

Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra ekonomiky



Diplomová práce

**Analýza determinant působících na vývoj ceny
kryptoměny bitcoin**

Bc. Daniel Rudolf

© 2022 ČZU v Praze

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Daniel Rudolf

Ekonomika a management
Provoz a ekonomika

Název práce

Analýza determinant působících na vývoj ceny kryptoměny bitcoin

Název anglicky

Analysis of determinants influencing development of the price of the cryptocurrency bitcoin

Cíle práce

Hlavním cílem práce je nalezení a následná kvantifikace podstatných determinant působících na vývoj ceny kryptoměny bitcoin. Dílčími cíli je provedení analýzy časových řad a zpracování podkladových dat k práci v SW Gretl. Dále zjistit, která z determinant působí na sledovanou veličinu nejvíce a posoudit, zda je možné provést prognózu do budoucna. Poté případně provést krátkodobou prognózu.

Metodika

Teoretická část práce bude zaměřena na provedení kompilace informací získaných prostudováním odborné literatury a relevantních internetových zdrojů.

Praktická část práce bude obsahovat analýzu časových řad a posouzení vývoje jednotlivých veličin v čase. Na základě těchto dat bude sestaven ekonometrický model a provedena jeho verifikace. Následně bude, pokud to získané výsledky umožní, provedena krátkodobá prognóza vývoje ceny kryptoměny bitcoin.

Doporučený rozsah práce

70-80

Klíčová slova

Ekonometrická analýza, determin, časová řada, kryptoměna, bitcoin

Doporučené zdroje informací

CIPRA, T. *Finanční ekonometrie*. Praha: Ekopress, 2008. ISBN 978-80-86929-43-9.

HANČLOVÁ, J. *Ekonometrické modelování : klasické přístupy s aplikacemi*. Praha: Professional Publishing, 2012. ISBN 978-80-7431-088-1.

HUŠEK, R. – VYSOKÁ ŠKOLA EKONOMICKÁ V PRAZE. *Aplikovaná ekonometrie : teorie a praxe*. Praha: Oeconomica, 2009. ISBN 978-80-245-1623-3.

SAMUELSON, P. A. – NORDHAUS, W. D. *Ekonomie : 19. vydání*. Praha: NS Svoboda, 2013. ISBN 978-80-205-0629-0.

STROUKAL, D. – SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti : historie, ekonomie a technologie kryptoměn, stručná příručka pro úplné začátečníky. Třetí rozšířené vydání*. Praha: Grada Publishing, 2021. ISBN 978-80-271-0742-1.

TVRDOŇ, J. – ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE. KATEDRA ZEMĚDĚLSKÉ EKONOMIKY. *Ekonometrie*. Praha: ČZU PEF Praha ve vydavatelství Credit, 2001. ISBN 80-213-0819-2.

Předběžný termín obhajoby

2021/22 LS – PEF

Vedoucí práce

Ing. Pavlína Hálová, Ph.D.

Garantující pracoviště

Katedra ekonomiky

Elektronicky schváleno dne 28. 8. 2021

prof. Ing. Miroslav Svatoš, CSc.

Vedoucí katedry

Elektronicky schváleno dne 19. 10. 2021

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 15. 03. 2022

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Analýza determinant působících na vývoj ceny kryptoměny bitcoin" 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 31. 3. 2022

Poděkování

Rád bych touto cestou poděkoval paní Ing. Pavlíně Hálové, Ph.D. za odborné vedení, cenné rady a konzultace při vypracování mé diplomové práce.

Analýza determinant působících na vývoj ceny kryptoměny bitcoin

Abstrakt

Diplomová práce je zaměřena na určení a kvantifikování důležitých determinant týkajících se ceny kryptoměny bitcoin. Dále se práce zabývá analýzou časových řad důležitých pro sestavení modelu.

K vypracování práce jsou využity metody ekonometrické analýzy a parametry jsou odhadované v softwaru Gretl. V tomto programu je proveden odhad jednorovnicového modelu v mocinné funkční formě, který popisuje působení důležitých determinant na cenu kryptoměny bitcoin. Podkladová data pro finální model jsou ve formě měsíčních časových řad za období od 1. 4. 2013 do 1. 6. 2021. Model je následně verifikován a použit k aplikaci.

Co se týče intenzity působení, nejvíce působí velikost peněžního agregátu M2 v USA s koeficientem pružnosti 3,290 %, tento determinant je jediný pružný. Druhý nejvíce ovlivňující determinant je cena kryptoměny litecoin, který působí se střední intenzitou 0,608 %. Nejméně působí cena kryptoměny bitcoin zpožděná o 6 období, s hodnotou 0,175 %. Na závěr je provedena prognóza ex-post na 6 posledních období. Se střední absolutní procentuální chybou 5,717 % je model vhodný k predikci.

Klíčová slova: Ekonometrická analýza, determinant, časová řada, kryptoměna, Bitcoin

Analysis of determinants influencing development of the price of the cryptocurrency bitcoin

Abstract

The thesis is focused on determining and quantifying of the important determinants related to the price of the cryptocurrency Bitcoin. Furthermore, the thesis is focused on the analysis of the time series important for the compilation of the model.

In a Bitcoin price model are used econometric analysis methods. Parameters are estimated in the Gretl software. In this software is performed an estimation of the single-equation power model, which describes influence of the main determinants to the price of the cryptocurrency Bitcoin. The underlying data for the final model is in the form of monthly time series for the period from 1. 4. 2013 to 1. 6. 2021. The model is subsequently verified and used for an application.

Speaking about elasticity coefficients, the most influencing is the supply of the M2 aggregate in the USA with coefficient of elasticity 3,290 %. Only this determinant is elastic. The second most influencing determinant is the price of the cryptocurrency Litecoin, which acts with a mean intensity of 0,608 %. The price of the cryptocurrency Bitcoin lagged by 6 periods, with a value of 0,175 %, have the least influencing effect. Lastly, an ex-post forecast is performed for the last 6 periods of time series. With a mean absolute percentage error of 5,717 %, the model is suitable for predictions.

Keywords: Econometric Analysis, Determinant, Time Series, Cryptocurrency, Bitcoin

Obsah

1 Úvod.....	12
2 Cíl práce a metodika	13
2.1 Cíl práce	13
2.2 Metodika	13
2.2.1 Časové řady.....	13
2.2.2 Indexní analýza	14
2.2.3 Stacionarita a nestacionarita časových řad	14
2.2.4 Sezónnost časových řad	15
2.2.5 Ekonometrický model.....	15
2.2.6 Konstrukce ekonometrického modelu	15
2.2.7 Formulace modelu	16
2.2.8 Sběr dat a analýza dat	17
2.2.9 Odhad parametrů modelu.....	17
2.2.10 Verifikace modelu.....	19
2.2.11 Využití ekonometrického modelu.....	22
3 Teoretická východiska	24
3.1 Úvod do světa kryptoměn	24
3.2 Těžba kryptoměn.....	26
3.2.1 Proof of work (PoW)	28
3.2.2 Proof of stake (PoS).....	32
3.3 Změna Bitcoinového protokolu.....	33
3.3.1 Bitcoin Improvement Proposal (BIP)	33
3.4 Nákup kryptoměn.....	36
3.4.1 Kryptoměnové burzy a směnárný	37
3.4.2 Bitcoinové bankomaty	38
3.4.3 Přímý nákup od lidí.....	39
3.5 Uchování bitcoinu	39
3.5.1 Hardwarové peněženky.....	39
3.5.2 Softwarové peněženky	40
3.5.3 Kryptoměnové burzy	41
3.6 Používání Bitcoinu	41
3.6.1 Transakce v Bitcoinové síti.....	42
3.6.2 Blockchain explorer.....	44
3.7 Silné a slabé stránky Bitcoinu.....	45
3.8 Česká prvenství týkající se Bitcoinu	47
3.9 Regulace kryptoměn.....	47

3.10	Ekonomika Bitcoinu.....	48
4	Vlastní práce	51
4.1	Analýza časových řad potenciálních determinant působících na cenu bitcoinu.....	51
4.1.1	Vývoj ceny kryptoměny bitcoin.....	51
4.1.2	Vývoj ceny akciového indexu S&P500	52
4.1.3	Vývoj ceny kovů	53
4.1.4	Porovnání vývoje sledovaných časových řad	55
4.2	Ekonometrický Model 1, cena kryptoměny bitcoin (1. 7. 2016 – 1.6.2021) ...	58
4.2.1	Ekonomický a ekonometrický model	58
4.2.2	Korelační matice	60
4.2.3	Rozšířený Dickey-Fullerův test (ADF-test)	61
4.3	Ekonometrický Model 2, cena kryptoměny bitcoin (1. 1. 2011 – 1.6.2021) ...	62
4.3.1	Rozšířený Dickey-Fullerův test (ADF-test)	62
4.3.2	Sezónnost časových řad (X-12 ARIMA)	63
4.3.3	Korelační matice	63
4.3.4	Ekonomický a ekonometrický model	64
4.3.5	Odhad parametrů pomocí BMNČ	65
4.3.6	Verifikace modelu.....	65
4.4	Ekonometrický Model 3, cena kryptoměny bitcoin (1. 9. 2015 – 1.6.2021) ...	66
4.4.1	Rozšířený Dickey-Fullerův test (ADF-test)	67
4.4.2	Korelační matice	67
4.5	Ekonometrický Model 4, cena kryptoměny bitcoin (1. 4. 2013 – 1.6.2021) ...	68
4.5.1	Ekonomický a ekonometrický model	69
4.5.2	Rozšířený Dickey-Fullerův test (ADF-test)	70
4.5.3	Odhad parametrů pomocí BMNČ s HACC errors (Možnost 1)	70
4.5.4	Odhad parametrů pomocí Cochrane-Orcutt (Možnost 2)	72
4.5.5	Odhad parametrů modifikovaného modelu se zpožděnými u_t (Možnost 3).....	74
4.5.6	Aplikace modelu	75
5	Závěr.....	78
6	Seznam použitých zdrojů.....	81
6.1	Knižní publikace.....	81
6.2	Internetové zdroje.....	82
7	Přílohy	86

Seznam obrázků

Obrázek 1: Mempool	29
Obrázek 2: Merkle tree s výškou 4	30
Obrázek 3: Hledání vyhovující nonce	31
Obrázek 4: Přehled poolů	32
Obrázek 5: Vznik forku a orphan bloků	36
Obrázek 6: BATMFour.....	38
Obrázek 7: Místa přijímající bitcoin (ČR).....	42
Obrázek 8: Transakce v Bitcoinové síti.....	43
Obrázek 9: Papírová peněženka.....	44

Seznam tabulek

Tabulka 1: Obsah hlavičky bloku	30
Tabulka 2: Struktura bloku	31
Tabulka 3: Bazický index ceny kryptoměny bitcoin	56
Tabulka 4: Bazické indexy sledovaných proměnných	57
Tabulka 5: Deklarace proměnných, Model 1.....	60
Tabulka 6: Korelační matice, Model 1	61
Tabulka 7: ADF-test, Model 1.....	61
Tabulka 8: ADF-test, Model 2.....	62
Tabulka 9: X-12 ARIMA, Model 2	63
Tabulka 10: Korelační matice, Model 2	64
Tabulka 11: Deklarace proměnných, Model 2.....	65
Tabulka 12: Odhad parametrů BMNČ, Model 2	65
Tabulka 13: Deklarace proměnných, Model 3.....	67
Tabulka 14: Korelační matice, Model 3	68
Tabulka 15: Integrace 1. řádu, Model 3.....	68
Tabulka 16: Deklarace proměnných, Model 4.....	70
Tabulka 17: ADF-test, Model 4.....	70
Tabulka 18: Odhad parametrů BMNČ, HACC errors, Model 4.....	70
Tabulka 19: Ekonomická verifikace, Model 3. Možnost 1.....	72
Tabulka 20: Odhad parametrů metodou Cochrane-Orcutt, Model 4.....	72
Tabulka 21: Ekonomická verifikace, Model 4, Možnost 2.....	73
Tabulka 22: Odhad parametrů modifikací metody Just and Pope, Model 4.....	74
Tabulka 23: Ekonomická verifikace, Model 4, Možnost 3.....	75
Tabulka 24: Koeficienty pružnosti, Model 4, Možnost 3	76
Tabulka 25: Prognóza ex-post, Model 4 (2/2)	77

Seznam grafů

Graf 1: Monetární inflace Bitcoinu.....	50
Graf 2: Vývoj ceny kryptoměny bitcoin	51
Graf 3: Vývoj ceny akciového indexu S&P500.....	52
Graf 4: Vývoj ceny kovů	53
Graf 5: Vývoj peněžního agregátu M2 v USA	54
Graf 6: Porovnání bazických indexů ceny SPX, kovů, M2 v USA	55
Graf 7: Prognóza ex-post, Model 4 (1/2).....	76

1 Úvod

Tato práce je zaměřena na analýzu determinant působících na vývoj ceny kryptoměny Bitcoin. Bitcoin vznikl jako vůbec první kryptoměna v historii a do současnosti si našel řadu fanoušků a zastánců této zajímavé technologie. První zmínka sahá do konce října roku 2008, kdy tvůrce s pseudonymem Satoshi Nakamoto zveřejnil průvodní článek Bitcoinu, ve kterém popsal myšlenku a fungování tohoto nového platebního systému. Na začátku ledna roku 2009 byla již síť Bitcoinu spuštěna. I když byla zprvu využívána jen opravdovými nadšenci a programátory, postupem času si nachází cestu k čím dál širší veřejnosti. Spolu s rostoucí popularitou vznikají i další kryptoměny, kterou jsou více či méně odlišné od původního konceptu Bitcoinu. V současné době existuje přes 9 tisíc rozdílných kryptoměn, mezi nejznámější patří v současné době např. Ethereum, Litecoin, Binance Coin, Ripple, Terra a Solana. I když se v případě kryptoměn stále jedná o poměrně malý trh, oproti tradičním finančním trhům, jeho velikost stále roste. v současnosti (konec března 2022) je celková tržní kapitalizace okolo 2,1 bil. USD, z čehož celých 890 mld. USD zastává Bitcoin. V listopadových maximech roku 2021 dosahovala celková tržní kapitalizace téměř 3 bil. USD. Jedná se o velmi rychle se rozvíjející odvětví s mnoha příležitostmi, v němž si Česká republika drží v mnoha aspektech světová prvenství. v teoretické části bude tato problematika detailně rozebrána pro bližší pochopení fungování a možností této technologie.

Po vymezení metodických postupů je v první části vlastní práce provedena analýza vybraných časových řad, které se jeví jako vhodné pro vysvětlení vývoje ceny kryptoměny bitcoin. Na základě získaných dat o časových řadách je v druhé části práce prováděno ekonometrické modelování, které si klade za cíl identifikovat a kvantifikovat hlavní determinanty působící na cenu kryptoměny bitcoin. Po úspěšném vytvoření a verifikaci modelu (Model 4, možnost 3) a zhodnocení naplnění ekonomických předpokladů proměnných, je v závěrečné části pomocí koeficientů pružnosti vysvětleno působení jednotlivých proměnných na cenu kryptoměny bitcoin a následně v rozsahu 6 měsíců provedena ex-post prognóza. V závěru práce jsou zhodnoceny a interpretovány získané výsledky ekonometrického modelování. K ekonometrickému modelování je využívám volně dostupný software Gretl a částečně software Statistica, dále jsou prováděny výpočty v Microsoft Excel.

2 Cíl práce a metodika

2.1 Cíl práce

Hlavním cílem diplomové práce je nalezení a následná kvantifikace podstatných determinant působících na vývoj ceny kryptoměny bitcoin. Dílčími cíli je provedení analýzy časových řad a zpracování podkladových dat k práci v SW Gretl. Dále zjistit, která z determinant působí na sledovanou veličinu nejvíce a posoudit, zda je možné provést prognózu do budoucna. Poté případně provést krátkodobou prognózu.

Dílčím cílem teoretické části práce je uvedení do problematiky kryptoměn, zejména Bitcoinu. Vysvětlení vzniku, technologie a fungování kryptoměn, dále možností využití a držení (úschovy) kryptoměn.

2.2 Metodika

Teoretická část práce bude rešerše zaměřená na vysvětlení podstaty kryptoměn, zejména Bitcoinu, a jejich fungování, těžbu, uchovávání a užívání. V závěru teoretické části bude pojednáváno o regulacích a ekonomice Bitcoinu.

V praktické části budou analyzovány zvolené časové řady, provedena indexní analýza a poté s využitím ekonometrického modelování, v SW Gretl, odhadnuty parametry pro model ceny kryptoměny Bitcoin. Model bude verifikován a využit k potvrzení či vyvrácení stanovených předpokladů o vlivech proměnných na cenu kryptoměny Bitcoin. Dále bude pro aplikaci modelu provedena strukturální analýza a prognóza ex-post.

2.2.1 Časové řady

Podle Hindlse (2007) reprezentuje časová řada věcně a prostorově srovnatelné hodnoty pozorování dané veličiny. Tyto hodnoty jsou jednoznačně uspořádány ve směru rostoucího času. „Časovou řadu s počtem pozorování n můžeme zapsat jako posloupnost y_1, y_2, \dots, y_n v čase t_1, t_2, \dots, t_n , neboli y_i v čase t_i , kde $t_i = t_1 + (i - 1) \Delta t_i$, $i = 1, \dots, n$. Hodnota Δt_i představuje délku časového kroku, s níž bylo prováděno pozorování.“

Dále Hindls (2007) rozlišuje časové řady, podle periodicity sledovaných údajů, na krátkodobé (v kterých jsou údaje zaznamenány v čtvrtletních, měsíčních, týdenních, aj. periodách) a na dlouhodobé (kde jsou údaje zaznamenány v ročních periodách). Dle způsobu vyjádření údajů se časové řady člení na časové řady peněžních ukazatelů

a naturálních ukazatelů. Také lze časové řady rozlišit podle druhu sledovaných ukazatelů na časové řady primárních, či sekundárních ukazatelů.

Cipra (1986) udává, že časovou řadu je možné rozložit na čtyři části, a to trend, sezónní složku, cyklickou složku a reziduální složku. Trend zachycuje dlouhodobé změny v průměrném chování časové řady. Hindls (2007) doplňuje, že trend může být rostoucí, klesající, či konstantní. Sezónní složka pak dle Cipry (1986) popisuje periodické změny v časové řadě, které se odehrají během jednoho kalendářního roku a každý rok se opakují. Cyklická složka podle Hindlse (2007) značí kolísání okolo trendu časové řady, v důsledku dlouhodobého cyklického vývoje, který má délku vlny delší než jeden rok. Náhodnou složku vysvětluje jako veličinu, kterou nelze popsat žádnou funkcí času. Tato veličina zbývá po vyloučení trendu, sezónní a také cyklické složky.

2.2.2 Indexní analýza

Tato metoda statistického zjišťování má za úkol zjistit vývoj hodnot časové řady. Na sledovaná data se použije metoda jednoduchých individuálních indexů. Výsledkem provedeného statistického zjišťování je ukazatel, který vyjadřuje změnu v období zkoumaném, oproti obdobím minulým. Jednoduché indexy je možné dělit na řetězové s proměnlivým základem (také koeficient růstu), nebo bazické, počítané ze stejného základu. Často je využíván i průměrný koeficient růstu, který je vyjádřen geometrickým průměrem jednotlivých koeficientů růstu (Hindls, a další, 2007).

$$\text{Řetězový index (koeficient růstu)} \quad I_{\frac{q_n}{q_{n-1}}} = \frac{q_2}{q_1}, \frac{q_3}{q_2}, \frac{q_4}{q_3}, \dots, \frac{q_n}{q_{n-1}} \quad (1)$$

$$\text{Bazický index} \quad I_{\frac{q_n}{q_1}} = \frac{q_2}{q_1}, \frac{q_3}{q_1}, \frac{q_4}{q_1}, \dots, \frac{q_n}{q_1} \quad (2)$$

$$\text{Průměrný koeficient růstu} \quad \bar{k} = \sqrt[n-1]{\frac{q_2}{q_1} \frac{q_3}{q_2} \frac{q_4}{q_3} \dots \frac{q_n}{q_{n-1}}} = \sqrt[n-1]{\frac{q_n}{q_1}} \quad (3)$$

2.2.3 Stacionarita a nestacionarita časových řad

Z hlediska statistiky jsou časové řady stále stejné (stacionární časová řada) anebo dochází ke změnám v průměru či variabilitě (nestacionární časové řady). Podle Hančlové (2012) u řady stacionární není možné odlišit dle průměru či rozptylu jeden úsek časové řady od úseku druhého. Naopak u nestacionární časové řady se průměr či rozptyl výrazně liší v jednotlivých úsecích, je tedy možné říci, že časová řada vykazuje změny v chování. Je možné pracovat vždy jen se stejným typem časových řad (stacionární/nestacionární).

Pro otestování stacionarity je možné využít rozšířený Dickey-Fullerův test (ADF-test). Při využívání nestacionárních dat je možné zjistit tzv. zdánlivou regresi, kdy regresní vztah je detekován bez racionální podstaty (Cipra, 2013).

2.2.4 Sezónnost časových řad

Sezónní složkou časové řady se rozumí periodické kolísání, které má systematický charakter. Kolísání se odehrává během jednoho roku a každý rok se ve stejné nebo modifikované podobě opakuje (u např. kratších denních časových řad se kolísání může odehrávat během dnů a pravidelně se opakovat v jednotlivých týdnech). Pro možnost použití takovýchto řad, společně s časovými řadami bez sezónní složky, je nutné provést očištění sezónní časové řady (Artl, a další, 2003). Zjištění přítomnosti sezónnosti je možné například pomocí F-testu pro sezónnost získaného provedením analýzy X-12 ARIMA v SW Gretl.

2.2.5 Ekonometrický model

Hušek (1995) uvádí, že ekonomický model je odvozen z ekonomických teorií a zároveň je zjednodušením vyjádření reálného světa. Takto definovaný ekonomický model slouží ke střetu teorie s realitou. Ekonometrický model vznikne v okamžiku, kdy je ekonomickému modelu určena funkční forma a přidána náhodná složka. Tím je respektována nahodilost modelovaného vztahu.

2.2.6 Konstrukce ekonometrického modelu

Hančlová (2012) rozděluje metodologický postup klasického ekonometrického modelování do pěti základních etap.

1. *„Formulace modelu*
 - a. *Ekonomická*
 - b. *Matematická*
 - c. *Ekonometrická*
2. *Sběr a analýza dat*
3. *Odhady parametrů modelu*
4. *Verifikace modelu*
 - a. *Statistická*
 - b. *Ekonometrická*

- c. *Ekonomická*
- 5. *Využití ekonometrického modelu pro*
 - a. *Analýzu zkoumaného jevu a simulace*
 - b. *Predikci*
 - c. *Optimální řízení*

2.2.7 Formulace modelu

Klasifikace proměnných v ekonometrickém modelu se dle Huška (1995) provádí následovně:

- Endogenní proměnné (také závislé, vysvětlované) se označují písmenem „y“. Jsou předmětem zkoumání v modelu a jejich hodnoty jsou získány z modelu. Představují výsledek působení predeterminovaných proměnných a náhodných proměnných.
- Exogenní proměnné (také nezávislé, vysvětlující) se označují písmenem „x“. Vysvětlují endogenní část rovnice a jejich hodnoty nejsou určeny model, ale ekonomickým prostředím.
- Predeterminované proměnné, které zahrnují proměnné exogenní, exogenní zpožděné a také endogenní zpožděné.
- Náhodná složka se označuje „ u_t “. Tvoří ji tři složky, které se nedají kvantitativně rozlišit. Obsahuje vliv dalších proměnných na endogenní proměnnou, chyby uskutečněné při měření hodnot proměnných a také chyby vznikající zjednodušením analytického tvaru příslušné funkce. Je rovna odchylce skutečné hodnoty endogenní proměnné od její teoretické hodnoty.

Pro **formulaci ekonomického modelu** se je dle Hančlové (2012) nutné zabývat následujícími aktivitami, pro zjednodušení reality zkoumaného problému:

- Stanovit předmět zkoumání.
- Klasifikovat ekonomické veličiny.
- Vymezit verbálně popis vazeb a vztahů mezi veličinami ve zkoumaném systému.
- Formulovat výchozí základní předpoklady či tvrzení o chování ekonomických veličin.

Formulace matematického modelu spočívá ve třech krocích:

- Vymežit klíčové proměnné v modelu.
- Provést transformaci ekonomického modelu do analytické formy funkčního předpisu.
- Stanovit očekávání pozitivních/negativních vztahů, případně omezení pro parametry modelu (Hančlová, 2012).

Formulace ekonometrického modelu, dle Hančlové (2012), lze dosáhnout přidáním náhodné složky (u_t) do deterministického modelu.

