocurrency and Litecoin Mining*. 2017.

23. TAKASHIMA, Ikuya. *Litecoin: The Ultimate Guide to the World of Litecoin*. CreateSpace Independent Publishing Platform, 2018. ISBN 978-1986181235.

24. ARTL, Josef a Markéta ARTLOVÁ. *Analýza ekonomických časových řad s příklady*. Praha: Vysoká škola ekonomická, Fakulta informatiky a statistiky, 2002. ISBN 80-245-0307-7.

28. TVRDOŇ, Jiří. *Ekonometrie*. Vyd. 5. Praha: Česká zemědělská univerzita, 2001. ISBN 978-80-213-0819-0.

32. NEUBAUER, Jiří, Marek SEDLAČÍK a Oldřich KŘÍŽ. *Základy statistiky: aplikace v technických a ekonomických oborech*. 2., rozšířené vydání. Praha: Grada, 2016. ISBN 978-80-247-5786-5.

33. HINDLS, Richard. *Statistika pro ekonomy*. 8. vyd. Praha: Professional Publishing, 2007. ISBN 978-80-86946-43-6.

34. SAMUELSON, Paul Anthony a William D. NORDHAUS. *Ekonomie: 19. vydání*. Praha: NS Svoboda, 2013. ISBN 978-80-205-0629-0.

35. LÁNSKÝ, Jan. *Kryptoměny*. V Praze: C.H. Beck, 2018. ISBN 978-807-4007-224.

36. STROUKAL, Dominik. *Ekonomické bubliny: kdo je nafukuje, proč praskají a jak v další krizi neztratit vše*. Praha: Grada, 2019. ISBN 978-80-271-2194-6.

37. HARTMAN, Ondřej. *Začínáme na burze: jak uspět při obchodování na finančních trzích: akcie, komodity, forex a kryptoměny*. Nové rozšířené vydání. Brno: BizBooks, 2018. ISBN 978-80-265-0780-2.

38. ŠTĚDROŇ, Bohumír. *Prognostické metody a jejich aplikace*. V Praze: C.H. Beck, 2012. Beckova edice ekonomie. ISBN 978-807-1791-744.

39. CIPRA, Tomáš. *Finanční ekonometrie*. 2., upr. vyd. Praha: Ekopress, 2013. ISBN 978-80-86929-93-4.

40. FORBELSKÁ, Marie. *Stochastické modelování jednorozměrných časových řad*. Brno: Masarykova univerzita, 2009. ISBN 978-80-210-4812-6.

43. WEATHERFORD, Jack. *The History of Money*. Reprint edition. Crown Business, 1998. ISBN 978-0609801727.

Elektronické články

1. POLASIK, Michal. *Price Fluctuations and the Use of Bitcoin: An Empirical Inquiry* [online]. 2014 [cit. 2019-11-26]. Dostupné z: https://www.researchgate.net/publication/280570108_Price_Fluctuations_and_the_Use_of_Bitcoin_An_Empirical_Inquiry

2. BOUOIYOUR, Jamal a Refk SELMI. *What Does Bitcoin Look Like?* [online]. 2015 [cit. 2019-11-26]. Dostupné z: http://down.aefweb.net/AefArticles/aef160211Bouoiyour.pdf

3. VAN ALSTYNE, Marshall. *Why Bitcoin has value* [online]. [cit. 2019-11-26]. Dostupné z: https://www.researchgate.net/publication/273609426_Why_Bitcoin_Has_Value

Legislativní dokumenty

9. *Sdělení k účtování a vykazování digitálních měn*. In: . 2018. Dostupné také z: https://www.mfcr.cz/assets/cs/media/Ucetnictvi_2018_Sdeleni-MF-k-uctovani-a-vykazovani-digitalnich-men.pdf

42. *Zákon č. 253/2008 Sb*. In: . 2008. Dostupné také z: https://www.mfcr.cz/cs/legislativa/legislativni-dokumenty/2008/zakon-c-253-2008-sb-3191

Elektronické publikace a weby

14. *CoinMarketCap* [online]. [cit. 2019-11-26]. Dostupné z: https://coinmarketcap.com/

18. Bitcoin Electronic Waste Monitor. In: *Digiconomist.com* [online]. [cit. 2019-11-26]. Dostupné z: https://digiconomist.net/bitcoin-electronic-waste-monitor/

21. *Bitcoin daily transactions* [online]. In: . [cit. 2019-11-26]. Dostupné z: https://charts.bitcoin.com/btc/chart/daily-transactions#5moc

25. HANČLOVÁ, Jana a Luboš TVRDÝ. *Úvod do analýzy časových řad.* [online]. VŠB Ostrava, 2003 [cit. 2019-11-26]. Dostupné z: https://www.fd.cvut.cz/department/k611/PEDAGOG/VSM/7_AnalyzaCasRad.pdf

26. *Investing.com* [online]. [cit. 2019-11-26]. Dostupné z: https://www.investing.com/crypto/bitcoin/btc-usd

27. PETRÁŠKOVÁ, Vladimíra. *Prognostické modely v oblasti modelování finančních časových řad* [online]. 2006 [cit. 2019-11-26]. Dostupné z: https://www.pef.czu.cz/dl/46392

29. RÁDY, Andrej. *Index amerického dolaru.* [online]. In: . 2009 [cit. 2019-11-26]. Dostupné z: https://www.investicniweb.cz/2009-11-26-index-americkeho-dolaru-s-kym-mame-tu-cest/

30. KOŤÁTKO, Lukáš. *S&P 500 index* [online]. In: . [cit. 2019-11-26]. Dostupné z: https://www.lynxbroker.cz/vzdelavani/sp-500-index/

31. BISKUP, Roman. *Statistika: Regresní a korelační analýza* [online]. In: . Jihočeská univerzita v Českých Budějovicích, 2008 [cit. 2019-11-26]. Dostupné z: http://www2.ef.jcu.cz/~birom/stat/prednasky/17.pdf

41. *BTC.com* [online]. [cit. 2019-11-26]. Dostupné z: https://pool.btc.com/?jump=logo

44. *Box-Jenkinsova metodologie* [online]. Masarykova univerzita [cit. 2019-11-26]. Dostupné z: https://is.muni.cz/el/1431/jaro2006/M0122/M0122.pdf

45. DORDA, Michal. *Regresní a korelační analýza* [online]. Technická univerzita Ostrava [cit. 2019-11-26]. Dostupné z: http://homel.vsb.cz/~dor028/Regrese.pdf