2.2.8 Sběr dat a analýza dat

Hušek (1995) uvádí, že ekonometrická analýza může vycházet z:

- Časové řady
- Průřezových dat
- Panelových dat

2.2.9 Odhad parametrů modelu

Dle Cipry (2008) mají parametry ekonometrického lineárního modelu požadované vlastnosti (jsou nejlepší, nestranné a konzistentní, tzv. BLUE¹), pokud splňují následující **předpoklady o náhodné složce**:

1. Průměr náhodné složky je nulový.

$$E(u_t) = 0 \quad (4)$$

2. Rozptyl náhodné složky v čase se nemění (homoskedasticita).

$$\text{Var}(u_t) = \sigma^2 < \infty \quad (5)$$

3. Kovariance reziduí je rovna nule.

$$\text{Cov}(u_i, u_j) = 0 \text{ pro } i \neq j \quad (6)$$

4. Kovariance mezi i-tou proměnnou a reziduem je rovna nule.

$$\text{Cov}(x_{it}, u_t) = 0 \quad (7)$$

¹ Nejlepší – není větší reziduální rozptyl, než ten ke kterému ho porovnáváme; Nestrannost – nedochází k systematickému nadhodnocení, či podhodnocení; Konzistence odhadu – při rostoucím počtu pozorování konverguje v pravděpodobnosti k hodnotě odhadovaného parametru

5. Normální rozdělení náhodné složky.

Dále musí dle Huška (1995) model splňovat následující **specifikační předpoklady**:

1. Nejsou zahrnuty irelevantní vysvětlující proměnné.
2. Neopomenutí zahrnutí významných vysvětlujících proměnných.
3. Je zvolena vhodná funkční forma modelu.
4. Odhadnuté parametry jsou stabilní.
5. Neexistuje simultánní vztah mezi vysvětlující a vysvětlovanou proměnnou.
6. Není přítomna perfektní multikolinearita.

BMNČ (Běžná metoda nejmenších čtverců, anglicky OLS) je využívána k odhadnutí parametrů lineárního regresního modelu. Podstatou metody je nalézt parametry, které minimalizují součet čtverců odchylek teoretických hodnot vysvětlované proměnné od skutečných hodnot této proměnné. Metoda BMNČ poskytne BLUE odhad, pokud jsou splněny výše uvedené předpoklady a následující kritérium (Hančlová, 2012).

$$\min \sum_{t=1}^n (y_t - \hat{y}_t)^2 \quad (8)$$

kde

y_t ... skutečná hodnota endogenní proměnné v čase t

\hat{y}_t ... teoretická hodnota endogenní proměnné v čase t

Vztah pro **odhad parametrů** modelu pomocí BMNČ je poté následující:

$$\gamma = (X^T X)^{-1} X^T y \quad (9)$$

kde

γ ... vektor ($k \times 1$) odhadovaných parametrů

X ... matice o rozměru $n \times k$, která obsahuje napozorované hodnoty „ k “ vysvětlujících proměnných

y ... vektor ($n \times 1$), který obsahuje napozorované hodnoty vysvětlované proměnné (Čechura, a další, 2013)

Pokud je v modelu detekována heteroskedasticita, je vhodné k odhadu **BMNČ využít robustních odhadů směrodatné chyby (HACC errors)**. Při detekované heteroskedasticita a autokorelaci v modelu je možné využít speciální **iterační metodu Cochran-Orcutt**, která nevyužívá k výpočtu minimalizaci sumy čtverců reziduí tak, jako BMNČ (Hančlová, 2012). Pro odfiltrování autokorelace z náhodné složky modelu je možné využít **modifikaci odhadu běžnou metodou nejmenších čtverců podle Čechury (2021)**. Výpočet spočívá ve třech krocích. Nejdříve je model odhadnut pomocí BMNČ, poté je v druhém kroku vytvořen kvadrát reziduí odhadnuté modelu. Třetím krokem je nový odhad modelu pomocí BMNČ i se zahrnutím právě získaného kvadrátu reziduí

zpožděného o 1 období. Pokud je tento kvadrát reziduí v modelu statisticky významný, povedlo se odfiltrování autokorelace z náhodné složky modelu na tento kvadrát (Čechura, a další, 2021).

2.2.10 Verifikace modelu

Před aplikací odhadnutého ekonometrického modelu je nutné provést verifikaci. Tedy ověřit, zda jsou odhadnuté parametry v souladu s výchozími hypotézami a zda splňují požadované ekonomické, statistické, ekonometrické a matematické charakteristiky (Hušek, 1995).

Ekonomická verifikace

Ekonomická verifikace spočívá v posouzení směru a intenzity působení vysvětlujících proměnných na proměnnou vysvětlovanou. Směr je udán znaménkem před parametrem a intenzita je udána hodnotou parametru. Model je ekonomicky verifikován, pokud směr a intenzita působení parametrů odpovídá očekávání podle ekonomických teorií (Hušek, 2009).

Statistická verifikace

Statistická verifikace spočívá v posouzení statistické významnosti odhadnutých parametrů i celého modelu jako celku. Mezi nejpoužívanější kritéria statistické významnosti patří standardní chyby odhadnutých parametrů, koeficienty vícenásobné determinace, t-test a F-test (Hušek, 1995).

Testování hypotéz se dle Hančlové (2012) řídí statistickou teorií o testování hypotéz. Toto testování je rozděleno do 3 kroků.

1. Formulace nulové hypotézy (H_0) a alternativní hypotézy (H_1)
2. Vypočtení testovací statistiky
3. Rozhodnutí o přijetí či zamítnutí nulové hypotézy pro zvolenou hladinu významnosti α . Testovací statistika je nalezena za předpokladu platnosti H_0 , zvolené hladiny významnosti, stanovené kritické hodnoty a porovnání vypočtené statistiky s kritickou hodnotou. Statistický test se dá provést s pomocí kritického oboru testovací statistiky, s pomocí p-hodnoty nebo pomocí intervalu spolehlivosti.

Statistickou významnost jednotlivých parametrů je možno určit pomocí **t-testu**.

Stanovíme si následující hypotézy:

$H_0: \beta_i = 0$, β_i parametr je statisticky nevýznamný

$H_1: \beta_i \neq 0$, β_i parametr je statisticky významný

K vyhodnocení platnosti H_0 porovnáme vypočtenou p-hodnotu s zvolenou hladinou významnosti α (zpravidla $\alpha=0,01;0,05;0,1$). Pokud je p-hodnota nižší než zvolená hladina významnosti, potom zamítáme H_0 ve prospěch alternativní H_1 (Hančlová, 2012).

Vhodnost modelu jako celku je posuzována obdobně pomocí **F-testu** (Fisherova testu). Opět jsou stanoveny hypotézy:

$H_0: \beta_i = 0$, β_i jsou statisticky nevýznamné koeficienty

$H_1: \beta_i \neq 0$, β_i jsou statisticky významné koeficienty

K vyhodnocení platnosti H_0 porovnáme vypočtenou p-hodnotu se zvolenou hladinou významnosti α . Pokud je p-hodnota nižší než zvolená hladina významnosti, potom zamítáme H_0 ve prospěch alternativní H_1 (Hančlová, 2012).

Shoda modelu s daty je posuzována pomocí **koeficientu determinace (R^2)**. Ten udává, z kolika % jsou změny závisle proměnné vysvětleny změnami nezávisle proměnné. Je založen na rozkladu celkového rozptylu vysvětlované proměnné (S_y^2) na rozptyl teoretický ($S_{\hat{y}}^2$) a reziduální (S_u^2). Tento R^2 má tendence narůstat s přidáním dalších vysvětlujících proměnných do modelu, z tohoto důvodu je využíván korigovaný (adjustovaný) koeficient determinace ($\overline{R^2}$), kde p je počet odhadovaných parametrů v rovnici a n je délka časové řady (Hindls, a další, 2007).

$$S_y^2 = S_{\hat{y}}^2 + S_u^2 \quad (10)$$

$$R^2 = 1 - \frac{S_u^2}{S_y^2} \quad (11)$$

$$\overline{R^2} = 1 - (1 - R^2) \frac{n-1}{n-p} \quad (12)$$

Ekonometrická verifikace

Tvrdoň (2001) uvádí, že ekonometrická verifikace ověřuje nezbytné podmínky pro úspěšnou aplikaci ekonometrických metod. Pokud by došlo k nesplnění jednoho či více kritérií, může dojít ke zkreslení modelu. Mezi kritéria patří:

1. Nepřítomnost autokorelace.
2. Nepřítomnost heteroskedasticity.

3. Normální rozdělení náhodných složek.

Autokorelace je v modelu testována pomocí **Breusch-Godfreyova testu** pro autokorelaci prvního řádu. Stanovíme si následující hypotézy:

H₀: Není přítomna autokorelace

H₁: Je přítomna autokorelace (Hušek, 1995)

Přítomnost **heteroskedasticity** se zjišťuje pomocí **Whiteova testu**. Hypotézy jsou stanoveny následovně.

H₀: Není přítomna heteroskedasticita

H₁: Je přítomna heteroskedasticita (Hušek, 1995)

Pro určení **normality rozdělení** se využívá **Chí-kvadrát test** s následujícími hypotézami.

H₀: Náhodné chyby jsou normálně rozděleny

H₁: Náhodné chyby nejsou normálně rozděleny (Hušek, 1995).

Pro ověření **specifikace modelu** (vhodné funkční formy) je možné využít **Ramseyův RESET test**. Jsou definovány hypotézy:

H₀: Specifikace modelu je adekvátní

H₁: Specifikace modelu není adekvátní (Hušek, 1995).

Stabilita parametrů je možná otestovat pomocí **Harvey-Collierova CUSUM testu**. Definovány jsou následující hypotézy:

H₀: Žádná změna v parametrech modelu

H₁: Změna v parametrech modelu (Hušek, 1995).

Multikolinearita vyjadřuje závislost mezi vysvětlujícími proměnnými a zjišťuje se například pomocí **korelační matice**. Korelační matice je naplněna párovými korelačními koeficienty. Pokud se vyskytují mezi predeterminovanými proměnnými hodnoty vyšší než |0,8|, zejména vyšší než |0,9|, značí to problém multikolinearity. Při vysoké multikolinearitě není možné separovat vliv dotčených vysvětlujících proměnných na vysvětlovanou proměnnou. Pokud je závislost mezi dvěma predeterminovanými proměnnými deterministická, dochází k perfektní multikolinearitě. Ta znemožňuje odhadnout regresní koeficienty. Vysoká korelovanost mezi vysvětlovanou proměnnou a predeterminovanými proměnnými neznamena multikolinearitu a je naopak žádaná (Cipra, 2013).

Dle Huška (1995) je možné vysokou multikolinearitu odstranit několika způsoby:

- Vyloučením korelované proměnné.
- Provedení prvních diferencí nebo relativních odchylek na podkladových datech.
- Ignorováním proměnné.
- Nahrazením vektoru proměnné, která problém způsobuje, dummy proměnnou.

2.2.11 Využití ekonometrického modelu

Dle Huška (1995) je odhadnutý ekonometrický model možné aplikovat v následujících oblastech:

- Kvantifikace a verifikace ekonomických hypotéz na makroúrovni.
- Zkoumání mikroekonomických vztahu na mikroúrovni.
- Analýza vývoje v chování zkoumaného systému (predikce ex-post).
- Předpověď budoucích hodnot vysvětlovaných proměnných.

Strukturální analýza

K aplikaci modelu v oblasti strukturální analýzy se často využívá koeficientů pružnosti (elasticity). Odhadnutý parametr udává, jak zvolená vysvětlující proměnná působí na vysvětlovanou proměnnou v jednotkách, v jakých jsou obě proměnné sledovány. Elasticita umožňuje vyjádřit toto působení relativně, tedy v procentech. Tím je umožněno porovnat intenzitu působení jednotlivých vysvětlujících proměnných na vysvětlovanou proměnnou, i když jsou vyjádřeny v rozdílných jednotkách (Hindls, a další, 2007).

$$E = \frac{dy}{dx_i} \frac{x_i}{\hat{y}} \quad (13)$$

Predikce a ex-post

Hančlová (2012) uvádí, že predikce ex post představuje předpověď vysvětlované proměnné, při které jsou známy hodnoty všech vysvětlujících proměnných s jistotou pro predikované období. Prognóza má negativní prognostický horizont a ověřuje prognostické vlastnosti modelu. Všeobecně totiž není platné, že model, který vyhovuje kritériím verifikace v období pozorování, je vhodný pro předpověď. Dle Cipry (2013) je určení

přesnosti prognózy možné pomocí průměru čtverce chyby prognózy (MSE) a střední průměrné kvadratické chyby prognózy (RMSE).

$$\text{MSE} = \frac{1}{n} \sum_{i=1}^n (y_i - \hat{y}_i)^2 \quad (14)$$

$$\text{RMSE} = \sqrt{\text{MSE}} \quad (15)$$

3 Teoretická východiska

3.1 Úvod do světa kryptoměn

V následujících podkapitolách bude vysvětlen důvod vzniku Bitcoinu a myšlenka, která vedla Satoshiho Nakamota k vytvoření tohoto platebního systému. Na úvod bude vysvětleno několik důležitých termínů potřebných k pochopení zkoumané problematiky.

Myšlenka Bitcoinu a jeho vznik

Podle Nakamota (2008) je obchodování na internetu téměř z celé části závislé na finančních institucích, které při probíhajícím obchodu hrají roli důvěryhodné třetí strany, prostředníka, který musí transakci schválit a potvrdit. Ačkoliv tento zaběhlý model funguje pro většinu transakcí dostatečně, je stále založen na důvěře v třetí stranu, která zprostředkovává transakci a transakce není nevratná. V některých případech ale tento model nedostačuje a mohl by být nahrazen dokonalejším platebním systémem. Zprostředkování transakce třetí stranou totiž do transakce zanáší další poplatky a omezení týkající se transakčních nákladů, nákladů na řešení problémů s transakcemi, minimální velikosti transakce a také nemožnosti provést nevratnou platbu za nevratnou službu.

Zde se nabízí možnost vytvořit decentralizovaný elektronický platební systém typu klient-klient, který místo na důvěře ve finanční instituce bude založen na kryptografii a umožní kterémukoli dvěma stranám provést přímou nevratnou transakci bez nutnosti použít další důvěryhodnou osobu nebo instituci. Nakamoto (2008) ve svém článku „*Bitcoin: a Peer-to-Peer Electronic Cash System*“ nabízí možnost, jak vyřešit problém tzv. dvojí útraty, a říká, že tento systém, který pojmenovává „*Bitcoin*“, bude bezpečný tak dlouho, jak dlouho budou poctivé uzly ovládat dohromady většinu výpočetního výkonu sítě.

Když Satoshi Nakamoto (2008) zveřejnil 31. 10. 2008 na fóru bitcoin.org průvodní článek Bitcoinu, který popisoval myšlenku a fungování tohoto nového platebního systému, započala nová etapa, která přetrvává dodnes. Již krátce na to byl 3. 1. 2009 Bitcoin oficiálně spuštěn spolu s vytvořením prvního bloku blockchainu (tzv. „*genesis block*“) spolu s prvními 50 bitcoiny. Od této chvíle budou všechny transakce, které proběhly do současnosti, a které v budoucnu proběhnou, zaznamenány v blockchainu, který si lze pro zjednodušení prozatím představit jako obrovskou neměnnou účetní knihu. Po spuštění

Bitcoinu se o něj začali zajímat nadšenci a vývojáři, kteří si navzájem posílali transakce, nové návrhy na zlepšení a testovali tento systém. Satoshi Nakamoto poté v roce 2010 předal jednomu z nadšenců, kterým byl Gavin Andresen (později hlavní vývojář projektu), doménu bitcoin.org a ustoupil do ústraní.

Tvůrce Bitcoinu: Satoshi Nakamoto

Za celou dobu od vzniku Bitcoinu se stále kolem jeho tvůrce, Satoshiho Nakamota, točí tajemství a nejistota. Nikdo totiž neví, kdo je tento záhadný tvůrce. Podle propracovanosti systému je pravděpodobné, že se nejedná o jednu osobu, ale o skupinu osob, které vystupují pod daným pseudonymem. Pro vytvoření takového platebního systému bylo zajisté nutné disponovat hlubokými znalostmi kryptografie, programování a ekonomických teorií. Dále je známé, že ať už je Satoshi Nakamoto kdokoliv, tak velmi dbá na svou anonymitu a nezanechává sledovatelné stopy. Navzdory jménu pocházejícímu z Japonska se komunita shoduje na tom, že vzhledem k jeho perfektní angličtině může jít o někoho z anglicky mluvících zemí. Sám Nakamoto ale tuto skutečnost nikdy nenaznačil. Jedinou informací, kterou o sobě zanechal, je jeho věk. Na fóru P2P foundation uvedl ve svém profilu datum narození 5. 4. 1975, je však možné, že toto datum je pouze symbolické. Tvůrce Bitcoinu se krátce po jeho spuštění v roce 2010 zřekl role hlavního vývojáře a odmlčel se až do roku 2014. Na Bitcoinovém fóru bitcointalk.org (2009) lze u jeho profilu pozorovat, že byl naposledy aktivní 13. 12. 2010.

Tajemná identita vyvolala vlnu pátrání, jak u vznikající Bitcoinové komunity, tak u novinářů. Jako možní autoři Bitcoinu byly postupně označeni matematik Shinichi Mochizuki, dále trojice autorů Neal King, Vladimir Oksman a Charles Bry. Všichni ale spojení odmítli a hledání pokračovalo dál. Z dalších hledaných tvůrců je možné uvést Michaela Cleara (student kryptografie, který psal o sítích klient-klient), Hala Finneyho, Gavina Andresena a Jeda McCaleba (významní vývojáři Bitcoinu), nebo Rosse Ulbrichta (zakladatel ilegálního tržiště Silk Road). Vrchol hledání proběhl v roce 2014, kdy se uskutečnila velká mediální masáž Japonce Dorian Nakamota, který v Kalifornii pracoval jako systémový inženýr. Ten však odmítal práci na projektu Bitcoin a v souvislosti s tímto označením se naposledy ozval i Satoshi Nakamoto (2014), který na fóru P2P foundation 7. 3. 2014 napsal pod svůj původní příspěvek, vysvětlující Bitcoin, komentář ve znění „*I am not Dorian Nakamoto*“ (Nejsem Dorian Nakamoto). V roce 2016 se o autorství začal

sám od sebe hlásil podnikatel Craight Wright, který ale nebyl schopen podat jediný důkaz pro své tvrzení. V současné době vypadá jako nejpravděpodobnější tvůrce maďarský programátor Nick Szabo, vše jsou to ale jen domněnky (Stroukal, a další, 2021).

Základní termíny spojené s kryptoměnami

Bitcoin s velkým „B“ je decentralizovaná platební síť v internetu, využívající architekturu klient-klient. Síť spravuje veškerou historii transakcí mezi jejími uzly. Jednotka měny se též nazývá bitcoin, v tomto případě ale s malým „b“ (Stroukal, a další, 2021).

Uzel („Node“) je nezávislá jednotka v Bitcoinové síti. Každý úplný uzel obsahuje kompletní kopii blockchainu a působí na informace přenášené skrze nezabezpečená síťová připojení, každý uzel může dojít ke stejnému závěru jako ostatní uzly a ověřit správnost kopie blockchainu, který působí jako veřejný účetní systém. Pomocí mechanismu, jakým uzly fungují, je zajišťován vznik shody a bezpečnost celého blockchainu. K dosažení shody ale není dosahováno explicitně, každý uzel působí samostatně a řídí se jasně danými pravidly. Shoda je dosahována asynchronním působením desítek tisíc nezávislých úplných uzlů (Antonopoulos, 2014).

Blockchain je účetní kniha všech transakcí provedených v Bitcoinovém protokolu. V této účetní knize jsou zachyceny všechny potvrzené (vytěžené) bloky a v nich zahrnuté transakce v neměnné podobě. Každý si může jakýkoliv záznam z této účetní knihy zobrazit a sám ověřit. Blockchain nahrazuje potřebu třetí strany, která by dohlížela nad prováděním transakcí (Coen, 2019).

3.2 Těžba kryptoměn

Těžba je proces, kterým se získávají nové jednotky kryptoměny. Antonopoulos (2014) popisuje, že pro Bitcoin, a jemu podobné, je používán proces těžby založený na důkazu práce („*proof of work*“). Další rozdílné kryptoměny ale mohou vznikat rozdílnými způsoby, jako je například důkaz vlastnictví („*proof of stake*“). Hlavním úkolem těžby ale není vytvářet nové mince, klíčová úloha spočívá v zajištění bezpečnosti daného systému a ochraně před tvorbou dvojí útraty (utracení totožné kryptoměny více, než jednou). Pro pochopení procesu těžby je nutné porozumět termínům, jako je hash, blok, nonce, pool, mempool a halving.

Hash je výsledkem hashovací funkce, která je kryptografickým zobrazením množiny dat obecné délky do množiny dat omezené délky. Je možné zobrazit například soubor s libovolnou délkou do množiny 256bitových čísel. Takováto funkce musí být vysoce nelineární a mít asymetrickou složitost zpětného výpočtu. V Bitcoinovém protokolu je využívána funkce SHA-256, pomocí které jsou těženy bloky. Hash tvoří název bloku (Chilamkurti, a další, 2021).

Blok („*Block*“) je datová struktura v Bitcoinovém protokolu. Jednotlivé bloky tvoří blockchain, který uchovává všechny dosud potvrzené transakce. V každém bloku jsou zakódované všechny transakce, které se rozhodli těžaři do daného bloku zahrnout. Právě jedna z transakcí je mincovorná generující transakce, která dle pravidel protokolu tvoří nové bitcoiny a odměňuje s nimi těžaře, který blok vytvořil. Zbylé transakce v bloku jsou uživatelů Bitcoinové sítě (Stroukal, a další, 2021).

Nonce je číslo, které je těžaři přidáváno k vytvořené hlavičce bloku za účelem nalezení takového hashe hlavičky bloku, který bude nižší než stanovený obtížnostní cíl. Pokud je těžařem nalezena správná hodnota nonce, a hash hlavičky bloku tedy plní podmínku obtížnostního cíle, je takto vytvořený blok vytěžen. (Kaliský, 2018).

Pool je sdružení těžařů, kteří těží společně. Nově vzniklé mince včetně poplatků tak putují do vlastnictví poolu. Ten je poté rozděluje mezi své členy podle jejich poskytnutého podílu na výpočetním výkonu celého poolu. Pool tímto způsobem zvyšuje frekvenci úspěšného nalezení nového bloku a tím i frekvenci výplat členů poolu (Slush Pool, 2021).

Mempool je virtuální prostor, do kterého se vkládají vytvořené čekající nepotvrzené transakce. Je to svým způsobem čekárna pro transakce, které doposud těžaři nezahrnuli do bloku. Není to však jedno velké úložiště, každý uzel má svůj vlastní mempool a získané transakce rozšiřuje mezi další uzly. Těžaři si poté z mempoolu vybírají transakce, které se rozhodnou zahrnout do připravovaného bloku (Binance academy, 2021).

Půlení („*halving*“) je situace, která nastává v Bitcoinovém protokolu přibližně jednou za 4 roky (přesně jednou za 210 000 vytěžených bloků). Jak už název napovídá, jedná se zde o půlení odměny pro těžaře za vytěžený blok. První základní blok vznikl spolu s 50 bitcoiny, po 4 letech se odměna snížila na 25 bitcoinu a postupem času se dostala až na současnou odměnu za vytěžený blok, která je 6,25 bitcoinů. Nejbližší půlení odměny nastane za méně než 151 000 bloků. Časově to odpovídá období přibližně kolem dubna 2024 (CoinMarketCap, 2021).

3.2.1 Proof of work (PoW)

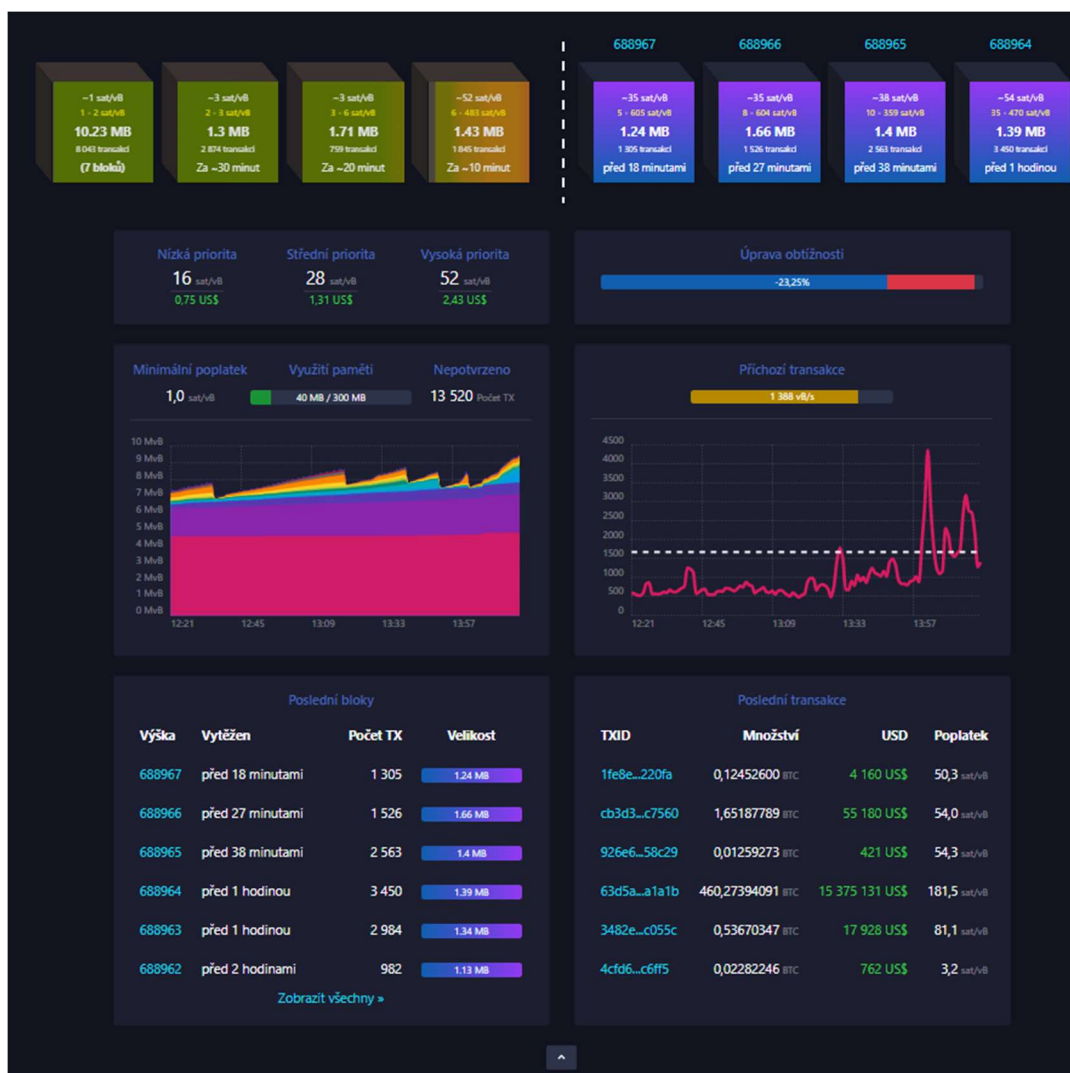
Způsob těžby důkazem práce bude rozveden nejdříve, protože se tento proces využívá pro těžbu Bitcoin a je také nejrozšířenější. Je možné, že slovo “těžba“ může být matoucí, protože kryptoměna se ve skutečnosti nijak fyzicky netěží, z její podstaty to ani není možné. Zjednodušeně je možné říct, že těžba je řešení matematické úlohy, která není nijak náročná, ale je potřeba ji vyřešit mnohokrát, aby bylo získáno správné řešení. Postup, pomocí kterého se tvoří nové mince, je takto nazývám z důvodu, že odměna je stále se zmenšující a podobá se zmenšujícím se výnosům při skutečné těžbě drahého kovu. Tento systém zmenšování odměny, kterému se říká půlení („halving“), bude popsán později (Antonopoulos, 2014).

Jak již bylo řečeno, vytvoření nových mincí není hlavním úkolem těžby. Je to pouze pobídka pro těžaře, která je motivuje k zabezpečování sítě a zároveň tvoří měnovou zásobu. Těžba se provádí pro udržení bezpečnosti Bitcoinové sítě, pro ověření probíhajících transakcí a pro jejich zaznamenání do blockchainu v neměnné podobě. V případě těžby důkazem práce je to prováděno poskytnutím výpočetního výkonu do Bitcoinové sítě. Za tuto službu jsou těžaři odměněni bitcoiny, které se skládají jak z nově vytvořených bitcoinů vygenerovaných v nově vytěženém bloku, tak také z transakčních poplatků, které platí odesílatelé transakcí (Antonopoulos, 2014).

Poté, co byla vytvořena transakce odesílatelem bitcoinů (proces tvorby a odesílání transakcí bude popsán v kapitole Používání Bitcoinu), je uložena do prostoru zvaného „*mempool*“, kde čeká, dokud se ji nerozhodnou těžaři zařadit do těženého bloku. Doba, po kterou zůstává transakce v mempoolu, je závislá na aktuální velikosti mempoolu (počet čekajících nepotvrzených transakcí) a na poplatku, který se za transakci rozhodne odesílatel zaplatit (Kaliský, 2018).

Aktuální zaplněnost mempoolu a vhodnou výši poplatku je možné nalézt na stránce mempool.space (2021). Dle aktuálních dat z 27. 6. 2021, 14:20 čeká v mempoolu 13 520 nepotvrzených transakcí, nízká velikost poplatku činí 16 sat/vB, střední priorita transakce 28 sat/vB a vysoká priorita 52 sat/vB. Stránka dále zobrazuje předchozí vytěžené bloky a transakce, které bloky obsahují.

Obrázek 1: Mempool



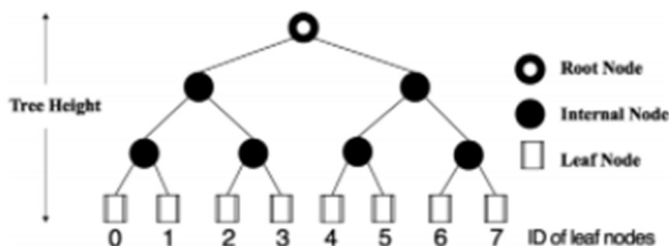
Zdroj: (Mempool.space, 2021)

Antonopoulos (2014) popisuje, že těžaři, kteří jsou speciálním případem uzlů, skládají právě zmiňované nepotvrzené transakce, které jsou odloženy v mempoolu, do nových bloků. Vytvoření nového bloku je svým způsobem malý závod mezi těžaři, kteří se snaží jako první správně sestavit a potvrdit právě svůj blok. Těžář, který úspěšně vytěží blok, ho odešle mezi zbylé uzly, které potvrdí jeho správnost a zařadí ho do blockchainu. V tu samou chvíli začíná další malý závod, ve kterém se těžaři snaží o vytěžení následujícího bloku. Samotný výběr transakcí a jejich složení do bloku není náročné.

Transakce jsou těžářem zvoleny podle výše poplatků, dále z nich začne vytvářet binární „merkle tree“. Tento strom obsahuje všechny transakce (ve formě jeho „listů“), které budou do bloku zahrnuty. Jde o postup, při kterém jsou hashe 2 transakcí znovu přepočteny hashovací funkcí a vznikne z nich jeden výsledný hash, tímto způsobem strom

klesá až ke svému kořeni, kde zůstává jeden výsledný hash, který obsahuje všechny zařazené transakce. Tento konečný hash je nazýván „merkle root“, tedy kořen sestaveného stromu. Na následujícím obrázku je zobrazen merkle tree s výškou 4, v případě tvorby merkle tree pro potřeby nového bloku jsou zařazovány stovky až nižší jednotky tisíců transakcí. Merkle tree je tedy značně vyšší (Blockchain - ICBC 2018, 2018).

Obrázek 2: Merkle tree s výškou 4



Zdroj: (Blockchain - ICBC 2018, 2018)

Nyní přichází nejnáročnější část práce, těžař musí nalézt správnou hodnotu „nonce“, aby výsledný hash hlavičky bloku byl nižší než hodnota nastaveného obtížnostního cíle. v následující tabulce lze vidět obsah hlavičky bloku (Binance academy, 2021).

Tabulka 1: Obsah hlavičky bloku

Velikost	Název pole	Český popis
4 byty	Version	Verze Bitcoinového protokolu
32 bytů	Previous Block Hash	Hash předchozího bloku zařazeného v blockchainu
32 bytů	Merkle root	Vypočtený kořen "merkle tree" pro aktuální blok
4 byty	Timestamp	Časová značka vytvořeného bloku
4 byty	Difficulty Target	Stanovený obtížnostní cíl pro daný blok
4 byty	Nonce	Hodnota hledaná algoritmem pro důkaz práce

Zdroj: (Vlastní zpracování dle Antonopoulou, 2014)

V současné době je obtížnostní cíl nastaven na číslo 19,39 bilionů, to odpovídá nutnost nalézt hash hlavičky bloku začínající 19 nulami. S aktuálním výkonem sítě kolem 100 EH/s jsou každou sekundu prováděny triliony pokusů nalézt správnou hodnotu nonce a vytěžit sestavený blok. Nový blok je nalezen v průměru každých 10 minut, protože Bitcoinový protokol automaticky každých 2016 bloků (cca 14 dní) upraví obtížnostní cíl podle aktuálního celkového výpočetního výkonu celé sítě tak, aby doba pro nalezení nového bloku odpovídala času 10 minut. Obtížnostní cíl se ale nemusí pouze zvyšovat, pokud klesá výpočetní výkon sítě, tak je obtížnostní cíl upraven i na opačnou stranu, aby bylo stále v možnostech zbylých těžařů nalézt blok každých 10 minut. Nejbližší následující úprava obtížnostního cíle proběhne 3. 7. 2021 a za současné situace předpokládá snížení

obtížnostního cíle o přibližně 25 %. To bude znamenat obtížnostní hodnotu okolo 15,27 bilionů (BTC.com, 2021).

Pro lepší představu je na následujícím obrázku znázorněno hledání vyhovující hodnoty nonce, která musí být nižší než stanovený obtížnostní cíl.

Obrázek 3: Hledání vyhovující nonce



Zdroj: (Pritzker, 2020)

V následující tabulce jsou sepsány podle Antonopoulose (2014) všechny složky, které obsahuje těžený blok. Drtivou většinu jeho velikosti tvoří transakce, jedna transakce má velikost alespoň 250 bytů a blok obsahuje stovky až tisíce transakcí. Oproti tomu hlavička bloku má velikost pouze 80 bytů.

Tabulka 2: Struktura bloku
















Velikost	Název pole	Český popis
4 byty	Block Size	Velikost bloku v kilobytech
80 bytů	Block Header	Položky tvořící hlavičku bloku
1-9 bytů	Transaction Counter	Kolik transakcí následuje
Různé	Transactions	Transakce zaznamenané v daném bloku

Zdroj: (Vlastní zpracování dle Antonopoulose, 2014)

Po úspěšném nalezení správné nonce a vytěžení bloku získá těžař odměnu, výše odměny je závislá na půlení, které probíhá přibližně každé 4 roky. v současné době činí odměna 6,25 bitcoinu. Dále těžař získá poplatky za jednotlivé transakce. Po přepočtení na hodnotu v korunách vychází dle dnešního (28. 6. 2021) kurzu směnárny Coinmate (2021) 6,25 BTC na přibližně 4,6 milionu korun. Je tedy zřejmé, že při takto vysokých odměnách a velikosti výpočetního výkonu sítě musí být těžba pro jednotlivce téměř nemožná. Z ekonomických důvodů se tedy těžaři spojují do poolů a provádějí těžbu společně, získané odměny si pak proporcionalně rozdělují. Tímto způsobem mají šanci na získání odměny i malí těžaři, kteří by na vlastní pěst vytěžili úspěšně blok jen velmi nepravděpodobně (Stroukal, a další, 2021).

Na následujícím obrázku je zachycen seznam největších těžebních skupin, ve kterých se těžaři sdružují. Zajímavé je zmínit Slush pool, který dle Braiins (2021) vznikl v roce 2010 jako vůbec první pool na světě a byl založen v České republice Markem Palatinem, který si přezdívá „Slush“.

Obrázek 4: Přehled poolů

Ranking	Pools	Hashrate	Share	Blocks Mined	Empty Blocks Count (Percentage)	Avg. Tx Fees Per Block (BTC)	Tx Fees/ Block Reward	Last Block
0	NETWORK	92295.21 PH/s	100.00%	247	0(0%)	0.42261598	6.76%	689.038
1	 F2Pool	12704.60 PH/s	13.77%	34	0(0%)	0.49142024	7.86%	689.035
2	 AntPool	11583.61 PH/s	12.55%	31	0(0%)	0.37932548	6.07%	689.038
3	 ViaBTC	10836.28 PH/s	11.74%	29	0(0%)	0.46667692	7.47%	689.020
4	 Binance Pool	10462.62 PH/s	11.34%	28	0(0%)	0.43308360	6.93%	689.032
5	 Poolin	10088.95 PH/s	10.93%	27	0(0%)	0.40809829	6.53%	689.037
6	 BTC.com	9715.29 PH/s	10.53%	26	0(0%)	0.46600419	7.46%	689.030
7	 Foundry USA	7473.30 PH/s	8.10%	20	0(0%)	0.43810853	7.01%	689.034
8	unknown	6352.30 PH/s	6.88%	17	0(0%)	0.36829112	5.89%	689.036
9	 SlushPool	5604.97 PH/s	6.07%	15	0(0%)	0.29235685	4.68%	688.993
10	 Rawpool	2989.32 PH/s	3.24%	8	0(0%)	0.39736875	6.36%	689.012
11	 EMCDPool	1120.99 PH/s	1.21%	3	0(0%)	0.32141506	5.14%	688.941
12	 SBI Crypto	1120.99 PH/s	1.21%	3	0(0%)	0.45588894	7.29%	689.029
13	 Sigmoidpool.com	747.33 PH/s	0.81%	2	0(0%)	0.35358409	5.66%	688.962
14	 BTC.TOP	747.33 PH/s	0.81%	2	0(0%)	0.33249835	5.32%	688.968
15	 SpiderPool	373.66 PH/s	0.40%	1	0(0%)	0.66857412	10.70%	688.974
16	 WAYL.CN	373.66 PH/s	0.40%	1	0(0%)	0.16396028	2.62%	688.930

Zdroj: (BTC.com, 2021)

3.2.2 Proof of stake (PoS)

Mezi další možnosti těžby kryptoměn patří algoritmus důkazu vlastnictví („*proof of stake*“). Dle Mathise (2018) je tento způsob těžby a potvrzování transakcí zcela odlišný od algoritmu důkazu práce, na kterém funguje Bitcoinová síť. Žádný výpočetní výkon zde nehraje roli a místo těžařů zde hrají roli validátoři a delegátoři. Aby se mohl člověk stát validátorem, musí mít k dispozici určitý obnos kryptoměny, kterou chce validovat. Ten, kdo nemá tento potřebný obnos se může stát delegátorem a své malé množství kryptoměny delegovat nějakému z ověřených validátorů. Model proof of stake nespolehá tedy na těžaře, validátoři se zde zaručují svými kryptoměnami za správnost bloku, který chtějí potvrdit. Šance na úspěšné potvrzení bloku a obdržení odměny je náhodná. Následně si pak odměnu nechává validátor, nebo po odečtení svého poplatku rozděluje část odměny

delegujícím. Pokud by se validátor snažil z jakéhokoli důvodu potvrzovat chybné transakce, bude jeho kryptoměna, kterou se zaručil, navždy ztracena. Část svého držení balíčku může validátor ztratit i v případě, že bude offline a nebude tudíž úspěšně validovat.

Koncem roku 2020 bylo spuštěno Ethereum 2.0, které funguje na algoritmu PoS. Do budoucna je plánován kompletní přechod Etherea z PoW na PoS a těžba Etherea kompletně zanikne. Pro možnost stát se validátorem v síti Etherea 2.0 je nutné disponovat 32 ethery. Při menších částkách je možné ether pouze delegovat. Při aktuální ceně (28. 6. 2021) 45 000 Kč/ETH je nutné vlastnit ether v hodnotě téměř 1,5 milionu korun. z tohoto důvodu se objevuje názor, zda nebude přechod Etherea na Ethereum 2.0 zvyšovat centralizaci sítě (Ogino, 2021).

3.3 Změna Bitcoinového protokolu

Již bylo uvedeno, že Bitcoinový protokol funguje jako decentralizovaná platební síť typu klient-klient, nové transakce jsou do systému zapisovány pomocí důkazu vykonané práce a každý z uzlů může veškerou historii transakcí zobrazit a ověřit. Odkud ale pocházejí pravidla, podle kterých Bitcoin funguje? A jak tato pravidla mohou být měněna a upravována, když nad Bitcoinovým protokolem není žádná autorita ani správce, který by je mohl implementovat?

Bitcoin je software typu open source, což znamená, že každý může do jeho zdrojového kódu nahlížet a také do své kopie přidat jakékoli změny. Do Bitcoinového protokolu (softwaru, který se řídí podle určité množiny pravidel) je možné vkládat každým uzlem, který má jeho kopii uloženou, libovolné modifikace, pokud budou stále dodržována pravidla sítě. Nejznámější a nejrozšířenější implementací je Bitcoin Core, který byl vytvořen Satoshi Nakamotem. Pokud nějaký z uzlů provede modifikaci, která pravidlům neodpovídá, nebudou jím vytěžené bloky potvrzeny a přijaty zbylými uzly v síti. Systém je totiž distribuovaný a na nových pravidlech se musí shodnout všechny uzly (Pritzker, 2020).

3.3.1 Bitcoin Improvement Proposal (BIP)

Takzvaný „BIP“ je dokument, kterým je navrhována úprava Bitcoinového protokolu a implementace změn. Jak již bylo uvedeno, Bitcoin je open source, a tudíž každý může vytvořit a publikovat BIP, aby ale vstoupil v platnost, je nutné jeho schválení Bitcoinovou komunitou. Pokud je návrh přínosný a komunita má zájem o jeho implementaci, je

prováděno přísné experimentální posuzování kódu a hledání nedostatků. Kód je veřejný, a proto může být revidován a komentován kýmkoliv. Jednotlivé návrhy se označují písmeny BIP a pořadím návrhu (Antonopoulos, 2014).

V současné době je aktuální BIP 0341, 0342 a 0343, který společně zavádí do Bitcoinu „Taproot“. BIP 0341, který navrhl 19. 1. 2020 Pieter Wuille (2022), procházel úspěšným signalizačním obdobím od 30. 5. 2021 do 13. 6. 2021 (přibližné období těžby 2016 bloků po kterém se změní obtížnostní cíl těžby). V tomto časovém okně mají těžařské pooly za úkol vyjádřit svůj postoj k zavedení Taprootu. Při úspěšném vytěžení bloku označují blok souhlasem nebo nesouhlasem se zavedením změny. Po skončení období je potřeba obdržet 90 % podporu pro implementaci Taprootu. Těžařské pooly se na podpoře z většiny shodly a 12. 6. 2021 byl českým „Slush pool“ (který zrovna tak označil i první blok podporující Taproot) označen poslední potřebný blok, 1815 z 2016 (blok č. 687 285), pro překročení 90% hranice podpory. Implementace a aktivace Taprootu by měla proběhnout v bloku 709 632, který časově odpovídá přibližně 12. 11. 2021. Po dlouhé době proběhne tedy významná změna v Bitcoinovém protokolu, poslední velkou změnou byl v roce 2017 BIP 0091 aktivující SegWit (Osato, 2021).

Dříve než bude vysvětleno, co vlastně implementace Taprootu přinese, je vhodné uvést jakým způsobem je v Bitcoinové síti potvrzováno vlastnictví doposud. Od dob vzniku Bitcoinu je využíván protokol digitálního podpisu s využitím eliptických křivek („*Elliptic Curve Digital Signature Algorithm*“). Tyto eliptické křivky umožňují ze soukromého klíče („*private key*“) odvodit veřejné klíče („*public key*“). Proces je ale jednoduché provést jen jedním směrem, v současné době je nemožné zjistit na základě veřejného klíče hodnotu klíče soukromého (a tím získat přístup k bitcoinům protistrany). Více o problematice transakcí bude uvedeno v kapitole **Používání Bitcoinu** (Binance academy, 2021).

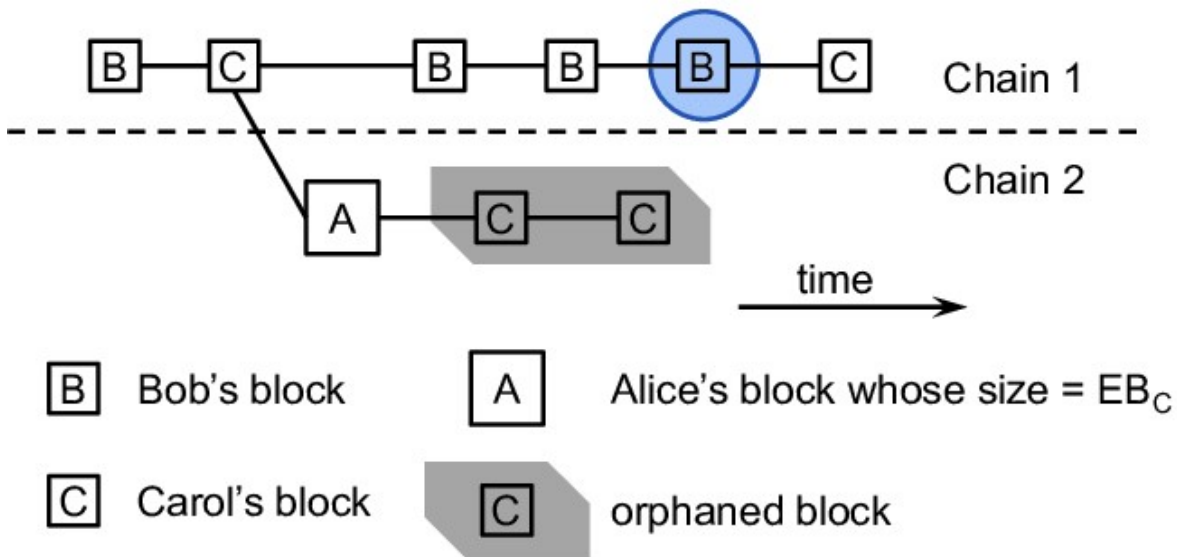
Co to onen „Taproot“ vlastně je? Jedná se o rozšíření Bitcoinového protokolu typem „*softfork*“. Hlavním přínosem Taprootu jsou Schnorrové podpisy („*Schnorr signature*“), které oproti doposud využívanému protokolu digitálního podpisu s využitím eliptických křivek zajistí větší soukromí odesílatele bitcoinů a zjednoduší práci se složitějšími transakcemi, které se nakonec zobrazí jako jednoduchá transakce z jednoho bodu do druhého. Velký přínos hrají Schnorrové podpisy pro vytváření vícepodpisových („*multisignature*“) transakcí. Jedná se o transakce, které vyžadují pro provedení podpis

(schválení) více soukromými klíči, jako například při správě kryptoměn ve firmě. Do současné doby bylo při provedení takové transakce možné dohledat v blockchainu skutečnost, že transakce byla podepsána více soukromými klíči. Nově se ale bude, s použitím Schnorrova podpisu, vícepodpisová transakce jevit jako transakce podepsána jedním prostým soukromým klíčem, protože podpisy agreguje do jediného „*master signature*“. BIP 0341 tedy přinese jak zvýšení anonymity pro používání vícepodpisových transakcí, kdy nebude možná dohledat v blockchainu skutečnost, že se jedná o takovýto typ transakce a už vůbec nebude možné odhalit, kolik podpisů a koho podpisy byly použity. Další výhodou je snížení množství přenesených a uložených dat do blockchainu a s tím i možnost vložit více transakcí do bloku a za jednotlivé transakce zaplatit nižší poplatky. Implementace Taprootu má vliv i na „*Lightning network*“, o kterém bude psáno v kapitole **Škálování** (Binance academy, 2021).

Fork

„Fork“, česky vidlička, označuje situaci, kdy dojde k zapojení dvou bloků za stejný předchozí blok. Situace není nic neobvyklého a „forky“ s délkou jednoho bloku se objevují často. Pokud vytěží téměř ve stejný čas dva rozdílní těžaři 2 rozdílné bloky, každý z nich zahájí rozesílání bloku ostatním uzlům ke kontrole a ty ho zařadí do své verze blockchainu, aniž by věděli o bloku vytěženém druhým těžařem. Který z bloků bude ale platnou větví blockchainu? Určení je velice jednoduché, platnou větví se stává vždy nejdelší větev blockchainu. Aby nastala situace, kdy dojde k vytěžení následujícího bloku na obou větvích blockchainu ve stejný čas, opakovaně je velice nepravděpodobné. Pokud jsou větve stále stejně dlouhé, platná je ta větev, na jejíž vytěžení bylo spotřebováno více práce. Kratší větev je poté neplatná a k bloku se přistupuje, jako by nebyl vytěžen (nese označení sirotek „*orphan block*“). Těžaři nenáleží odměna a transakce je potřeba znovu zahrnout do následujícího bloku. Při odesílání transakce je vždy znám potřebný počet potvrzení transakce, který značí potřebnou hloubku bloku v blockchainu. Tento kontrolní mechanismus zajišťuje, že nedojde k provedení dvojí útraty mincí. Schéma situace „forku“ a vzniku osířelých bloků je znázorněno na následujícím obrázku (Stroukal, a další, 2021).

Obrázek 5: Vznik forku a orphan bloků



Zdroj: (Zhang, 2017)

Fork může být také důsledkem změny Bitcoinového protokolu. Při úpravách Bitcoinového protokolu, které byly popsány v předchozí podkapitole: Bitcoin Improvement Proposal (BIP), se jedná o takzvaný „*softfork*“. Softfork je změna Bitcoinového protokolu, která je zpětně kompatibilní, protože stará verze protokolu považuje data za validní. Jednoduše řečeno softfork pravidla zpřísňuje, nebo dává prázdným rezervovaným hodnotám v protokolu nový význam. Situace, kdy je změna natolik velká a rozsáhlá, že protokol není zpětně kompatibilní, se říká „*hardfork*“. Stará verze Bitcoinového protokolu považuje nové bloky za nevalidní, a tudíž dále řadí vytvořené bloky za poslední blok před vznik hardforku. Část komunity a těžařů, kteří se rozhodnou uznávat nová pravidla, začnou vytvářet nové bloky do své odštěpené větve. Hardfork zjednodušeně pravidla uvolňuje a zvětšuje množinu validních bloků. Důsledkem hardforku může být trvalé rozdělení blockchainu („*split*“), kdy se komunita rozdělí na části a každá z nich podporuje svou větev blockchainu. Příkladem významného hardforku je Bitcoin Cash, který vznikl neshodami o zavedení větší velikosti bloku (Stroukal, a další, 2021).

3.4 Nákup kryptoměn

Nákup kryptoměn není dle Kaliského (2018) složitý, často je ale v dnešní době doprovázen tzv. „FOMO“ (fear of missing out) efektem. Tento strach nepropásnout životní příležitost a zbohatnout rychlou cestou bez hlubších znalostí pak zaviňuje nevhodně

načasované nákupy a také nahrává podvodníkům. Proto je dobré si nejdříve vše nastudovat a zvolit nejvhodnější cestu, pomocí které začít kryptoměny promyšleně nakupovat.

Se stoupající cenou se zájem o kryptoměny zvyšuje, a proto největší vlny obchodníků přicházejí právě v tu dobu, kdy je cena na vrcholku. Kryptoměny jsou známe obrovskou volatilitou a lidé, kteří nakoupí bez rozmyšlení a v ovlivnění FOMO efektu často nevydrží napětí při klesající ceně a jakmile přijdou větší cenové výkyvy směrem dolů, prodají s panikou kryptoměnu ve ztrátě (Mikulášek, 2021).

Před použitím jedné z možností nákupu, kterými jsou burza, směnárna, bitcoinový bankomat a nákup od lidí je vhodné prozkoumat transparentnost, reputaci, zákaznickou podporu, rychlost, poplatky a spread. Spread označuje rozdíl u směnárny a burz mezi cenou, za kterou dotyčný nakupuje a prodává (Kaliský, 2018).

U nákupu kryptoměn se definují 2 základní rozdělení nákupu na decentralizované („DEX“) a centralizované („CEX“) možnosti. Ty centralizované podléhají regulacím a musí dle zákonů plnit procesy „KYC/AML“ (Know Your Customer / Anti-Money Laundering), které jim ukládají za povinnost ověřovat identitu svých klientů. U decentralizovaných služeb neprochází uživatel procesem identifikace, protože není možnost, jak tento proces vymáhat. Na decentralizovaných burzách není z tohoto důvodu možné obchodovat kryptoměnové páry oproti běžným fiat měnám, jako jsou USD a EUR. Na takovýchto burzách se obchodují již pouze kryptoměny v páru se stablecoiny nebo jinými kryptoměnami (Wolf, 2021).

3.4.1 Kryptoměnové burzy a směnárny

Burzy patří k nejpoblárnějším možnostem nákupu kryptoměn. Na kryptoměnové burze se propojuje nabídka s poptávkou, burza tedy umožňuje nákup a prodej nejen bitcoinu, ale i jiných kryptoměn, dále také držení získaných kryptoměn na burzovním účtu. Je jich několik typů, některé umožňují zůstat v anonymitě a nevyžadují zadávání osobních údajů, jsou decentralizované (DEX). Ty nejznámější však decentralizované nejsou a vyžadují zmiňovaný proces identifikace klienta (KYC/AML). Mezi nejznámější burzy patří Coinbase, Kraken, Gemini, Binance, Huobi Global a FTX. Kryptoměnová směnárna má zpravidla vyšší poplatky a kurzovní spread než burzy, nenabízí propracované možnosti využívání ani doplňkové služby spojené s různými deriváty. Nákup na směnárně se provádí za kurz vypsany směnárnou. Nákup je sice dražší, ale pro začínající uživatele

jednodušší a intuitivnější. Pro začátečníky a nenáročné, kteří s kryptoměnami nechtějí obchodovat na denní bázi je dostatečným řešením (Investopedia, 2021).

3.4.2 Bitcoinové bankomaty

Bankomat na bitcoin nebo tzv. bitcoinmat slouží k rychlému nákupu a prodeji. v České republice můžeme nejčastěji vidět bitcoinmaty dodávané firmou General Bytes. Hotovost v korunách z něj lze získat téměř okamžitě, pokud si člověk přeje bitcoin prodat. Nejnižší částkou, za kterou lze bitcoin koupit v těchto automatech je 500 korun. Kurz vychází z aktuálních cen na burzách + poplatku bankomatu. Výstupem z bankomatu je buďto soukromý klíč vytištěný na papír (papírová peněženka), nebo pokud bude bitcoinmatem naskenován QR kód vlastního veřejného klíče, budou prostředky zaslány přímo tam (Fillner, 2018).

V posledních letech jsou bitcoinmaty stále více oblíbené. v České republice jsou nejrozšířenější ATM od výrobce General Bytes. Dle Coinmap (2021) jsou v ČR bitcoinmaty umístěny na 62 místech, nejvíce v Praze. Z údajů Coinatmradar (2021) vyplývá, že po celém světě je umístěno více než 22 615 těchto bankomatů, z toho více než 19 000 v USA. Na celé území Evropy poté připadá téměř 1 350 míst Na následujícím obrázku je zachycen jeden z nejnovějších bitcoinmatů čtvrté generace, od společnosti General Bytes, který je umístěn v pražské Paralelní Polis.

Obrázek 6: BATMFour



Zdroj: (General Bytes, 2021)

3.4.3 Přímý nákup od lidí

Jednou z možností přímého nákupu od lokálních obchodníků je celosvětová služba localbitcoins.com. Ta propojuje všechny zájemce a prodejce bitcoinů. Při zadání polohy nebo povolení lokalizaci v GPS, můžete vyhledat nejbližšího obchodníka, poté se domluvíte na ceně a způsobu platby. Je zde nutná opatrnost, na portálu lze nalézt i jednotlivé reference jednotlivých uživatelů. Výhodou této formy zisku bitcoinů je rychlost a minimum byrokracie, nevýhodou pak vyšší ceny (Fillner, 2018).

Další možností přímého obchodu je tzv. „*face-to-face*“. Ze začátku se může jevit obtížné najít důvěryhodnou protistranu ve svém okolí, po objevení Bitcoinové komunity a navázání kontaktů s ostatními nadšenci ze světa kryptoměn se ale tento způsob jeví jako nejjednodušší, nejsnadnější a nejvíce udržující anonymitu držitele kryptoměn. z pohledu ceny je obchod z očí do očí na stejné úrovni jako nákup z burzy. Obchody se zpravidla provádí za aktuální cenu na vybrané burze (Stroukal, a další, 2021).

3.5 Uchování bitcoinu

Bitcoin lze uchovávat několika způsoby, všechny však nejsou zcela bezpečné. V krypto světě se chyby neodpouští, není zde třetí strana, která by případné kroky mohla vrátit zpět. K uchování bitcoinu není třeba drahé zařízení, pro nejméně náročné postačí papír a tužka. Je známo hned několik typů peněženek, a těmi jsou hardwarové peněženky, softwarové peněženky, papírové peněženky a burzovní peněženky. V podkapitolách budou představeny podrobně (Kohout, 2021).

Nejzásadnějším rozdílem v uchování bitcoinu je ukládání v podobě HOT a COLD. Označení HOT znamená, že peněženka je připojena k internetu. Peněženky připojené k internetu mohou být zneužity útokem na dálku, patří tedy k nižší úrovni bezpečnosti. Jsou to například softwarové peněženky, které jsou nainstalované na počítači s přístupem k internetu, nebo burzy. Označení COLD nesou zařízení, která jsou offline, aktuálně nejsou nebo nemohou být vůbec připojeny na internet. Jsou to například papírové peněženky nebo hardwarové peněženky (Finex Media, 2021).

3.5.1 Hardwarové peněženky

Hardwarové peněženky jsou velmi bezpečné, patří vlastně mezi nejbezpečnější, díky tomu že nejsou přístupné online. Nejznámější „*hardware wallet*“ jsou od firmy Trezor

nebo Ledger. v případě odcizení, ztráty či poškození lze obnovit svůj předchozí účet a dostat se zpět k uloženému bitcoinu, a jiným kryptoměnám, díky „seedu“, což je fráze pro obnovení. „Seed“ má 12 nebo 24 náhodných slov, která generují privátní a veřejné klíče. Výhodou HW peněženky je vyšší bezpečí pro danou investici, vyplatí se hlavně při vyšším vkladu peněz. HW peněženka má v sobě uložený soukromý klíč, který je stále offline mimo počítač a internet. Potvrzování transakcí a přístup do HW peněženky se provádí pouze pomocí pinu. Aktivace HW peněženky je snadná a oba výrobci poskytují stručné návody. U Trezoru je to odkaz na trezor.io/start, a v případě Ledger je to ledger.com/start. Značnou nevýhodou je podpora jen určitých kryptoměn, pokud se člověk rozhodne experimentovat s méně známějšími kryptoměnami, v HW peněženkách u nich často nenajde podporu. Další nevýhodou může být vyšší cena která se pohybuje v řádů nižších tisíců korun. Za nejbezpečnější možnost uložení kryptoměn se ale tuto částku vyplatí bezesporu utratit (KryptoHodler.cz, 2021).

3.5.2 Softwarové peněženky

Softwarové peněženky jsou nejpoblárnější, a to díky snadnosti, rychlosti a pohodlnosti. Největší výhodou těchto peněženek je možnost mít je vždy při sobě, a to jak v chytrých mobilních zařízeních, tak i v tabletech, počítačích a chytrých hodinkách. Další výhodou je, že jsou téměř vždy zdarma. Nejvíce používané jsou Electrum nebo Exodus (CryptoSvet.cz, 2020).

Softwarové peněženky se dělí na desktopové krypto peněženky, mobilní krypto peněženky a on-line peněženky. Desktopové je potřeba nainstalovat a stáhnout do počítače. Uživatel má poté přístup jen z jednoho zařízení. Úroveň zabezpečení je vyšší díky ukládání privátních klíčů na hard-disk počítače. Vytvořením takovéto peněženky na počítači odpojeném od internetu (a dále nepřipojeném) je možné získat tzv. „cold“ SW peněženku. Nejčastějším typem je právě již zmiňovaný Exodus nebo Atomic Wallet či Jaxx. Mobilní krypto peněženky je potřeba nainstalovat do mobilního zařízení v podobě aplikace. Snadno se ovládají a jsou vhodné pro lidi kteří chtějí se svojí kryptoměnou běžně platit. Patří sem BRD, Coinomi, Mycelium a Trust Wallet (Finex Media, 2021).

3.5.3 Kryptoměnové burzy

Zanechání prostředků na účtu burzy je nejméně bezpečné. Již se několikrát v minulosti stalo, že burza byla vykradena a uživatelé přišli o své držené kryptoměny. U kryptoměn je prakticky vyloučeno, že by vám je někdo někdy vrátil (Krause, 2021).

Jako varovné případy lze uvést například burzu Bithumb, která byla v roce 2017 vykradena (patřila mezi 5 největších burz s kryptoměnami), burza působí v Jižní Koreji. Ztráta dosáhla téměř 1,2 miliardy wonů, což je v přepočtu 22,6 milionů korun (Insider Inc., 2021).

Nejznámější a doposud největší útok na burzu a krádež kryptoměny (v tomto případě bitcoinů) je z února roku 2014. Napadená burza Mt. Gox v té době obstarávala až 70 % všech bitcoinových transakcí. Z burzy bylo ukradeno přes 850 000 bitcoinů, které v té době tvořili okolo 6 % z celkové dostupné zásoby. Burze Mt. Gox se povedlo lokalizovat 200 tisíc bitcoinů, zbylých 650 tisíc se ale rozplynulo na Bitcoinový trh. V době krádeže se jednalo o BTC v hodnotě více než 450 milionů dolarů, v dnešních cenách by 600 tisíc BTC mělo hodnotu více než 20,7 miliard dolarů. s již neoperující burzou se dodnes vedou soudní spory (Investopedia, 2021).

Fráze „*Not you keys, not your coin*“, která je v Bitcoinové komunitě často skloňovaným ponaučením, znamená že pokud nekontrolujete klíče peněženky, nemáte kontrolu nad kryptoměnou. Kryptoměnových burz jsou stovky a dá se skrze ně jednoduše nakoupit nejrůznější kryptoměny, následné uchovávání kryptoměn zde je ale potřeba pečlivě zvážit (Cointelegraph, 2016).

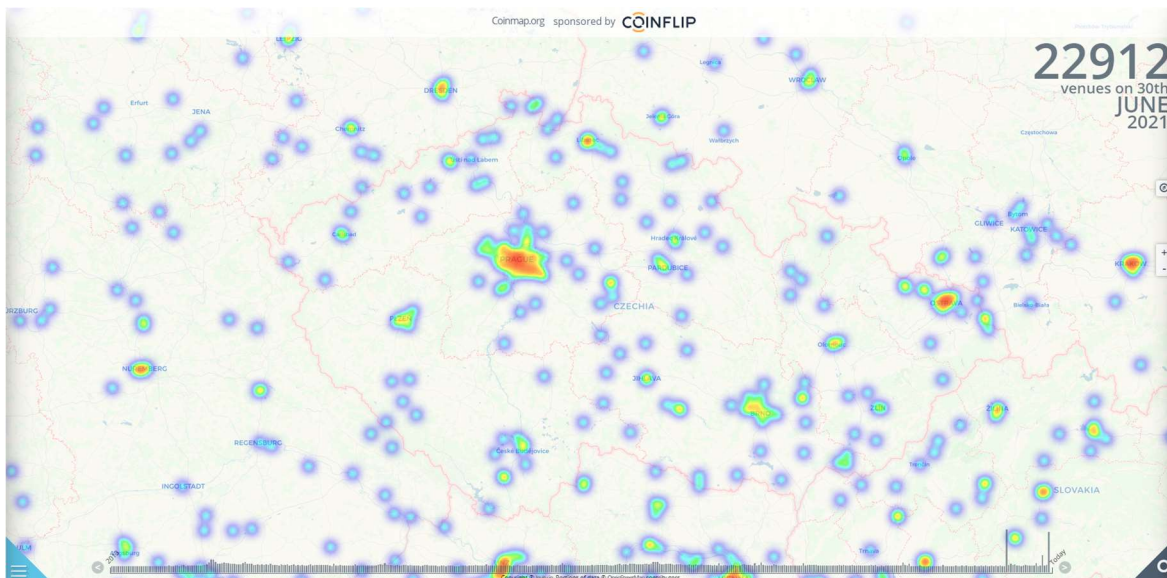
3.6 Používání Bitcoinu

Někteří vlastníci bitcoinu vyznávají strategii „HODL“ (termín vznikl zkomolením slova „hold“, tedy držet, když jeden z členů Bitcoinové komunity napsal na fóru Bitcointalk (2013) příspěvek o tom, že své bitcoiny při propadu ceny neprodá a bude je dále držet), která spočívá v nákupu bitcoinu a jeho následného držení bez obchodování nebo utrácení. Bitcoin byl ale vytvořen jako platební systém, a tudíž je na místě, aby byl k placení využívám (Stroukal, a další, 2021).

V současné době je možné využít bitcoin, i jiné kryptoměny, k nákupu nejrůznějšího zboží a služeb. Na stránce Coinmap (2021) je možné nalézt místa, kde je platba prostřednictvím bitcoinu akceptována. V současné době eviduje téměř 23 000 míst po

celém světě. Výčet je samozřejmě pouze orientační a ve skutečnosti existují mnohá další místa, která stránka coinmap.org neuvádí. Na následujícím obrázku je zobrazena síť míst přijímajících bitcoin na území ČR.

Obrázek 7: Místa přijímající bitcoin (ČR)



Zdroj: (Coinmap, 2021)

3.6.1 Transakce v Bitcoinové síti

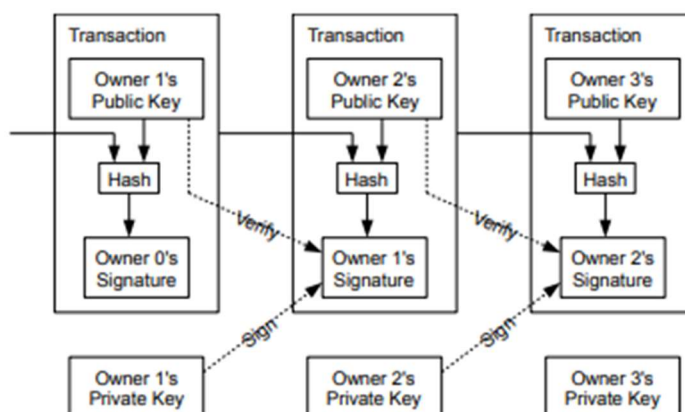
Jak již bylo řečeno v kapitole Bitcoin Improvement Proposal (BIP), veřejné klíče jsou odvozeny pomocí protokolu digitálního podpisu s využitím eliptických křivek z klíče soukromého. Ke každému soukromému klíči může být vygenerováno téměř neomezené množství veřejných klíčů, z kterých jsou vypočteny veřejné adresy. Pro provedení transakce je potřeba mít k dispozici právě oba z těchto klíčů (v případě vícepodpisových transakcí i větší počet soukromých klíčů). Příjemce bitcoinů musí odesílateli poskytnout svou vygenerovanou veřejnou adresu, na kterou odesílatel odešle libovolné množství bitcoinů a svým soukromým klíčem stvrdí vlastnictví odesílané kryptoměny a právo s ní disponovat. Odesílatel zná sice veřejnou adresu příjemce, může v blockchainu sledovat, jestli na ní prostředky zůstávají, nebo se přesouvají dále, nemůže s nimi ale disponovat. Právo využívat prostředky z této veřejné adresy má pouze příjemce, který musí jejich případný pohyb opět stvrdit svým soukromým klíčem (Stroukal, a další, 2021).

Je velký rozdíl mezi klíčem soukromým a klíčem veřejným. Pokud by byl prozrazen soukromý klíč peněženky, získá nový majitel tohoto klíče plný přístup k peněžence a prostředkům, které jsou na ní uloženy. Je tedy nesmírně důležité uchovávat tento klíč

v bezpečí a soukromí. Naopak veřejný klíč (veřejnou adresu) je úplně běžné sdělovat protistraně, bez její znalosti by nebylo možné bitcoiny obdržet a transakce by nemohla proběhnout. Je nutné mít na paměti, že z podstaty Bitcoinového protokolu a blockchainu, který funguje jako otevřená účetní kniha, jsou všechny transakce v celé historii dohledatelné. Jakmile získá kdokoliv určitou veřejnou adresu a dokáže si ji propojit s určitým majitelem, může pak sledovat pohyby prostředků daného majitele na získané adrese, a to jak minulé, tak budoucí. Veřejných adres je možné vygenerovat téměř neomezené množství, proto je vhodné pro každou přijímací transakci použít, pro zachování anonymity, nově generovanou adresu (Antonopoulos, 2014).

Transakce mohou být různých typů. Základní transakce využívá jeden vstup a vytváří jeden výstup (v případě odeslání celého zůstatku) nebo dva výstupy (v případě neodeslání celého zůstatku se v druhém výstupu přeposílá zbytek zůstatku na adresu původního majitele). Při tvorbě transakce je ale možné použít více vstupů (více veřejných adres) a vytvořit více výstupů (rozeslat na více veřejných adres), nebo zmíněné možnosti libovolně kombinovat. Roli hraje také to, zda jde o obyčejnou transakci, nebo se jedná o transakci vícepodpisovou. Čím je transakce komplikovanější a složenější z více různých vstupů a výstupů, tím je její velikost větší a odesílatel musí uhradit vyšší poplatek za uskutečnění. Následující obrázek graficky znázorňuje cyklus prostředků zaslaných v transakci tak, jak bylo výše popsáno (Nakamoto, 2008).

Obrázek 8: Transakce v Bitcoinové síti



Zdroj: (Nakamoto, 2008)

Pro potřeby práce byla na adrese bitaddress.org, kde si může každý vyzkoušet vygenerovat a vytvořit bitcoinovou peněženku, vytvořena následující sada klíčů, která je znázorněna na následujícím obrázku. Pokud by měl člověk zájem sadu klíčů opravdu

využít, bylo by nemyslitelné zveřejnit i soukromý klíč, který je uveden v pravé části obrázku. Soukromý klíč nově vytvořené peněženky, pro potřeby práce, je ve tvaru: KxMDSUbaRKXNyDWUoABBr1Mv1HZAr5wW9e7VoV1sM8aEEQkU9B3W. Veřejná adresa odvozená z veřejného klíče, který by potřeboval odesílatel prostředků, je ve tvaru: 19C5wjeoY3Jbc6gmZYvBkmPvC4DdXKUaLD. Obě části mají pro zjednodušení použití i svůj QR kód.

Obrázek 9: Papírová peněženka



Zdroj: (Bitaddress, 2021)

3.6.2 Blockchain explorer

Pomocí „*blockchain exploreru*“, tedy nástroje na prohledávání blockchainu, je možné na základě čísla bloku, hashe nebo adresy hledat jednotlivé transakce a sledovat pohyb prostředků na adresách. Pokud je znám majitel zkoumané adresy, je možné sledovat pohyb jeho prostředků. Služba je dostupná na stránce blockchain.com (Blockchain, 2021).

Pokročilejší možností analyzovat blockchain je například walletpolice.com, který vytvořil Aleš Janda v roce 2013 jako první službu svého druhu. Tento Bitcoinový explorer umožňuje seskupování adres a peněženek na základě vazeb mezi nimi. Dokáže tak například odhalit kam putují kradené bitcoiny (Janda, 2021).

Velmi pokročilou úroveň analýzy blockchainu nabízí společnost Chainalysis. Její placené služby využívají jak státní a finanční instituce tak největší směnárny ve více než 60 zemích světa. Chainalysis provádí úspěšné trasování bitcoinů (a jiných kryptoměn) a hraje

velkou roli při odkrývání zločinů spojených s kryptoměny. Již zmiňovaný Aleš Janda zde pracuje jako analytik blockchainu a občasně poskytuje v Bitcoinové komunitě informace o službách Chainalysis (Chainalysis, 2021).

3.7 Silné a slabé stránky Bitcoinu

Mezi nejsilnější stránky Bitcoinu patří, dle Frue (2018), jeho schopnost provádět bezpečně transakce mezi příjemcem a odesílatelem bez zahrnutí třetí kontrolní strany, jako je například banka. Bitcoin je tedy decentralizovaný a odolný vůči cenzuře, která není řízena jedním subjektem. Při správném využívání je do jisté míry anonymní.

Dále má ze všech kryptoměn nejdelší historii a největší uživatelskou základnu, je tedy ze všech kryptoměn nejjistější. Je to největší první digitálně omezené aktivum na světě, které poukazuje na možnost nespolehat pouze na banky a vlády. Zvyšující se zájem velkých společností ukazuje prostor pro růst (Thoma, a další, 2021).

Mezi slabé stránky patří pomalé transakce a omezená propustnost sítě. V další řadě nepředvídatelnost ceny a její velká volatilita. Tak, jako může ze dne na den hodnota stoupat, může se také prudce propadnout. Cena bitcoinu byla historicky velmi kolísavá. Pomalé transakce, s někdy vysokými poplatky, zabraňují použití v každodenním životě. Velice kritizována je i vysoká spotřeba energie při těžbě a možné vlivy na životní prostředí. Stále vyvíjející se regulační prostředí může ovlivnit negativně budoucnost Bitcoinu (Thoma, a další, 2021).

Za další slabou stránku je z některých úhlů pohledu možné považovat veřejnost platební historie zapsané v blockchainu. Potom také rizika spojená se zabezpečením burz a online peněženek, kdy již v minulosti byly napadeny hackery. Jelikož Bitcoin není kontrolován žádnou třetí autoritou, nese si za případné ztráty každý svou zodpovědnost a transakce jsou plně nevratné (Rajput, 2020).

Některé z vlastností Bitcoinu nelze jednoduše zařadit jako silnou nebo slabou stránku, protože záleží na tom, z jakého pohledu a kdo na danou vlastnost nahlíží. Bezesporu jde ale o velmi zajímavou a přínosnou technologii, která si své uplatnění v průběhu let úspěšně nachází.

Anonymita Bitcoinu

Bitcoin je ve skutečnosti pseudonymní, jelikož každý uživatel má veřejnou adresu, kterou lze vysledovat prostřednictvím analýzy Bitcoinové sítě. Transakce spolu s veřejnými adresami jsou zařazeny v jednotlivých blokách blockchainu, neodkazují však na osobní identitu. Pokud je adresa použita pro převod bitcoinu koupeného na burze, nebo prostřednictvím jiné služby, která vyžaduje podstoupení procesu KYC, může být takováto adresa poté spojena s pravou identitou držitele. V blockchainu jsou zaznamenány trvale a neměně veškeré bitcoinové transakce, které kdy proběhly. Jestli bude možné adresu spojit s identitou vlastníka adresy záleží jen na jeho přístupu k vlastnímu soukromí a způsobu nákupu / utrácení bitcoinů. Pokud je tedy adresa spojena se skutečnou identitou, není bitcoin vůbec anonymní. Pomocí blockchainové analýzy je naopak možné propojit veškeré provedené transakce s majitelem adresy (Bitcoin magazine, 2020).

Škálování

Soukup (2021) popisuje, že transakce jsou zpracovávány, ověřovány a zapisovány do blockchainu pomocí „těžby“ bloků, kde je jejich velikost omezena na 1 MB, velikost transakce činí minimálně 250 bytů a těžba zabere v průměru 10 minut. Bitcoin tedy zpracuje nanejvíc 7 transakcí za sekundu (navíc aby byla transakce opravdu ověřena, je potřeba vytěžit 4–6 bloků). z toho vychází problém škálovatelnosti Bitcoinu. Úspěšné ověření transakce trvá 40–60 minut. Tento problém se dá vyřešit zvětšením bloku, to ale musí schválit většina těžařů. Zmiňovaný pokus už neúspěšně proběhl a dal v roce 2017 vzniknout kryptoměně Bitcoin Cash prostřednictvím hardforku blockchainu.

Dalším možným řešením by bylo využití „*shardingu*“, tedy rozdělení uzlů na několik částí, které by odděleně prováděly těžbu. Prosazení těchto řešení je časově náročné, a navíc by snižovalo bezpečnost sítě. Jak již bylo zmíněno, bezpečnost blockchainu je zaručena velkým množstvím uzlů, které vykonávají stejnou práci. Milníkem v řešení škálování byl „*SegWit*“ v roce 2017, ten položil základy pro „*Lightning Network*“ (Kaliský, 2018).

Lightning Network je jakási transakční síť, která se řadí nad blockchain. Představuje druhou vrstvu blockchainu. Umožňuje vlastně neomezený počet transakcí s nízkým poplatkem. Je také poměrně anonymní, díky zapsání až konečné transakce, nikoliv dílčích převodů. Nejznámější lightningová peněženka je Blue Wallet. Síť tedy ve zkratce umožňuje zavádění Bitcoinu do běžného spotřebního života (Hamilton, 2020).

3.8 Česká prvenství týkající se Bitcoinu

Ačkoliv patří Česká republika svou rozlohou mezi malé země, ve světě kryptoměn má velmi dobré postavení a někteří z českých představitelů jsou známí po celém světě. Praha je sídlem společnosti SatoshiLabs, která vyvinula první hardwarovou peněženku na světě, Trezor. Zároveň jeden z jejich zakladatelů, Marek „Slush“ Palatinus, přišel s nápadem těžby v poolech a založil úplně první těžební pool na světě, Slush Pool. Dále se dá v Praze navštívit Paralelní Polis, v které sídlí kavárna Bitcoin Coffee. Jde o jedinou kavárnu na světě, kde si je možné zakoupit kávu pouze za kryptoměny. V Paralelní Polis se také konají různé semináře, přednášky a světové konference týkající se světa kryptoměn. Společnost SatoshiLabs také vytvořila stránku coinmap.org, která eviduje po celém světě místa přijímající bitcoin. Dále u nás sídlí společnost General Bytes, která vyrábí bitcoinové bankomaty a řadí se mezi největší na světě (Stroukal, 2018).

Slush Pool přispívá k zabezpečení největší decentralizované platební sítě. Odstartoval svoji dráhu koncem roku 2010, kdy byl založen Čechem, Markem Palatinem, známým na internetu pod přezdívkou Slush. Je to první světový těžářský pool bitcoinů s dosud vytěženými více než 1 200 000 BTC (CryptoSvet, 2020).

Trezor založili dva programátoři a krypto nadšenci Pavol „Stick“ Rusnák a Marek „Slush“ Palatinus. Začalo to jako hobby vytvoření hardwarových peněženek pro přátele, později si pak uvědomili díru na trhu. V roce 2013 založili tvůrci Trezoru SatoshiLabs, společnost, která vyvíjí a prodává Trezor. Existují dva modely, a to Trezor One a Trezor Model T, který je novější a rychlejší (SatoshiLabs, 2018).

Wallet explorer vytvořený Alešem Jandou je prvním blockchainovým explorem, který umožňuje automatické párování adres a peněženek na základě jejich vzájemných vazeb. Aleš Janda sehrál se svým wallet explorem důležitou roli při dopadení tvůrce nelegálního tržiště Sheep Marketplace, které se nacházelo na běžně nepřístupné části internetu, tzv. darknetu (Janda, 2021).

3.9 Regulace kryptoměn

Z právního hlediska je v České republice každý token či coin věcí nehmotnou a movitou. Token je také věc zastupitelná, může být tedy nahrazen jinou věcí téhož druhu. Kryptoměny zatím nemají ucelenou regulaci. Česká národní banka neuznává kryptoměny jako virtuální peníze, cizí měnu ani jako obdobu cenného papíru. Z tohoto důvodu spadají

příjmy z prodeje kryptoměn do §10 Zákona o daních z příjmu – Ostatní příjmy (Generální finanční ředitelství, 2018).

Je pochopitelné, že někomu se může zdát zdanění decentralizované kryptoměny nemístné, podle české legislativy je však nutné zisk zdanit. Je potřeba mít na paměti, že u kryptoměn neexistuje nic takového, jako časový test u akcií. Nezáleží na tom, jak dlouho je kryptoměna držena, daň ze zisku je nutné zaplatit vždy. Velká část držitelů kryptoměn si myslí, že správný postup danění kryptoměn je danit až konečný převod kryptoměny zpět na fiat měnu. Tento přístup je také chybný. Správný postup je danit každou směnu kryptoměny na fiat měnu, směnu kryptoměny za jinou kryptoměnu nebo pořízení zboží či služeb za kryptoměny. Osvobozeno je pouze darování mezi příbuznými v přímé linii, některých v pobočné linii a manžela. Při daru převyšujícím 5 mil. Kč je nutné dar nahlásit. Obdarovaný pak při prodeji daní rozdíl mezi cenou v okamžiku nabytí a cenou prodejní (Hanych, a další, 2018).

Platba v kryptoměnách podléhala povinnosti EET. O kryptoměnách se také zmiňuje daňový balíček z roku 2017. Těžba kryptoměn je brána jako služba poskytovaná, tedy podnikání. Pro těžbu kryptoměn je nutné mít tedy zřízenou živnost. Příjem z tohoto podnikání se zdaňuje dle §7 Zákona o dani z příjmu. Když dosáhne FO při těžbě kryptoměn zisku, zdaní se 15 % (Finex, 2021).

Tak jako v ČR, i ve světě podléhají zisky spojené s kryptoměnami zdanění. V USA platí stejné podmínky jako u obvyklého daňového zařazení podle Vašeho příjmu, jsou rozlišovány krátkodobé a dlouhodobé kapitálové výnosy. V Evropě není jednotný proces, každá se zemí jedná podle vlastních zákonů. Například v Německu nejsou daněny dlouhodobé kapitálové příjmy již po jednom roce, daní se pouze meziroční zisky. V Bělorusku a Portugalsku za kryptoměny nezdaňují téměř vůbec, tyto země se snaží přilákat nové investory (SatoshiLabs, 2021).

3.10 Ekonomika Bitcoinu

Myšlenka Bitcoinu je nápadně podobná názorům rakouské ekonomické školy, je tedy pravděpodobné že vychází z jejich teorií. Bitcoin totiž nepotřebuje pro provádění transakcí třetí dohlížející stranu, ale snaží se o vložení finanční svobody do rukou jeho uživatelů. Do svého fungování ale zařadil nové prvky jako je síť typu klient-klient, asymetrická kryptografie a digitální měna. Otázkou však je, zda se může ve spojení s Bitcoinem mluvit

o penězích. Minimálně v současné době není bitcoin všeobecně přijímaným, není známo ani území, kde by byl všeobecně přijímaným (první náznaky se ale objevují, dle serveru BBC (2021), stát El Salvador uzákonil 9. 6. 2021 bitcoin jako zákonné platidlo a v následujících 90 dnech provedl jeho zavedení). Dokonce ani v žádné komunitě, pokud ji nedefinujeme jako Bitcoinová komunita, není všeobecně přijímaným. Dalším faktem je, že jen málokdo provádí ekonomickou kalkulaci ceny v bitcoinu, drtivá většina uživatelé stále přepočítává cenu na svou domácí fiat měnu. Aby se stal bitcoin všeobecně přijímaným prostředkem směny, musel by nejdříve překonat i tuto překážku (Stroukal, a další, 2021).

Inflace a deflace

Bitcoinů je předem stanovené omezené množství, a jednou z hlavních výtek proti tomuto systému je jeho deflační prostředí. Na takové prostředí nejsou lidé ze systému tradičních měn zvyklí. Cílené znehodnocování měny zde není možné, tudíž není ani možné vytvářet inflaci. Zásoba bitcoinů bude navždy neměnná, dokonce je klesající, z důvodu ztrát přístupových údajů k adresám uchovávajícím bitcoiny. Pokud tedy nebude poptávka po bitcoinech klesat, měla by jejich cena zákonitě růst. Pokud roste hodnota peněz, musí klesat ceny všeho ostatního. Snižování cen je navíc běžným jevem tržního prostředí, kdy na cenu působí nové produkty a technologické inovace. Z těchto důvodů se mluví o možném vzniku deflační spirály. Argument je opodstatněný v tradičním peněžním světě, kde by umělé znehodnocování peněz vedlo s velkou pravděpodobností k ekonomickým problémům (Stroukal, a další, 2021).

V měnové politice mohou centrální banky za účelem cílení inflace snižovat úrokové sazby, čím motivují k vyššímu půjčování a zvýšení peněžní zásoby komerčních bank, až ke dnu likvidity. Existuje ale strach, že lidé se budou obávat, že půjčky bude v budoucnu dražší splatit, což je bude motivovat k dřívějšímu splacení stávajících půjček a nebrání si půjček nových. Toto chování snižuje peněžní zásobu, znehodnocuje peníze a vytváří tedy deflaci (Samuelson, a další, 2013).

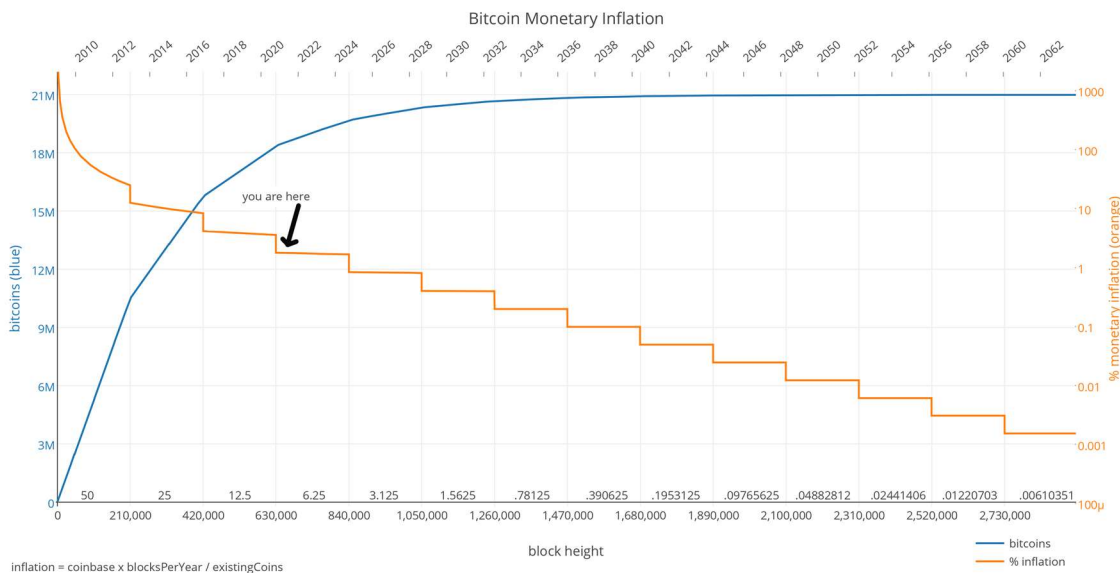
Obava deflační spirály je pro Bitcoin neopodstatněná, protože se nejedná o konstrukt obíhající dluhů, ale o spontánně vytvořenou „komoditu“. Hromadění bitcoinů v důsledku snižování cen nemůže vést k nekonečné spirále, protože pokud je lidé nepoužijí ve směně, poroste relativně hodnota jiného prostředku směny, což by mělo za následek snižování

hodnoty bitcoinů. Systém se tímto mechanismem sám reguluje. Na teoretické úrovni by mohla invence v podobě Bitcoinu odstranit hospodářské cykly, protože bitcoinů je omezené a předem známe množství, které nelze rozšířit. Lidé stále mohou podlehnout efektu stáda nebo udělat hromadné chyby. Hlavní spouštěč období expanze, tedy umělá změna peněžní zásoby, je ale ve světě Bitcoinu odstraněna. Tuto teoretickou myšlenku by bylo však obtížné ověřit (Stroukal, a další, 2021).

Pod pojmem inflace/deflace je dle Samuelsona (2013) myšlen růst/pokles cenové hladiny, který je měřen pomocí cenových indexů. Zatímco cenová inflace peníze znehodnocuje, cenová deflace je zhodnocuje. Přiměřená hladina inflace vyvažuje technologický pokrok a ceny zůstávají technicky na totožné úrovni.

Bitcoin má svou měnovou inflaci, která se každé 4 roky, s půlením odměny za vytěžený blok, snižuje na polovinu. Na následujícím obrázku je zachycen průběh změn v měnové inflaci Bitcoinu a současné časové zařazení. Všechny bitcoiny budou vytěženy v roce 2140, poté dosáhne měnová inflace nulové hodnoty. Prakticky jí dosáhne mnohem dříve, protože v důsledku ztráty přístupu k bitcoinům jejich množství bude klesat rychleji než tvorba nových mincí. Pokud se uvažuje, že je ztraceno 0,5 % všech bitcoinů, bude Bitcoin měnově deflační již v roce 2036, při ztrátě 0,05 % v roce 2048.

Graf 1: Monetární inflace Bitcoinu



Zdroj: (Vlastní zpracování na základě podkladu z Cointelagraph, 2016)

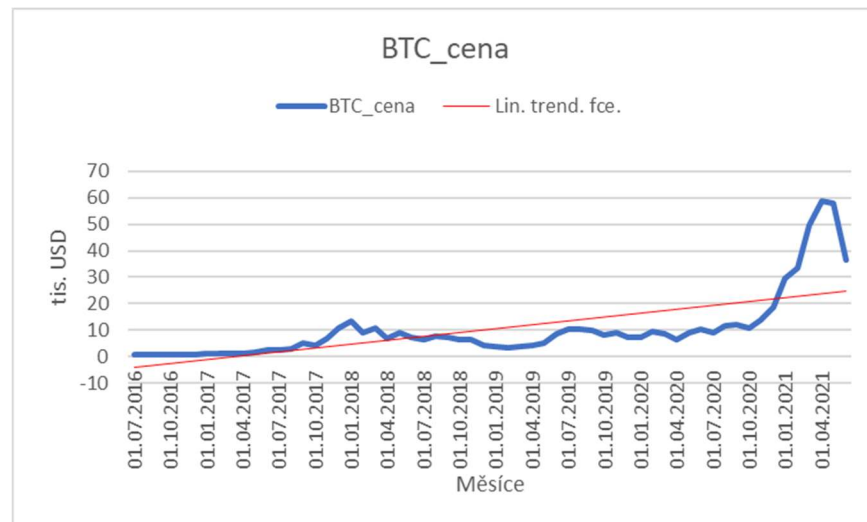
4 Vlastní práce

4.1 Analýza časových řad potenciálních determinant působících na cenu bitcoinu

V následující kapitole bude provedena graficky analýza vybraných časových řad, které budou použity k vytvoření ekonometrickém modelu. Jedná se o vývoj ceny bitcoinu, vývoj ceny akciového indexu S&P500, vývoj ceny kovů a vývoj peněžního agregátu M2 v USA. Časové řady jsou v měsíčních datech od července 2016 do června 2021 vždy k prvnímu dni daného měsíce. Jedná se tedy o sledované období 5 let s měsíční frekvencí.

4.1.1 Vývoj ceny kryptoměny bitcoin

Graf 2: Vývoj ceny kryptoměny bitcoin



Zdroj: (Vlastní zpracování na základě podkladů z CoinMetrics, 2021)

Z výše uvedeného grafu, zaznamenávajícího vývoj ceny bitcoinu v tisících USD v čase, proloženého lineární trendovou funkcí, je zřejmé, že od počátku sledování (července 2016) má cena bitcoinu rostoucí tendenci. Ze své hodnoty 678 USD/kus, v počátku sledování, vzrostl až do svého lokálního maxima, kdy dosáhl při měření 1. ledna 2018 na cenu 13 465 USD/kus (skutečné maximum nastalo 18. prosince 2017 s hodnotu 19 498 USD/kus). Po výrazné změně cena klesala až do února 2019, kdy byla cena bitcoinu pouhých 3 445 USD/kus. Po tomto rok trvajícím medvědímu trhu se trend obrátil a cena pozvolným tempem rostla až do října 2020, kdy započal další silný růst. V prosinci 2020 se bitcoin obchodoval těsně pod hranicí 29 tis. USD/kus, což znamená za daný rok nárůst o celých 416 %. Další růst v počátku roku 2021, který dosáhl k 1. 4. hodnoty celých

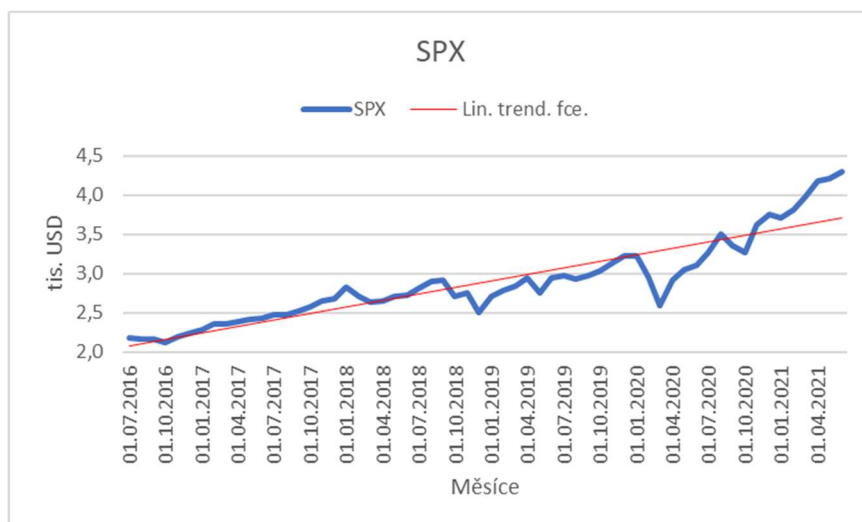
58 819 USD/kus položil nové absolutní maximum (skutečné maximum nastalo 12. 4. v 64 895 USD/kus) pro sledované období.

Jako pravděpodobné se jeví, že k silnému nárůstu bitcoinu v roce 2020 a 2021 dopomohl svou měrou vznik nemoci COVID-19 a s ním spojená panika, kdy v mnoha ekonomikách docházelo k poskytování stimulačních balíčků pro občany, nárůstu inflace a poklesu kupní síly. V květnu roku 2020 také došlo k halvingu, kdy po 4 letech klesla odměna za těžbu bloku z 12,5 na 6,25 bitcoinu/blok. V očích některých lidí se bitcoin jeví jako uchovatel hodnoty, a proto společně s novými penězi plynoucími do ekonomiky a čerstvým poklesem měnové inflace bitcoinu se do bitcoinu přilévají nové finanční prostředky. Z grafu je možné pozorovat velmi ostré změny v ceně v obou směrech, tímto se kryptoměny liší od klasických finančních trhů. Bitcoin od svého vzniku v roce 2009 narostl z nulové hodnoty až na dnešní cenovou úroveň. Lze očekávat, že cena bude se svými korekcemi nadále růst.

4.1.2 Vývoj ceny akciového indexu S&P500

Na následujícím grafu je uveden vývoj ceny akciového indexu S&P500 ve sledovaném období. Tento index obsahuje 500 nejvýznamnějších světových společností, které se obchodují na amerických burzách NYSE a NASDAQ. V indexu se silně odráží výkonnost americké ekonomiky.

Graf 3: Vývoj ceny akciového indexu S&P500



Zdroj: (Vlastní zpracování na základě podkladů z Investing, 2021)

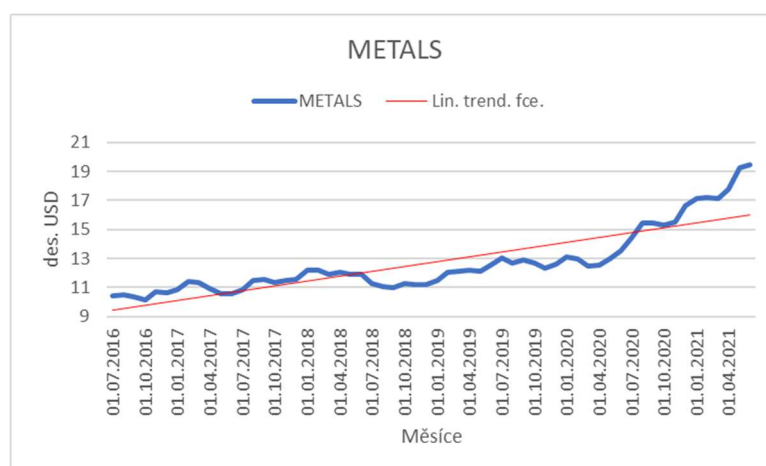
Z grafu vývoje ceny akciového indexu SPX, udávaného v tis. USD, je možné vysledovat rostoucí trend vývoje ceny. Od hodnoty 2 174 USD/kus v začátku sledovaného

období vzrostla cena indexu k 1. 6. 2021 až na 4 298 USD/kus, což značí průměrné tempo růstu (měsíční) o 1,162 % (odpovídá 14,87 % ročně). Oproti historickým údajům, které udávají od roku 1957, kdy bylo do indexu zařazeno právě 500 akcií, průměrný meziroční nárůst o 10,67 % (Maverick, 2022), toto sledované období svým růstem předčilo očekávání. Silný výkyv nastal s příchodem první vlny pandemie COVID-19, svého dna dosáhl index 23. 3. 2020 v hodnotě 2 237USD/kus. Situace na trzích ale umožnila rychlý návrat a dokonce překonání hodnot v začátcích roku 2021. Jak z průběhu lineární rostoucí trendové funkce, tak z historických údajů vývoje indexu, lze předpokládat jeho další růst v následujících letech.

4.1.3 Vývoj ceny kovů

Další zkoumaný graf ukazuje vývoj indexu zachycujícího cenu kovů IMF All Metals (a to jak základních, tak drahých²) ve sledovaném období. Grafem je rovněž proložena lineární trendová funkce, která naznačuje vývoj ceny v uvedeném období.

Graf 4: Vývoj ceny kovů



Zdroj: (Vlastní zpracování na základě podkladů z IMF, 2021)

Z průběhu grafu lze pozorovat velmi podobný trend růstu jako u akciového indexu SPX. Ve sledovaném období se hodnota indexu téměř zdvojnásobila. z hodnoty 104,15 USD/kus, na začátku období, dosáhla až na 194,96 USD/kus na začátku června 2021. Průměrné tempo růstu (měsíční) odpovídá 1,068 % (tedy 13,60 % ročně). Opět je zřejmé,

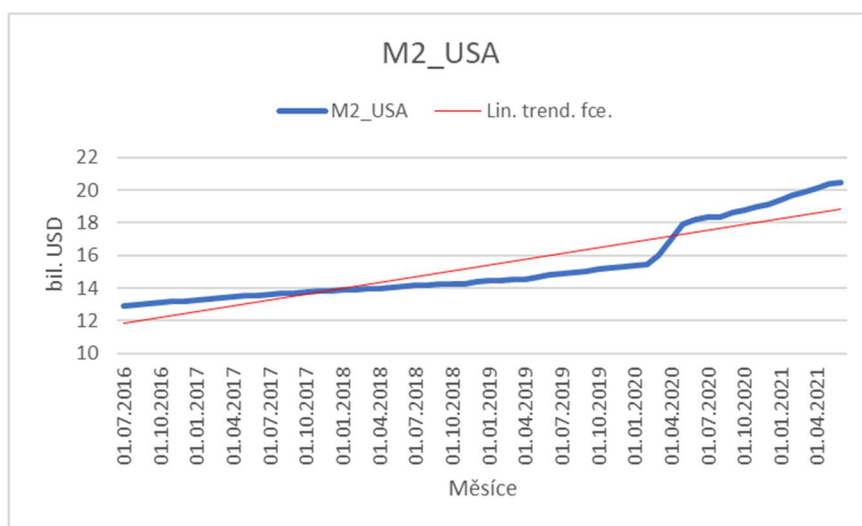
² Hliník, kobalt, měď, železná ruda, olovo, molybden, nikl, cín, uran, zinek, zlato, stříbro a platina

že index zažil po vzniku covidové pandemie prudký nárůst hodnot a výkyv, ve formě silného růstu, od svého trendu.

Vývoj peněžního agregátu M2 v USA

Následující graf zachycuje sezónně očištěný vývoj peněžního agregátu M2 v USA, agregát M2 před květnem 2020 obsahuje M1³ plus spořicí vklady, termínované vklady s nízkou nominální hodnotou (pod 100 000 USD) bez IRA a Keogh (typy důchodových plánů), zůstatky retailových fondů bez zůstatků IRA a Keogh. Od května 2020 již neobsahuje spořicí vklady a hodnota je dopočítána ze sezónně očištěných dat z dřívějších období.

Graf 5: Vývoj peněžního agregátu M2 v USA



Zdroj: (Vlastní zpracování na základě podkladů z FRED, 2021)

Na datech zachycených ve zmiňovaném grafu je zřejmý nárůst zásoby agregátu M2 v USA. Až do vzniku pandemie COVID-19 dochází v pozvolném nárůstu s neměnným mírně rostoucím trendem. Od počátku sledování, kdy velikost agregátu činila 12,889 bil. USD, zaznamenal za 45 měsíců do začátku pandemie v březnu roku 2020 nárůst o 3,122 bil. USD na hladinu 16,011 bil. USD. Oproti tomu po změně monetární politiky, kvantitativnímu uvolňování a stimulačních balíčcích pro občany, které měly podpořit

³ Oběživo, netermínované vklady, vklady úspor v bankách

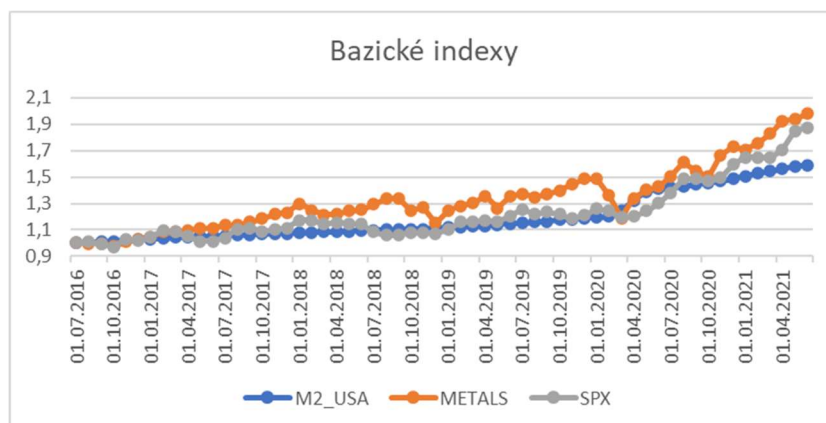
ekonomiku, došlo od začátku pandemie do konce sledovaného období k nárůstu o dalších 4,419 bil. USD za pouhých 15 měsíců. Celková zásoba agregátu M2 tedy k 1. 6. 2021 činí 20,430 bil. USD. Tento silný nárůst peněžní zásoby ovlivnil i průběh lineární trendové funkce popisující graf. Do budoucna je pravděpodobné, že tempo růstu se musí opět zmírnit na předchozí hladinu, protože takové množství nových peněz silně zvyšuje hladinu inflace. Reakce FEDu na situaci covidové pandemie je pozorovatelná i na předchozích zkoumaných časových řadách, kde právě po tomto zásahu trhy zaznamenaly příliv prostředků a silný nárůst.

4.1.4 Porovnání vývoje sledovaných časových řad

V této podkapitole bude cílem porovnat výše analyzované časové řady sledovaných veličin, kterými jsou vývoj ceny bitcoinu, vývoj ceny akciového indexu S&P500, vývoj ceny kovů a vývoj peněžního agregátu M2 v USA. Pro umožnění komparace budou využity hodnoty vypočtených bazických indexů. Jako báze je stanoveno první pozorování, tedy hodnoty naměřené prvního července 2016.

Po vypočtení bazických indexů pro všechny proměnné (Tabulka 4) bylo zjištěno, že cena bitcoinu narostla takovou měrou, že není možné vývoj graficky srovnat s ostatními zkoumanými proměnnými v totožném grafu. V následujícím grafu je tedy zachyceno pouze porovnání vývoje ceny SPX, kovů a peněžního agregátu M2 v USA.

Graf 6: Porovnání bazických indexů ceny SPX, kovů, M2 v USA



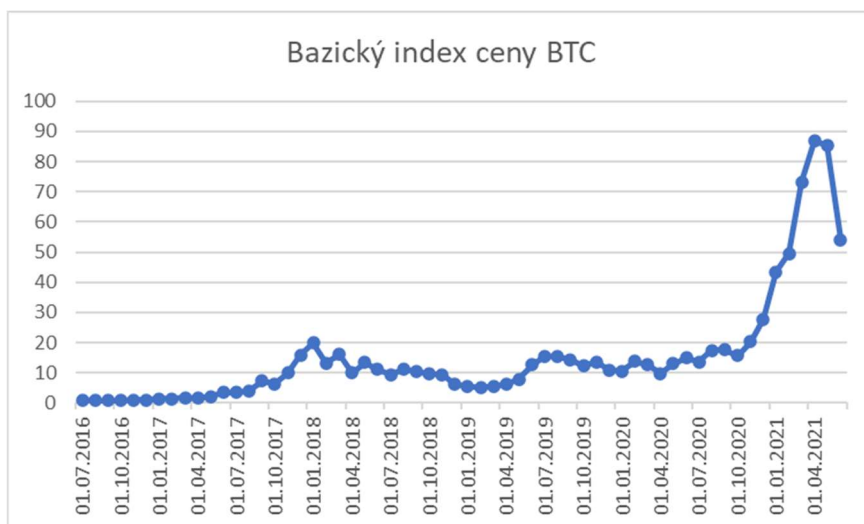
Zdroj: (Vlastní zpracování na základě podkladů z Investing, 2021, IMF, 2021, FRED, 2021)

Na základě předchozího výstupu (Graf 6) je možno říct, že od července roku 2016 dochází u všech sledovaných veličin k stabilnímu růstu. U ceny kovů lze pozorovat vyšší volatilitu než u ostatních determinant. Po zásazích do měnové politiky USA v březnu 2020

je zřetelně na sledovaných veličinách vidět, že zaznamenaly přísun nového kapitálu a jejich ceny rostly.

Pokud se zaměříme samostatně na graf znázorňující vývoj bazického indexu ceny bitcoinu, je v něm zjevné, že cenové výkyvy přicházejí ve stejných obdobích jako u výše zmiňovaných veličin.

Tabulka 3: Bazický index ceny kryptoměny bitcoin



Zdroj: (Vlastní zpracování na základě podkladů z CoinMetrics, 2021)

Výchytky od trendu jsou však mnohem silnější a cenový růst je mnohem více agresivní. Bazický index po vynásobení stem říká, na kolik % hodnota časové řady se dostala hodnota časové řady v čase t . V případě ceny kryptoměny bitcoin se v posledním období dostala hodnota na úroveň 5 411 %. Na svém úplném maximu v dubnu roku 2021 dokonce hodnot 8 682 %. Při porovnání s cenou SPX, kde hodnota v posledním období dosáhla 159 %, nebo ceny kovů, kde hodnota činí 198 %. Je zřejmé, že SPX a kovy jsou mnohem blíže semknuté s pozvolným růstem agregátu M2 v USA, kde hodnota v posledním období dosáhla 187 %.

Tabulka 4: Bazické indexy sledovaných proměnných

Období	BTC cena	SPX	METALS	M2 USA
	Bazický index	Bazický index	Bazický index	Bazický index
01.07.2016	1	1	1	1
01.08.2016	0,90	1,01	1,00	1,01
01.09.2016	0,84	1,01	1,00	0,99
01.10.2016	0,91	1,02	0,98	0,97
01.11.2016	1,08	1,02	1,01	1,03
01.12.2016	1,11	1,03	1,03	1,02
01.01.2017	1,47	1,03	1,05	1,04
01.02.2017	1,46	1,04	1,09	1,10
01.03.2017	1,81	1,04	1,09	1,09
01.04.2017	1,61	1,05	1,10	1,05
01.05.2017	2,12	1,05	1,11	1,02
01.06.2017	3,54	1,05	1,11	1,01
01.07.2017	3,56	1,06	1,14	1,04
01.08.2017	4,03	1,06	1,14	1,10
01.09.2017	7,26	1,06	1,16	1,11
01.10.2017	6,47	1,07	1,18	1,09
01.11.2017	9,93	1,07	1,22	1,10
01.12.2017	15,95	1,07	1,23	1,11
01.01.2018	19,87	1,08	1,30	1,17
01.02.2018	13,34	1,08	1,25	1,17
01.03.2018	16,12	1,08	1,21	1,15
01.04.2018	10,04	1,09	1,22	1,16
01.05.2018	13,39	1,09	1,24	1,15
01.06.2018	11,10	1,10	1,25	1,14
01.07.2018	9,39	1,10	1,30	1,09
01.08.2018	11,21	1,10	1,33	1,06
01.09.2018	10,62	1,10	1,34	1,06
01.10.2018	9,69	1,10	1,25	1,08
01.11.2018	9,36	1,11	1,27	1,08
01.12.2018	6,12	1,12	1,15	1,07
01.01.2019	5,62	1,12	1,24	1,10
01.02.2019	5,08	1,12	1,28	1,16
01.03.2019	5,62	1,13	1,30	1,16
01.04.2019	6,11	1,13	1,36	1,17
01.05.2019	7,85	1,14	1,27	1,16
01.06.2019	12,63	1,15	1,35	1,20
01.07.2019	15,60	1,15	1,37	1,26
01.08.2019	15,35	1,16	1,35	1,22
01.09.2019	14,41	1,17	1,37	1,24
01.10.2019	12,27	1,18	1,40	1,22
01.11.2019	13,65	1,18	1,45	1,19
01.12.2019	10,95	1,19	1,49	1,21
01.01.2020	10,58	1,20	1,48	1,26
01.02.2020	13,85	1,20	1,36	1,24
01.03.2020	12,61	1,24	1,19	1,20
01.04.2020	9,81	1,32	1,34	1,20
01.05.2020	13,07	1,39	1,40	1,24
01.06.2020	15,05	1,41	1,43	1,30
01.07.2020	13,64	1,42	1,50	1,38
01.08.2020	17,41	1,43	1,61	1,49
01.09.2020	17,67	1,44	1,55	1,49
01.10.2020	15,66	1,45	1,50	1,47
01.11.2020	20,28	1,47	1,67	1,49
01.12.2020	27,78	1,48	1,73	1,60
01.01.2021	43,37	1,50	1,71	1,65
01.02.2021	49,55	1,53	1,75	1,65
01.03.2021	73,26	1,54	1,83	1,64
01.04.2021	86,82	1,56	1,92	1,71
01.05.2021	85,41	1,58	1,93	1,85
01.06.2021	54,11	1,59	1,98	1,87

Zdroj: (Vlastní zpracování na základě podkladů z CoinMetrics, Investing, IMF, FRED, 2021)

4.2 Ekonometrický Model 1, cena kryptoměny bitcoin (1. 7. 2016 – 1.6.2021)

K vytvoření ekonometrického modelu byla sesbírána data 15 proměnných (1 endogenní, cena bitcoinu a 14 exogenních) za období od 1. 7. 2016 do 1. 6. 2021. Jedná se o časovou řadu v měsíčních datech, tedy o 60 pozorování.

4.2.1 Ekonomický a ekonometrický model

Teoretická východiska

Bude zkoumán vztah endogenní proměnné, která je cena kryptoměny bitcoin (y_{1t} - BTC_cena) a exogenních proměnných, které jsou velikost peněžního agregátu M2 v USA (x_{1t} - M2_USA), cena amerického akciového indexu S&P500 (x_{2t} - SPX), cena evropského akciového indexu Euro Stoxx 50 (x_{3t} - STOXX50E), cena čínského akciového indexu Shanghai Composite Index (x_{4t} - SSEC), cena indexu sledujícího zemědělské komodity Bloomberg Agriculture (x_{5t} - BCOMAG), cena indexu sledujícího kombinaci kovů IMF All Metals (x_{6t} - METALS), celková zásoba kryptoměny bitcoin (x_{7t} - BTC_zasoba), celkový výpočetní výkon sítě Bitcoinu (x_{8t} - BTC_hash_rate), celková tržní kapitalizace bitcoinu (x_{9t} - BTC_trz_kap), průměrný poplatek za transakci v Bitcoinové síti (x_{10t} - BTC_tx_pop), nově vytvořené mince za vytěžený blok v Bitcoinové síti (x_{11t} - BTC_odmena), místa akceptující platbu v bitcoinu (x_{12t} - BTC_mista), cena kryptoměny ether (x_{13t} - ETH_cena) a cena kryptoměny litecoin (x_{14t} - LTC_cena). V modelu je také zahrnut jednotkový vektor (x_{0t}). Veškeré závislosti jsou za předpokladu ceteris paribus.

Předpokládáme:

- Při růstu velikosti peněžního agregátu M2 v USA (x_{1t}) vzroste cena kryptoměny bitcoin (y_{1t}),
- Při růstu ceny amerického akciového indexu S&P500 (x_{2t}) vzroste cena kryptoměny bitcoin (y_{1t}),
- Při růstu ceny evropského akciového indexu Euro Stoxx 50 (x_{3t}) vzroste cena kryptoměny bitcoin (y_{1t}),
- Při růstu ceny čínského akciového indexu Shanghai Composite Index (x_{4t}) vzroste cena kryptoměny bitcoin (y_{1t}),

- Při růstu ceny indexu sledujícího zemědělské komodity Bloomberg Agriculture (x_{5t}) vzroste cena kryptoměny bitcoin (y_{1t}),
- Při růstu ceny indexu sledujícího kombinaci kovů IMF All Metals (x_{6t}) vzroste cena kryptoměny bitcoin (y_{1t}),
- Při růstu celkové zásoby kryptoměny bitcoin (x_{7t}) klesne cena kryptoměny bitcoin (y_{1t}),
- Při růstu celkového výpočetního výkonu sítě Bitcoinu (x_{8t}) klesne cena kryptoměny bitcoin (y_{1t}),
- Při růstu celkové tržní kapitalizace bitcoinu (x_{9t}) vzroste cena kryptoměny bitcoin (y_{1t}),
- Při růstu průměrného poplatku za transakci v Bitcoinové síti (x_{10t}) klesne cena kryptoměny bitcoin (y_{1t}),
- Při růstu počtu nově vytvořených mincí za vytěžený blok v Bitcoinové síti (x_{11t}) klesne cena kryptoměny bitcoin (y_{1t}),
- Při růstu počtu míst akceptujících platbu v Bitcoinu síti (x_{12t}) vzroste cena kryptoměny bitcoin (y_{1t}),
- Při růstu ceny kryptoměny ether (x_{13t}) vzroste cena kryptoměny bitcoin (y_{1t}),
- Při růstu ceny kryptoměny litecoin (x_{14t}) vzroste cena kryptoměny bitcoin (y_{1t}),

Deklarace proměnných

Tabulka 5: Deklarace proměnných, Model 1

Označení	Proměnná	Popis	Jednotky
y_{1t}	endogenní	Cena kryptoměny bitcoin	$1 \cdot 10^3$ USD/kus
x_{0t}		Jednotkový vektor	
x_{1t}	exogenní	Velikost peněžního agregátu M2 v USA	$1 \cdot 10^{12}$ USD
x_{2t}	exogenní	Akciový index S&P500	$1 \cdot 10^3$ USD/kus
x_{3t}	exogenní	Akciový index Euro Stoxx 50	$1 \cdot 10^3$ EUR/kus
x_{4t}	exogenní	Akciový index SSE	$1 \cdot 10^3$ CNY/kus
x_{5t}	exogenní	Index zemědělských komodit BCOMAG	USD/kus
x_{6t}	exogenní	Index kovů IMF All Metals	$1 \cdot 10^1$ USD/kus
x_{7t}	exogenní	Zásoba kryptoměny bitcoin	$1 \cdot 10^6$ kusů
x_{8t}	exogenní	Výpočetní výkon sítě Bitcoinu	EH/s
x_{9t}	exogenní	Tržní kapitalizace bitcoinu	$1 \cdot 10^{10}$ USD
x_{10t}	exogenní	Průměrný poplatek za transakci v Bitcoinové síti	USD/tx
x_{11t}	exogenní	Nově vytvořené mince v bloku	BTC/blok
x_{12t}	exogenní	Místa akceptující bitcoin	$1 \cdot 10^3$ míst
x_{13t}	exogenní	Cena kryptoměny ether	$1 \cdot 10^1$ USD/kus
x_{14t}	exogenní	Cena kryptoměny litecoin	USD/kus
u_t	stochastická	Náhodná složka v rovnici	

Zdroj: (Vlastní zpracování, 2022)

Popis dat

Podkladová data jsou k nalezení v přílohách práce (Příloha 1 a 2).

4.2.2 Korelační matice

S využitím korelační matice je zkoumáno, zda se v modelu vyskytuje mezi proměnnými vysoká, či dokonce perfektní multikolinearita. Po sestavení korelační matice je zřejmé, že mezi páry proměnných v modelu existuje vysoká multikolinearita, která by zkreslovala odhad a výsledky testování. Nejvyšší párový korelační koeficient byl zaznamenán u M2_USA – METALS s hodnotou 0,927, dále u SPX – METALS s hodnotou 0,953 a u BTC_zasoba – BTC_hash_rate s hodnotou 0,954.

Tabulka 6: Korelační matice, Model 1

Korelační matice															
Proměnná	BTC_cena	M2_USA	SPX	STOXX50E	SSEC	BCOMAG	METALS	BTC_zasoba	BTC_hash_rate	BTC_trz_kap	BTC_tx_pop	BTC_odmena	BTC_mista	ETH_cena	LTC_cena
BTC_cena	1,000	0,791	0,835	0,616	0,505	0,255	0,871	0,627	0,699	1,000	0,780	-0,682	0,657	0,951	0,620
M2_USA		1,000	0,927	0,315	0,425	-0,134	0,951	0,878	0,930	0,797	0,535	-0,928	0,836	0,688	0,470
SPX			1,000	0,575	0,419	-0,118	0,953	0,884	0,893	0,856	0,600	-0,795	0,883	0,774	0,539
STOXX50E				1,000	0,530	0,288	0,496	0,270	0,241	0,611	0,561	-0,211	0,310	0,667	0,503
SSEC					1,000	0,543	0,556	0,088	0,182	0,505	0,631	-0,525	0,032	0,607	0,420
BCOMAG						1,000	0,036	-0,517	-0,347	0,256	0,316	-0,001	-0,498	0,401	0,328
METALS							1,000	0,812	0,866	0,875	0,629	-0,862	0,794	0,810	0,607
BTC_zasoba								1,000	0,954	0,630	0,344	-0,693	0,984	0,481	0,314
BTC_hash_rate									1,000	0,705	0,379	-0,773	0,921	0,549	0,377
BTC_trz_kap										1,000	0,774	-0,688	0,658	0,948	0,622
BTC_tx_pop											1,000	-0,510	0,365	0,812	0,447
BTC_odmena												1,000	-0,628	-0,609	-0,387
BTC_mista													1,000	0,523	0,358
ETH_cena														1,000	0,689
LTC_cena															1,000

Zdroj: (Vlastní zpracování na základě podkladových dat v SW Statistica, 2022)

4.2.3 Rozšířený Dickey-Fullerův test (ADF-test)

S využitím rozšířeného Dickey-Fullerova testu je u časových řad ověřováno, zda jsou všechny řady nestacionární a lze je kombinovat. Po provedení ADF-testu u všech proměnných bylo zjištěno, že proměnné BTC_cena, STOXX50E, BTC_trz_kap a BTC_tx_pop jsou stacionární, a to i v případě diferencování řádem jedna.

Tabulka 7: ADF-test, Model 1

	ADF-test (10 zpoždění)		ADF-test u 1. dif.	
	s konst.	s konst. a trend.	s konst.	s konst. a trend.
BTC_cena	0,002	4,16E-05	2,02E-06	3,33E-05
M2_USA	0,999	0,974	-	-
SPX	0,987	0,835	-	-
STOXX50E	0,005	0,048	7,29E-12	5,51E-11
SSEC	0,614	0,859	-	-
BCOMAG	0,782	0,999	-	-
METALS	1,000	1,000	-	-
BTC_zasoba	0,378	0,998	-	-
BTC_hash_rate	0,997	0,425	-	-
BTC_trz_kap	0,843	1,64E-05	7,23E-07	1,15E-05
BTC_tx_pop	0,009	0,018	1,67E-18	1,66E-18
BTC_odmena	0,883	0,723	-	-
BTC_mista	0,949	0,904	-	-
ETH_cena	0,783	0,892	-	-
LTC_cena	1,000	1,000	-	-

Zdroj: (Vlastní zpracování na základě podkladových dat v SW Gretl, 2022)

Zvolené proměnné nelze tedy porovnávat, což je problém zejména v případě endogenní proměnné BTC_cena, kterou z modelu není možno vyřadit.

4.3 Ekonometrický Model 2, cena kryptoměny bitcoin (1. 1. 2011 – 1.6.2021)

Po zjištění problému se stacionaritou klíčové časové řady v Modelu 1, který obsahoval měsíční data za sledované období od 1. 7. 2016 do 1. 6. 2021, byla dohledána hlubší data až k 1. 1. 2011. Začátek roku 2011 je maximální možný rozsah časové řady, protože před tímto datem nebyla cena bitcoinu evidována (méně než 0,3 USD za jednotku) a obchodoval se pouze napřímo mezi dvěma stranami na základě domluvy. Je možné, že delší časová řada, by mohla tento problém se stacionaritou časové řady vyřešit. Dále jsou z modelu vyřazeny proměnné BTC_trz_kap a BTC_odmena, data pro ně tudíž nejsou ani dohledávána.

Popis dat

Podkladová data jsou k nalezení v Příloha 3 a 4

4.3.1 Rozšířený Dickey-Fullerův test (ADF-test)

Rozšíření časových řad vyřešilo problém se stacionaritou klíčové časové řady. Endogenní proměnná BTC_cena je nyní, dle výsledku ADF-testu, nestacionární. Proměnná BTC_zasoba je nestacionární pouze při diferencování řádem jedna a proměnná BTC_tx_pop je stacionární i po použití první diference.

Tabulka 8: ADF-test, Model 2

	ADF-test (10 zpoždění)		ADF-test u 1. dif.	
	s konst.	s konst. a trend.	s konst.	s konst. a trend.
BTC_cena	0,989	0,910	-	-
M2_USA	1,000	1,000	-	-
SPX	1,000	0,883	-	-
STOXX50E	0,582	0,159	-	-
SSEC	0,319	0,089	-	-
BCOMAG	0,504	0,982	-	-
METALS	0,916	1,000	-	-
BTC_zasoba	4,48E-04	0,030	0,335	0,093
BTC_hash_rate	1,000	0,999	-	-
BTC_tx_pop	0,035	0,016	1,20E-14	2,15E-14
BTC_mista	0,991	0,085	-	-
ETH_cena	0,981	0,956	-	-
LTC_cena	0,632	0,212	-	-

Zdroj: (Vlastní zpracování na základě podkladových dat v SW Gretl, 2022)

4.3.2 Sezónnost časových řad (X-12 ARIMA)

Dále jsou sledované časové řady otestovány na přítomnost sezónnosti pomocí modelu X-12 ARIMA. v tomto modelu se zajímáme o výsledky „D 8.A F-testů pro sezónnost“. Sezónnost je přítomna pouze v časové řadě BTC_mista. Tuto sezónnost je možné vyřešit přidáním sezónní diference do modelu. Nově vzniklá proměnná se poté využije namísto proměnné původní (BTC_mista).

Tabulka 9: X-12 ARIMA, Model 2

X-12 ARIMA	
F-test pro sezónnost	
BTC_cena	Ne
M2_USA	Ne
SPX	Ne
STOXX50E	Ne
SSEC	Ne
BCOMAG	Ne
METALS	Ne
BTC_zasoba	Ne
BTC_hash_rate	Ne
BTC_tx_pop	Ne
BTC_mista	Ano
ETH_cena	Nelze (nulové hodnoty)
LTC_cena	Nelze (nulové hodnoty)

Zdroj: (Vlastní zpracování na základě podkladových dat v SW Gretl, 2022)

4.3.3 Korelační matice

Z vytvořené korelační matice vychází, že párový korelační koeficient je vysoký zejména v případě proměnných BTC_zasoba s dvojicí M2_USA, SPX, BCOMAG a také BTC_mista. Dále v případě proměnné BTC_mista s dvojicí M2_USA, SPX, BCOMAG, BTC_zasoba, BTC_zasoba a BTC_hash_rate. Velmi vysoká hodnota je také mezi skupinou proměnných SPX a M2_USA.

Tabulka 10: Korelační matice, Model 2

Korelační matice													
Proměnná	BTC_cena	M2_USA	SPX	STOXX50E	SSEC	BCOMAG	METALS	BTC_zasoba	BTC_hash_rate	BTC_tx_pop	BTC_mista	ETH_cena	LTC_cena
BTC_cena	1,000	0,773	0,776	0,535	0,375	-0,338	0,389	0,502	0,786	0,823	0,652	0,925	0,832
M2_USA		1,000	0,973	0,665	0,533	-0,778	0,005	0,874	0,898	0,597	0,939	0,683	0,706
SPX			1,000	0,779	0,561	-0,798	-0,041	0,893	0,862	0,610	0,960	0,705	0,766
STOXX50E				1,000	0,694	-0,662	-0,318	0,746	0,459	0,471	0,726	0,525	0,594
SSEC					1,000	-0,553	-0,261	0,537	0,340	0,381	0,566	0,375	0,377
BCOMAG						1,000	0,501	-0,931	-0,581	-0,251	-0,891	-0,273	-0,475
METALS							1,000	-0,443	0,319	0,293	-0,166	0,364	0,193
BTC_zasoba								1,000	0,644	0,391	0,921	0,445	0,585
BTC_hash_rate									1,000	0,533	0,825	0,654	0,653
BTC_tx_pop										1,000	0,487	0,789	0,786
BTC_mista											1,000	0,577	0,707
ETH_cena												1,000	0,866
LTC_cena													1,000

Zdroj: (Vlastní zpracování na základě podkladových dat v SW Statistica, 2022)

4.3.4 Ekonomický a ekonometrický model

Na základě provedení ADF-testu, modelu X-12 ARIMA a vytvoření korelační matice na delší časové řadě (1. 1. 2011 – 1. 6. 2021) je rozhodnuto o nezařazení některých proměnných do Modelu 2. Z důvodu problému s multikolinearitou je nevyužita časová řada BTC_mista. Z důvodu stacionarity a vysoké multikolinearity je vyřazena časová řada BTC_zasoba, dále z důvodu stacionarity časová řada BTC_tx_pop.

Výsledný model nebude využívat proměnné STOXX50E a SSEC z důvodu, že při tvorbě modelu se tyto proměnné jeví jako nevýznamné. Vybrané proměnné byly využity ve formě zpožděných proměnných. Jedná se o exogenní proměnné: M2_USA zpožděnou o 3 období, SPX zpožděnou o 2 období, METALS zpožděnou o 2 období, BTC_hash_rate zpožděnou o 2 období, ETH zpožděnou o 1 období a endogenní proměnnou BTC_cena zpožděnou o jedno období.

Deklarace proměnných

Tabulka 11: Deklarace proměnných, Model 2

Označení	Proměnná	Popis	Jednotky
y_{1t}	endogenní	Cena kryptoměny bitcoin	$1 \cdot 10^3$ USD/kus
x_{0t}		Jednotkový vektor	
$x_{1(t-3)}$	exogenní zpožděná	Velikost peněžního agregátu M2 v USA zpožděná o 3 období	$1 \cdot 10^{12}$ USD
$x_{2(t-2)}$	exogenní zpožděná	Akciový index S&P500 zpožděný o 2 období	$1 \cdot 10^3$ USD/kus
x_{3t}	exogenní	Index zemědělských komodit BCOMAG	USD/kus
$x_{4(t-2)}$	exogenní zpožděná	Index kovů IMF All Metals zpožděný o 2 období	$1 \cdot 10^1$ USD/kus
$x_{5(t-2)}$	exogenní zpožděná	Výpočetní výkon sítě Bitcoinu zpožděný o 2 období	EH/s
$x_{6(t-1)}$	exogenní zpožděná	Cena kryptoměny ether zpožděná o 1 období	$1 \cdot 10^1$ USD/kus
x_{7t}	exogenní	Cena kryptoměny litecoin	USD/kus
$y_{1(t-1)}$	endogenní zpožděná	Cena kryptoměny bitcoin zpožděná o 1 období	$1 \cdot 10^3$ USD/kus
u_t	stochastická	Náhodná složka v rovnici	

Zdroj: (Vlastní zpracování, 2022)

4.3.5 Odhad parametrů pomocí BMNČ

Pro odhad modelu jsou použity měsíční pozorování z období 04.2011–06.2021 ($T=123$). Kompletní výstup ze SW Gretl je k nalezení v přílohách (Příloha 5).

Tabulka 12: Odhad parametrů BMNČ, Model 2

Proměnná	Parametr	Koeficient	t-podíl	p-hodnota
const	γ_0	-25,6655	-4,813	<0,0001
M2_USA_3	γ_1	1,92785	5,124	<0,0001
SPX_2	γ_2	-2,70446	-1,702	0,0914
BCOMAG	γ_3	0,0684213	1,860	0,0655
METALS_2	γ_4	0,311685	1,675	0,0967
BTC_hash_rate_2	γ_5	-0,0366893	-2,287	0,024
ETH_cena_1	γ_6	-0,125983	-7,936	<0,0001
LTC_cena	γ_7	0,0502558	6,475	<0,0001
BTC_cena_1	β_8	1,13577	13,83	<0,0001

Zdroj: (Vlastní zpracování na základě podkladových dat v SW Gretl, 2022)

4.3.6 Verifikace modelu

Statistická verifikace modelu

Tabulka 12 jasně udává, že všechny parametry jsou statisticky významné minimálně na hladině významnosti 0,1. Z kompletního výstupu v Příloha 5 je zřejmé, že v modelu je

vysoká shoda s daty ($R^2 = 96,00\%$) a že model jako celek je statisticky významný ($F(8, 114) = 342,129$, p -hodnota (F) = $6,17 \cdot 10^{-76}$).

Ze statistického hlediska je model verifikován.

Ekonometrická verifikace modelu

Testování autokorelace reziduí (Breusch-Godfreyův test)

Výstup z SW Gretl: „*Testovací statistika: LMF = 5,01799 s p-hodnotou = $P(F(12, 102) > 5,01799) = 1,69037e-06$* “.

V modelu se vyskytuje pozitivní autokorelace reziduí.

Normalita

Výstup z SW Gretl: „*Testovací statistika: Chí-kvadrát(2) = 69,1756 s p-hodnotou = $9,52152e-16$* “.

V modelu není normální rozdělení.

Heteroskedasticita (Whiteův test)

Výstup ze SW Gretl: „*Testovací statistika: LM = 121,156 s p-hodnotou = $P(\text{Chí kvadrát}(44) > 121,156) = 3,89989e-09$* “.

V modelu je heteroskedasticita, rozptyl náhodné složky není stále stejný v čase.

Ramseyův RESET test

Výstup ze SW Gretl: „*Testovací statistika: $F(2, 112) = 29,519$ s p-hodnotou = $P(F(2, 112) > 29,519) = 5,04676e-11$* “.

Po použití Ramseyova RESET testu je zřejmé, že pro model není zvolena vhodná funkční forma.

Po zjištění, že Model 2 nelze z ekonometrického hlediska považovat za ověřený, tudíž se dále nebudeme zabývat kvantifikací vztahů a splněním předpokladů. Bude přistoupeno k tvorbě nového modelu v mocninné funkční formě.

4.4 Ekonometrický Model 3, cena kryptoměny bitcoin (1. 9. 2015 – 1.6.2021)

Po zjištění, že Model 2 má nevhodně zvolenou funkční formu a nelze ekonomicky a ekonometricky verifikovat, je přistoupeno k tvorbě nového modelu, nyní v mocninné funkční formě. Podkladová data jsou totožná, jako pro Model 2, pouze jsou logaritmována přírodním logaritmem. Z důvodu, že cena etheru je možná sledovat pouze od 1. 9. 2015

(dřívější hodnoty jsou nulové), budou časové řady v SW Gretl automaticky zkráceny. Nulové hodnoty nelze při mocinné funkční formě využít.

Popis dat

Podkladová data jsou totožná, jako u Modelu 2. Případně k nalezení v přílohách (Příloha 3 a 4).

Deklarace proměnných

Tabulka 13: Deklarace proměnných, Model 3

Označení	Proměnná	Popis	Jednotky
y_{1t}	endogenní	Cena kryptoměny bitcoin	$1 \cdot 10^3$ USD/kus
X_{0t}		Jednotkový vektor	
x_{1t}	exogenní	Velikost peněžního agregátu M2 v USA	$1 \cdot 10^{12}$ USD
x_{2t}	exogenní	Akciový index S&P500	$1 \cdot 10^3$ USD/kus
$x_{3(t-1)}$	exogenní zpožděná	Akciový index Euro Stoxx 50 zpožděný o 1 období	$1 \cdot 10^3$ EUR/kus
$x_{4(t-1)}$	exogenní zpožděná	Index kovů IMF All Metals zpožděný o 1 období	$1 \cdot 10^1$ USD/kus
x_{5t}	exogenní	Cena kryptoměny ether	$1 \cdot 10^1$ USD/kus
x_{6t}	exogenní	Cena kryptoměny litecoin	USD/kus
$y_{1(t-1)}$	endogenní zpožděná	Cena kryptoměny bitcoin zpožděná o 1 období	$1 \cdot 10^3$ USD/kus
u_t	stochastická	Náhodná složka v rovnici	

Zdroj: (Vlastní zpracování, 2022)

4.4.1 Rozšířený Dickey-Fullerův test (ADF-test)

Z důvodu, že časové řady jsou zkráceny pro možnost využít logaritmy proměnných, byla pro jistotu znovu otestována stacionarita časových řad. Všechny časové řady jsou nestacionární a lze je využít v modelu.

4.4.2 Korelační matice

Z vytvořené korelační matice je zřejmé, že mezi dvojicemi proměnných se vyskytuje vysoká multikolinearita (zejména v hodnotách nad 0,9). Jedná se zejména o proměnné l_METALS_1 s l_M2_USA , l_SPX a l_ETH_cena , dále byly vysoké hodnoty párového korelačního koeficientu zjištěny mezi proměnnými l_SPX a l_M2_USA s hodnotou 0,931. Také mezi proměnnou l_LTC_cena a l_ETH_cena , s hodnotou 0,946. Důsledkem vysoké multikolinearity je skutečnost, že dané proměnné působí společně a nelze separovat jejich vliv. Není možné jednoznačně určit, které působí s největší intenzitou.

Tabulka 14: Korelační matice, Model 3

Korelační matice								
Proměnná	l_BTC_cena	l_BTC_cena_1	l_M2_USA	l_SPX	l_STOXX50E_1	l_METALS_1	l_ETH_cena	l_LTC_cena
l_BTC_cena	1,000	0,987	0,834	0,938	0,551	0,888	0,943	0,947
l_BTC_cena_1		1,000	0,826	0,930	0,538	0,883	0,935	0,936
l_M2_USA			1,000	0,931	0,299	0,945	0,711	0,657
l_SPX				1,000	0,505	0,954	0,841	0,821
l_STOXX50E_1					1,000	0,471	0,523	0,592
l_METALS_1						1,000	0,800	0,748
l_ETH_cena							1,000	0,946
l_LTC_cena								1,000

Zdroj: (Vlastní zpracování na základě podkladových dat v SW Statistica, 2022)

Integrovaní 1. řádu

Proměnné jsou upraveny pomocí prvních diferencí a pomocí ADF-testu je testováno, zda jsou integrovány řádu jedna. Z následující tabulky je zřejmé, že proměnná „ETH_cena“ toto kritérium nespĺňuje a není ji tedy možné v modelu využít společně se zvolenými proměnnými. Cena kryptoměny ether je integrována až 2. řádu.

Tabulka 15: Integrace 1. řádu, Model 3

Integrace proměnných						
	1. řádu			2. řádu		
	bez konst.	s konst.	s konst. a trendem	bez konst.	s konst.	s konst. a trendem
BTC_cena	5,38E-09	7,61E-08	1,04E-05	-	-	-
M2_USA	1,52E-02	1,51E-02	2,30E-05	-	-	-
SPX	8,77E-14	5,00E-11	5,37E-11	-	-	-
STOXX50E	6,06E-15	5,97E-14	1,73E-13	-	-	-
METALS	6,03E-02	4,55E-09	5,96E-10	-	-	-
ETH_cena	0,527	0,855	0,931	5,91E-12	7,96E-11	1,86E-10
LTC_cena	2,11E-07	4,44E-06	4,17E-05	-	-	-

Zdroj: (Vlastní zpracování na základě podkladových dat v SW Gretl, 2022)

S modelem není v současné formě možné dále pracovat, v modelu není možné nechat zahrnutou proměnnou „ETH_cena“ z důvodu, že není integrována řádu 1. Pro další postup bude vytvořen Model 4.

4.5 Ekonometrický Model 4, cena kryptoměny bitcoin (1. 4. 2013 – 1.6.2021)

Po zjištění, že Model 3 obsahuje proměnnou, která není integrována prvního řádu, tak jako zbylé proměnné, je přistoupeno k tvorbě Modelu 4. Z modelu 3 je odebrána právě zmiňovaná cena kryptoměny ether, která je integrována až 2. řádu a dále proměnné, které

vykazují multikolinearitu („STOXX50E“ a „METALS“). Při delším časovém období není možné cenu kryptoměny litecoin sledovat. Z výše uvedených důvodů jsou všechny časové řady sledovány od dubna 2013 do června 2021. Proměnné zůstávají nadále logaritmovány a je využita mocninná funkční forma modelu. Nejdříve byl model tvořen pomocí odhadu OLS, s využitím zbývajících predeterminovaných proměnných ($M2_USA$, SPX , LTC_cena , BTC_cena zpožděná o 1 období (Příloha 8)). Model byl odhadnut s použitím robustních směrodatných chyb (tzv. HACC errors) a následně byla pro odhad využita iterační metoda Cochran-Orcutt, která uvažuje autokorelaci a heteroskedasticitu, V tomto modelu není normální rozdělení náhodné složky (Příloha 10 a Příloha 11) a není statisticky významná závislost ceny kryptoměny bitcoin na ceně akciového indexu S&P500 a na ceně kryptoměny bitcoin v předchozím měsíci. Z tohoto důvodu jsou tyto proměnné z modelu odebrány. Poslední úpravou modelu je využití pouze tří predeterminovaných proměnných „ $M2_USA$ “, „ LTC_cena “ a „ BTC_cena zpožděná o 6 období“.

Popis dat

Podkladová data jsou totožná, jako u Modelu 2 a 3. Případně k nalezení v přílohách (Příloha 3 a 4).

4.5.1 Ekonomický a ekonometrický model

Teoretická východiska.

Bude zkoumán vztah endogenní proměnné, která je cena kryptoměny bitcoin (y_{1t} – BTC_cena) a predeterminovaných proměnných, které jsou velikost peněžního agregátu M2 v USA (x_{1t} – $M2_USA$), cena kryptoměny litecoin (x_{2t} – LTC_cena), ceny kryptoměny bitcoin zpožděná o 6 období ($y_{1(t-6)}$ – BTC_cena). V modelu je také zahrnut jednotkový vektor (x_{0t}). Veškeré závislosti jsou za předpokladu ceteris paribus.

Předpokládáme:

- Při růstu velikosti peněžního agregátu M2 v USA (x_{1t}) vzroste cena kryptoměny bitcoin (y_{1t}),
- Při růstu ceny kryptoměny litecoin (x_{2t}) vzroste cena kryptoměny bitcoin (y_{1t}),
- Při růstu ceny kryptoměny bitcoin ($y_{1(t-6)}$), zpožděné o 6 období, vzroste cena kryptoměny bitcoin (y_{1t}),

Deklarace proměnných

Tabulka 16: Deklarace proměnných, Model 4

Označení	Proměnná	Popis	Jednotky
y_{1t}	endogenní	Cena kryptoměny bitcoin	$1 \cdot 10^3$ USD/kus
x_{0t}		Jednotkový vektor	
x_{1t}	exogenní	Velikost peněžního agregátu M2 v USA	$1 \cdot 10^{12}$ USD
x_{2t}	exogenní	Cena kryptoměny litecoin	USD/kus
$y_{1(t-6)}$	endogenní zpožděná	Cena kryptoměny bitcoin zpožděná o 6 období	$1 \cdot 10^3$ USD/kus
u_t	stochastická	Náhodná složka v rovnici	

Zdroj: (Vlastní zpracování, 2022)

4.5.2 Rozšířený Dickey-Fullerův test (ADF-test)

Z důvodu, že časové řady jsou zkráceny pro možnost využít logaritmy proměnných, byla pro jistotu znovu otestována stacionarita časových řad. I ve sledovaném období od dubna roku 2013 do června roku 2021 jsou všechny sledované časové řady nestacionární a lze je využít v modelu.

Tabulka 17: ADF-test, Model 4

ADF-test (10 zpoždění)		
	s konst.	s konst. a trend.
BTC_cena	0,981	0,560
M2_USA	1,000	0,998
LTC_cena	0,591	0,263

Zdroj: (Vlastní zpracování na základě podkladových dat v SW Gretl, 2022)

4.5.3 Odhad parametrů pomocí BMNČ s HACC errors (Možnost 1)

Pro odhad modelu jsou použity měsíční pozorování z období 04.2013–06.2021 (T=99). Odhad je proveden pomocí běžné metody nejmenších čtverců s použitím robustních směrodatných odchylek. Příloha 12 zobrazuje kompletní výstup ze SW Gretl.

Tabulka 18: Odhad parametrů BMNČ, HACC errors, Model 4

Proměnná	Parametr	Koeficient	t-podíl	p-hodnota
const	γ_0	-9,93159	-12,53	<0,0001
l_M2_USA	γ_1	3,34784	10,37	<0,0001
l_LTC_cena	γ_2	0,612771	16,71	<0,0001
l_BTC_cena_6	β_3	0,163492	5,277	<0,0001

Zdroj: (Vlastní zpracování na základě podkladových dat v SW Gretl, 2022)

Verifikace modelu

Statistická verifikace modelu

Tabulka 18 jasně udává, že všechny parametry jsou statisticky významné na hladině významnosti 0,01. Z kompletního výstupu v Příloha 12 je zřejmé, že v modelu je vysoká shoda s daty ($R^2 = 98,05 \%$) a že model jako celek je statisticky významný ($F(3, 89) = 781,523$, p -hodnota (F) = $8,56 \cdot 10^{-64}$).

Ze statistického hlediska je model verifikován.

Ekonometrická verifikace modelu

Testování stacionarity odhadnutých reziduí

Mimo to, že byly na stacionaritu testovány časové řady, byla pomocí ADF-testu otestována i odhadnutá rezidua v Modelu 4. Zjištěná p -hodnota ($6,176 \cdot 10^{-8}$) je nižší, než hladina statistické významnosti $\alpha=0,05$. Rezidua jsou stacionární a v modelu nedochází ke zdánlivé regresi.

Testování autokorelace reziduí (Breusch-Godfreyův test)

Výstup z SW Gretl: „ $LMF = 9,05286$ s p -hodnotou = $P(F(12, 83) > 9,05286) = 7,72887e-11$ “.

V modelu je přítomna autokorelace reziduí.

Normalita

Výstup z SW Gretl: „*Testovací statistika: Chí-kvadrát(2) = 3,6051* s p -hodnotou = $0,164878$ “.

V modelu jsou chyby normálně rozdělené.

Heteroskedasticita (Whiteův test)

Výstup ze SW Gretl: „*Testovací statistika: LM = 7,06091* s p -hodnotou = $P(\text{Chí kvadrát}(9) > 7,06091) = 0,630778$ “.

V modelu není přítomna heteroskedasticita.

Ekonomická verifikace modelu

Z důvodu, že model je mocninný a koeficienty jak závislé, tak také všech vysvětlujících proměnných jsou vyjádřeny v exponentech, zjištěné koeficienty interpretují rovnou koeficienty pružnosti a jednotky zde nehrají roli.

Tabulka 19: Ekonomická verifikace, Model 3, Možnost 1

Proměnná	Parametr	Koeficient	Interpretace
l_M2_USA	γ_1	3,34784	Pokud se zvýší (sníží) velikost peněžního agregátu M2 v USA o 1 %, potom se zvýší (sníží) ceny kryptoměny bitcoin o 3,348 %, ceteris paribus.
l_LTC_cena	γ_6	0,612771	Pokud se zvýší (sníží) cena kryptoměny litecoin o 1 %, potom se zvýší (sníží) ceny kryptoměny bitcoin o 0,613 %, ceteris paribus.
l_BTC_cena_6	β_7	0,163492	Pokud se zvýší (sníží) cena kryptoměny bitcoin, zpožděná o 6 období, o 1 %, potom se zvýší (sníží) ceny kryptoměny bitcoin o 0,164 %, ceteris paribus.

Zdroj: (Vlastní zpracování na základě podkladových dat v SW Gretl, 2022)

Ekonomické předpoklady vždy předpokládají vztahy ceteris paribus. z pohledu ekonomické teorie je vztah velikosti peněžního agregátu M2 v USA a ceny kryptoměny bitcoin v pořádku. Zvýšení velikosti peněžního agregátu, tedy růst peněžní zásoby, způsobí příliv nových peněz do ekonomiky a zvýší ochotu lidí investovat. Hlavně mezi movitější populací se toto investování projevuje ve formě nákupu různých instrumentů ať už do nemovitosti, akcií anebo právě kryptoměn. Vztah ceny kryptoměny bitcoin s cenou kryptoměny litecoin je také validní. Při pohybech na trhu kryptoměn zažívají totožný směr působení téměř všechny kryptoměny až na občasné výjimky. Bitcoin je jakožto největší a nestabilnější kryptoměna nejméně volatilní. Působení zpožděné endogenní proměnné je dle ekonomické teorie také v pořádku, je zřejmý trend v růstu ceny a tento parametr je tedy také ověřený.

4.5.4 Odhad parametrů pomocí Cochrane-Orcutt (Možnost 2)

Jako druhá možnost pro vytvoření Modelu 4 je zvolena iterační metoda Cochrane-Orcutt. Jedná se o speciální metodu pro detekovanou heteroskedasticita a autokorelaci. Pro odhad modelu jsou použity měsíční pozorování z období 05.2013–06.2021 (T=98). Příloha 13 zachycuje kompletní výstup ze SW Gretl.

Tabulka 20: Odhad parametrů metodou Cochrane-Orcutt, Model 4

Proměnná	Parametr	Koeficient	t-podíl	p-hodnota
const	γ_0	-10,4875	-28,80	<0,0001
l_M2_USA	γ_1	3,61619	7,05	<0,0001
l_LTC_cena	γ_2	0,557319	14,90	<0,0001
l_BTC_cena_6	β_3	0,1671	3,512	0,0007

Zdroj: (Vlastní zpracování na základě podkladových dat v SW Gretl, 2022)

Verifikace modelu

Statistická verifikace modelu

Tabulka 20 jasně udává, že všechny parametry jsou statisticky významné na hladině významnosti 0,01. Z kompletního výstupu v Příloha 13 je zřejmé, že v modelu je vysoká shoda s daty ($R^2 = 99,16\%$) a že model jako celek je statisticky významný ($F(3, 94) = 322,4572$, p -hodnota (F) = $2,47 \cdot 10^{-49}$).

Ze statistického hlediska je model verifikován.

Ekonometrická verifikace modelu

Testování stacionarity odhadnutých reziduí

Mimo to, že byly na stacionaritu testovány časové řady, byla pomocí ADF-testu otestována i odhadnutá rezidua v Modelu 4. Zjištěná p -hodnota ($4,14 \cdot 10^{-17}$) je nižší, než hladina statistické významnosti $\alpha=0,05$. Rezidua jsou stacionární a v modelu nedochází ke zdánlivé regresi.

Normalita

Výstup z SW Gretl: „*Testovací statistika: Chi-kvadrát(2) = 2,58149 s p-hodnotou = 0,275066*“.

V modelu jsou chyby normálně rozdělené.

Ekonomická verifikace modelu

Tabulka 21: Ekonomická verifikace, Model 4, Možnost 2

Proměnná	Parametr	Koeficient	Interpretace
l_M2_USA	γ_1	3,61619	Pokud se zvýší (sníží) velikost peněžního agregátu M2 v USA o 1 %, potom se zvýší (sníží) ceny kryptoměny bitcoin o 3,616 %, ceteris paribus.
l_LTC_cena	γ_6	0,557319	Pokud se zvýší (sníží) cena kryptoměny litecoin o 1 %, potom se zvýší (sníží) ceny kryptoměny bitcoin o 0,557 %, ceteris paribus.
l_BTC_cena_6	β_7	0,1671	Pokud se zvýší (sníží) cena kryptoměny bitcoin, zpožděná o 6 období, o 1 %, potom se zvýší (sníží) ceny kryptoměny bitcoin o 0,167 %, ceteris paribus.

Zdroj: (Vlastní zpracování na základě podkladových dat v SW Gretl, 2022)

Model je ekonomicky verifikován, směry působení a předpoklady jsou totožné jako v možnosti 1, determinanty pouze působí s mírně odlišnou intenzitou.

4.5.5 Odhad parametrů modifikovaného modelu se zpožděnými u_t (Možnost 3)

Jako třetí možnost pro vytvoření Modelu 4 je zvolen odhad pomocí modifikované BMNČ dle Čechury (2021). Princip odhadu spočívá ve třech krocích. Nejdříve je model odhadnut pomocí běžné metody neměnných čtverců, poté jsou uložena rezidua modelu a vytvořen jejich kvadrát. Posledním krokem je odhad modelu běžnou metodou nejmenších čtverců s přidáním kvadrátu reziduí zpožděného o jedno období. Toto reziduum na sebe naváže autokorelaci modelu a odfiltruje ji z náhodné složky.

Pro odhad modelu jsou použity měsíční pozorování z období 04.2013–06.2021 ($T=99$). Prvním krokem je odhad OLS, který je k nalezení v Příloha 14. Po vytvoření kvadrátu reziduí odhadnutého modelu je proveden odhad OLS znovu i s tímto kvadrátem reziduí zpožděným o jedno období. Příloha 15 zachycuje kompletní výstup ze SW Gretl.

Tabulka 22: Odhad parametrů modifikací metody Just and Pope, Model 4

Proměnná	Parametr	Koeficient	t-podíl	p-hodnota
const	γ_0	-9,79635	-15,240	<0,0001
l_M2_USA	γ_1	3,28987	13,150	<0,0001
l_LTC_cena	γ_2	0,60813	24,840	<0,0001
l_BTC_cena_6	β_3	0,175201	6,590	<0,0001
sq_rezidua_1		0,533267	1,799	0,0753

Zdroj: (Vlastní zpracování na základě podkladových dat v SW Gretl, 2022)

Verifikace modelu

Statistická verifikace modelu

Tabulka 22 jasně udává, že všechny parametry jsou statisticky významné minimálně na hladině významnosti 0,1. Z kompletního výstupu v Příloha 15 je zřejmé, že v modelu je vysoká shoda s daty ($R^2 = 98.38 \%$) a že model jako celek je statisticky významný ($F(3, 95) = 1926,471$, p-hodnota (F) = $6,41 \cdot 10^{-85}$).

Ze statistického hlediska je model verifikován.

Ekonometrická verifikace modelu

V takto modifikovaném modelu se již ekonometrické testy neprovádějí, zpožděný kvadrát rezidua odfiltroval autokorelaci z náhodné složky modelu. Detekované problémy jsou tímto způsobem odstraněny.

Ekonomická verifikace modelu

Tabulka 23: Ekonomická verifikace, Model 4, Možnost 3

Proměnná	Parametr	Koeficient	Interpretace
l_M2_USA	γ_1	3,28987	Pokud se zvýší (sníží) velikost peněžního agregátu M2 v USA o 1 %, potom se zvýší (sníží) ceny kryptoměny bitcoin o 3,290 %, ceteris paribus.
l_LTC_cena	γ_6	0,60813	Pokud se zvýší (sníží) cena kryptoměny litecoin o 1 %, potom se zvýší (sníží) ceny kryptoměny bitcoin o 0,608 %, ceteris paribus.
l_BTC_cena_6	β_7	0,175201	Pokud se zvýší (sníží) cena kryptoměny bitcoin, zpožděná o 6 období, o 1 %, potom se zvýší (sníží) ceny kryptoměny bitcoin o 0,175 %, ceteris paribus.

Zdroj: (Vlastní zpracování na základě podkladových dat v SW Gretl, 2022)

Model je ekonomicky verifikován, směry působení a předpoklady jsou totožné jako v možnosti 1, determinanty pouze působí s mírně odlišnou intenzitou.

Bude přistoupeno k provedení aplikace Modelu 4 vytvořeného pomocí třetí možnosti výpočtu. Při srovnání možnosti výpočtu 1 (OLS s HACC errors), možnosti výpočtu 2 (metoda Cochranne-Orcutt) a možnosti výpočtu 3 (modifikovaný odhad BMNČ dle Čechury (2021)) je jednoznačně nejlepší výpočet pomocí modifikované BMNČ podle prof. Čechury. V tomto modelu jsou odstraněny všechny detekované problémy a model je ověřený pro provedení prognózy.

4.5.6 Aplikace modelu

Aplikace modelu je provedena pomocí strukturální analýzy a vysvětlení působení predeterminovaných proměnných na proměnnou endogenní. Dále je provedena prognóza ex-post.

Strukturální analýza

Z níže uvedených koeficientů pružnosti je zřejmé, že endogenní proměnná je v reakci na změny predeterminovaných proměnných ve většině případů nepružná. Pouze v případě působení proměnné x_{1t} je reakce pružná a má také nejvyšší vliv. Právě při růstu velikosti peněžního agregátu M2 v USA o 1 %, dojde k růstu ceny kryptoměny bitcoin o 3,290 %. Cena kryptoměny bitcoin je velmi silně ovlivňována velikostí tohoto agregátu. Druhý nejvyšší vliv má cena kryptoměny litecoin, kde se jedná při nárůstu ceny o 1 % o nárůst

ceny kryptoměny bitcoin o 0,608 %. Pozorovatelný je i trend ve vývoji ceny kryptoměny bitcoin, kdy na cenu působí sama endogenní proměnná zpožděná o 6 období.

Tabulka 24: Koeficienty pružnosti, Model 4, Možnost 3

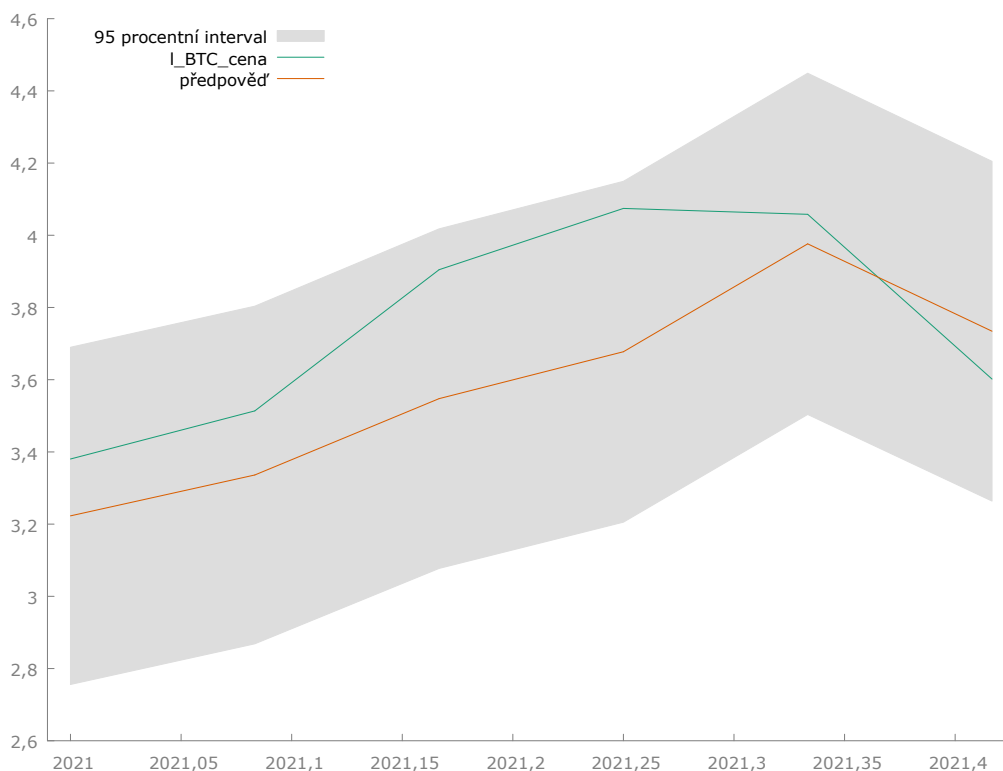
Proměnná	Koeficient pružnosti
Velikost peněžního agregátu M2 v USA, (x_{1t})	3,28987
Cena kryptoměny litecoin, (x_{2t})	0,60813
Cena kryptoměny bitcoin, zpožděná o 1 období, ($y_{1(t-6)}$)	0,175201

Zdroj: (Vlastní zpracování na základě podkladových, 2022)

Analýza ex-post

Prostřednictvím analýzy ex-post je otestována vhodnost modelu k predikci. Původní rozsah souboru je zkrácen o šest měsíců (1. – 6. 2021) a na toto období je vytvořena předpověď. K analýze je využit Model 4 s výpočtem pomocí modifikace BMNČ dle Čechury (2021). Na následujícím Grafu je zobrazeno porovnání skutečných hodnot a předpovídaných hodnot za posledních 6 období (1. - 6. 2011) se zobrazeným konfidenčním intervalem.

Graf 7: Prognóza ex-post, Model 4 (1/2)



Zdroj: (Vlastní zpracování na základě podkladových dat v SW Gretl, 2022)

Předpověď se pohybuje v konfidenčním intervalu 95 %. Z následující tabulky je zřejmé, že střední absolutní procentuální chyba nabývá hodnoty 5,7165 %. Při hodnotách střední chyby do 10 % je model vhodný k predikci.

Tabulka 25: Prognóza ex-post, Model 4 (2/2)

Pro 95% konfidenční intervaly, $t(87, 0,025) = 1,988$

	l_BTC_cena	předpověď	směr. chyba	95% konfidenční interval
2021:01	3,380338	3,222871	0,234951	2,755880 - 3,689862
2021:02	3,513641	3,336045	0,235239	2,868482 - 3,803607
2021:03	3,904685	3,547567	0,236585	3,077328 - 4,017806
2021:04	4,074465	3,677510	0,237481	3,205491 - 4,149529
2021:05	4,058088	3,976268	0,237739	3,503736 - 4,448801
2021:06	3,601724	3,734315	0,236693	3,263863 - 4,204767

Statistiky vyhodnocující předpověď using 6 observations

Střední chyba	0,17306
Odmocnina střední kvadratické chyby	0,24689
Střední absolutní chyba	0,21726
Střední procentuální chyba	4,4893
Střední absolutní procentuální chyba	5,7165
Theil's U2	0,93472
Zastoupení vychýlení, UM	0,49136
Zastoupení regrese, UR	0,028676
Zastoupení disturbancí, UD	0,47996

Zdroj: (Vlastní zpracování na základě podkladových dat v SW Gretl, 2022)

5 Závěr

Hlavním cíle práce bylo nalezení a následná kvantifikace vlivu podstatných determinant působících na vývoj ceny kryptoměny bitcoin. K cíli bylo postupováno plněním dílčích cílů. Prvním dílčím cílem bylo provedení analýzy časových řad, které byly vyhodnoceny jako stěžejní pro vysvětlení ceny kryptoměny bitcoin. Časové řady jsou sledovány s měsíční frekvencí od července roku 2016 do června roku 2021. Cena bitcoinu dosáhla od počátku sledování (678 USD/kus) svého maxima při měření 1. 4. 2021 s hodnotou 58 819 USD/kus (skutečné maximum nastalo 12. 4. v 64 895 USD/kus). Při pohledu do současnosti (k březnu roku 2022) je zřejmé, že si bitcoin stále udržuje svou silně rostoucí tendenci. 10. listopadu 2021 překonal své minulé maximum a dostal se na hodnotu 69 044 USD/kus. Koncem března 2022 se pohybuje cena bitcoinu kolem hranice 45 000 USD/kus.

Časová řada zachycující vývoj ceny akciového indexu S&P500, který silně odráží výkonost americké ekonomiky, ve sledovaném období také dosáhla znatelného růstu. Z hodnoty 2 174 USD/kus se S&P500 dostává průměrným tempem růstu (měsíčním) 1,068 % (odpovídá 14,87 % ročně) až na hranici 4 298 USD/kus ke konci sledovaného období. Index S&P500 tímto průměrným tempem růstu překonává své dlouhodobé průměrné hodnoty, které od roku 1957 činí 10,67 % meziročně.

Při zkoumání vývoje ceny indexu kovů IMF All Metals bylo zjištěno, že časová řada vykazuje podobné průměrné tempo růstu, jako akciový index S&P500. Cena indexu zaznamenává průměrné tempo růstu (měsíční) 1,068 % (odpovídá 13,60 % ročně) a z hodnoty 104,15 USD/kus se s drobnými výkyvy dostává ke konci sledovaného období na hodnotu 194,96 USD/kus.

Časová řada sezónně očištěného vývoje peněžního agregátu M2 v USA zobrazuje velmi pozvolný a stabilní nárůst. Od počátečních hodnot (12,889 bil. USD) v červenci roku 2016 zaznamenala do března roku 2020 (začátek pandemie Covid-19) nárůst o 3,122 bil. USD na hodnotu 16,011 bil. USD. Po reakci USA na situaci vzniklou zmiňovanou pandemií bylo tempo růstu znatelně navýšeno. Do konce sledovaného období došlo za pouhých 15 měsíců k nárůstu o 4,419 bil. USD. Celková zásoba agregátu M2 v USA tedy k 1. 6. 2021 činí 20,430 bil. USD.

Při využití bazických indexů, pro komparaci časových řad, je zjištěno, že od počátku sledovaného období dochází u všech sledovaných veličin ke stabilnímu růstu a jejich

kolísání ceny probíhá ve stejných okamžicích. U cen kovů jsou znatelné citlivější cenové výkyvy, než u indexu S&P500. U všech sledovaných veličin je také zřetelný prudký nárůst, až nad své původní hodnoty, po propadu spojeného se začátkem Covidové pandemie. Skutečnost odráží i prudký nárůst v zásobě peněžního agregátu M2 v USA, v totožné době, který znamená obrovský přísun peněz do ekonomiky, aby ji udržel v chodu. U ceny bitcoinu dochází k výkyvům ceny ve stejných obdobích, jako u ostatních sledovaných časových řad, jejich intenzita je ale mnohem mohutnější. Při srovnání bazických indexů je zřetelný obrovský nárůst v ceně bitcoinu, kdy se oproti původní úrovni báze dostává v posledním sledovaném období hodnota na úroveň 5 411 %. Při porovnání s cenou SPX, kde hodnota v posledním období dosáhla 159 %, nebo ceny kovů, kde hodnota činí 198 %. Je zřejmé, že SPX a kovy jsou mnohem blíže semknuté s pozvolným růstem agregátu M2 v USA, kde hodnota v posledním období dosáhla 187 % oproti původní úrovni báze.

Postupnými úpravami modelů a odstraňováním nedostatků byl vytvořen finální Model 4. Z Modelu 3 je odebrána „ETH_cena“ z důvodu integrace řádu 2, dále „STOXX50E“ a „METALS“ vykazující multikolinearitu. Z důvodu odebrání ceny kryptoměny ether je možné využít delší časovou řadu až od dubna roku 2013. Model 4 je tvořen ve 3 různých možnostech. Jako možnost 1 je proveden odhad OLS s využitím HACC errors, druhou možností je odhad pomocí iterační metody Cochrane-Orcutt a třetí možností odhad pomocí modifikované BMNČ. Právě možnost 3 je vyhodnocena jako jednoznačně nejlepší. V tomto modelu jsou odstraněny všechny detekované problémy a model je ověřený pro provedení prognózy.

Třetím dílčím cílem bylo zjistit, která z determinant působí na sledovanou veličinu nejvíce. Ze strukturální analýzy provedené pomocí koeficientů pružnosti vychází, že cena kryptoměny bitcoin je ve většině případů. Pouze v případě působení velikosti peněžního agregátu M2 v USA je reakce pružná a má také nejvyšší vliv. Právě při růstu této proměnné o 1 %, dojde k růstu ceny kryptoměny bitcoin o 3,290 %. Cena kryptoměny bitcoin je velmi silně ovlivňována velikostí tohoto agregátu. Druhý nejvyšší vliv má cena kryptoměny litecoin, kde se jedná při nárůstu ceny o 1 % o nárůst ceny kryptoměny bitcoin o 0,608 %. Pozorovatelný je i trend ve vývoji ceny kryptoměny bitcoin, kdy na cenu působí sama endogenní proměnná zpožděná o 6 období.

Posledním dílčím cílem byla aplikace modelu ve formě prognózy ex-post. K analýze je využit Model 4 (jeho třetí možnost pomocí modifikovaného odhadu BMNČ), kterému

byl pomocí softwaru Gretl zkrácen rozsah dat o šest období (1. – 6. 2021). Na těchto šest období byly poté predikovány hodnoty. V konfidenčním intervalu 95 % odpovídá střední absolutní procentuální chyba odhadu 5,407 %. Pokud se střední procentuální chyba prognózy skutečné a predikované liší o méně než 10 %, dá se model považovat za vhodný k predikci.

6 Seznam použitých zdrojů

6.1 Knižní publikace

Antonopoulos, M. Andreas. 2014. *Mastering Bitcoin: Programming the open blockchain.* místo neznámé : O'Reilly Media, Inc., 2014. ISBN: 978-1491954386.

Artl, Josef a Artlová, Markéta. 2007. *Ekonomické časové řady - vlastnosti, metody modelování, příklady a aplikace.* Praha : Grada, 2007. ISBN: 978-80-247-1319-9.

— . **2003.** *Finanční časové řady.* Praha : Grada, 2003. ISBN: 80-247-0330-0.

Blockchain - ICBC 2018. **Chen, Shiping, Wang, Harry a Zhang, Liang-Jie. 2018.** místo neznámé : Springer, 2018. ISBN: 9783319944784.

Cipra, Tomáš. 1986. *Analýza časových řad s aplikacemi v ekonometrii.* Praha : SNTL, 1986.

— . **2013.** *Finanční ekonometrie.* Praha : Ekopress, 2013. ISBN: 978-80-86929-93-4.

— . **2008.** *Finanční ekonometrie.* Praha : Ekopress, 2008. ISBN: 978-80-86929-43-9.

Coen, David. 2019. *Q/A about Bitcoin.* místo neznámé : David Coen, 2019. ISBN: 9781697134780.

Čechura, Lukáš, a další. 2013. *Cvičení z ekonometrie.* Praha : ČZU, 2013. ISBN: 978-80-213-2405-3.

Hančlová, Jana. 2012. *Ekonometrické modelování: klasické přístupy s aplikacemi.* Praha : Professional, 2012. ISBN: 978-80-7431-088-1.

Hanych, Michal, Drgová, Anna a Gremlica, Michal. 2018. *Zdanění kryptoměn.* Brno : Michal Hanych, 2018. ISBN: 978-80-87934-07-4.

Hindls, Richard, a další. 2007. *Statistika pro ekonomy.* Praha : Professional publishing, 2007. ISBN: 978-80-86946-43-6.

Hušek, Roman. 2009. *Aplikovaná ekonometrie: teorie a praxe.* Praha : Oeconomica, 2009. ISBN: 978-80-245-1623-3.

— . **1995.** *Základy ekonometrické analýzy.* Praha : VŠE, 1995. ISBN: 8070791020.

Chilamkurti, Naveen, Poongodi, T. a Balusamy, Balamurugan. 2021. *Blockchain, Internet of Things, and Artificial Intelligence.* místo neznámé : CRC Press, 2021. ISBN: 9781000359510.

Kaliský, Boris. 2018. *Bitcoin a ti druzí.* Praha : IFP Publishing s.r.o., 2018. ISBN: 978-80-87383-71-1.

Mathis, Tim. 2018. *Ethereum: Your Guide To Understanding Ethereum, Blockchain, and Cryptocurrency.* místo neznámé : Level Up Lifestyle Limited, 2018. ISBN: 9781984152183.

Pritzker, Yan. 2020. *Vynález jménem Bitcoin.* místo neznámé : BRAIINS Publishing, 2020. ISBN: 978-80-907975-1-2.

Samuelson, Paul A. a Nordhaus, William D. 2013. *Ekonomie 19. vydání.* Praha : NS Svoboda, 2013. ISBN: 978-80-205-0629-0.

Stroukal, Dominik a Skalický, Jan. 2021. *Bitcoin a jiné kryptopeníze budoucnosti: historie, ekonomie a technologie kryptoměn.* Praha : Grada Publishing, a.s., 2021. ISBN 978-80-271-1043-8.

Stroukal, Dominik. 2018. Praha je podle Forbesu hlavním městem Bitcoinu. *roklen24.cz*. [Online] 3. 8 2018. [Citace: 14. 6 2021.] <https://roklen24.cz/praha-je-podle-forbesu-hlavnim-mestem-bitcoinu-umistil-se-i-zatec/>.

Tvrdoň, Jiří. 2001. *Ekonometrie.* Praha : ČZU, 2001. ISBN: 80-213-0819-2.

6.2 Internetové zdroje

BBC. 2021. Bitcoin: El Salvador makes cryptocurrency legal tender. *bbc.com*. [Online] 2021. [Citace: 17. 6 2021.] <https://www.bbc.com/news/world-latin-america-57398274>.

Binance academy. 2021. Block header. *academy.binance.com*. [Online] 2021. [Citace: 8. 6 2021.] <https://academy.binance.com/en/glossary/block-header>.

—. 2021. Mempool. *academy.binance.com*. [Online] 2021. [Citace: 10. 6 2021.] <https://academy.binance.com/en/glossary/mempool>.

—. 2021. What Schnorr Signatures Mean for Bitcoin? *academy.binance.com*. [Online] 29. 5 2021. [Citace: 27. 6 2021.] <https://academy.binance.com/en/articles/what-do-schnorr-signatures-mean-for-bitcoin>.

Bitaddress. 2021. Paper Wallet. *bitaddress.org*. [Online] 2021. [Citace: 24. 6 2021.] <https://www.bitaddress.org/bitaddress.org-v3.3.0-SHA256-dec17c07685e1870960903d8f58090475b25af946fe95a734f88408cef4aa194.html>.

Bitcoin magazine. 2020. Is Bitcoin Anonymous. *bitcoinmagazine.com*. [Online] 17. 8 2020. [Citace: 19. 6 2021.] <https://bitcoinmagazine.com/guides/is-bitcoin-anonymous>.

Blockchain. 2021. Bitcoin Explorer. *blockchain.com*. [Online] 2021. [Citace: 14. 6 2021.] <https://www.blockchain.com/explorer>.

Braiins. 2021. První těžební pool na světě. *cs.braiins.com*. [Online] 2021. [Citace: 20. 6 2021.] <https://cs.braiins.com/>.

BTC.com. 2021. Pool Distribution. *explorer.btc.com*. [Online] 2021. [Citace: 28. 6 2021.] <https://explorer.btc.com/btc/insights-pools>.

—. 2021. Stats. *btc.com*. [Online] 2021. [Citace: 7. 6 2021.] <https://btc.com/stats/diff>.

Coinatmradar.com. 2021. Crypto ATM Distribution by Continents and Countries. *coinatmradar.com*. [Online] 2021. [Citace: 27. 6 2021.] <https://coinatmradar.com/charts/geo-distribution/>.

Coinmap. 2021. Map. *coinmap.org*. [Online] 2021. [Citace: 27. 6 2021.] <https://coinmap.org/view/#/map/50.12321958/14.21630859/9/atm>.

—. 2021. Map. *coinmap.org*. [Online] 2021. [Citace: 30. 6 2021.] <https://coinmap.org/view/#/world/49.87516778/15.08972168/8>.

- CoinMarketCap. 2021.** Bitcoin Halving Countdown. *coinmarketcap.com*. [Online] 2021. [Citace: 28. 6 2021.] <https://coinmarketcap.com/halving/bitcoin/>.
- Coinmate. 2021.** Home. *coinmate.io*. [Online] 2021. [Citace: 28. 6 2021.] <https://coinmate.io/>.
- CoinMetrics. 2021.** Data file download. *coinmetrics.io*. [Online] 2021. [Citace: 1. 10 2021.] <https://coinmetrics.io/community-network-data/>.
- Cointelegraph. 2016.** World's Best Performing Currency. *cointelegraph.com*. [Online] 2016. [Citace: 28. 6 2021.] <https://cointelegraph.com/storage/uploads/view/1d067f3721f10f0a76439de9860a4e54.png>.
- Cointelegraph. 2016.** Antonopoulos: Your Keys, Your Bitcoin. Not Your Keys, Not Your Bitcoin. *cointelegraph.com*. [Online] 10. 8 2016. [Citace: 25. 6 2021.] <https://cointelegraph.com/news/antonopoulos-your-keys-your-bitcoin-not-your-keys-not-your-bitcoin>.
- CryptoSvet. 2020.** Kdo je Marek "Slush" Palatinus? *cryptosvet.cz*. [Online] 5. 2 2020. [Citace: 17. 6 2021.] <https://cryptosvet.cz/slushpool-penezenka-trezor/>.
- CryptoSvet.cz. 2020.** Jak vybrat krypto peněženku? *cryptosvet.cz*. [Online] 2020. [Citace: 20. 6 2021.] <https://cryptosvet.cz/bitcoin-penezenka-na-kryptomeny/>.
- Čechura, Lukáš, a další. 2021.** Climate Change and Sustainability in Czech Wheat Production. *Agris on-line Papers in Economics and Informatics*. 2021, Sv. XIII, 4.
- Fillner, Karel. 2018.** Jak na bitcoin. *btctip.cz*. [Online] 2018. [Citace: 21. 6 2021.] <https://btctip.cz/wp-content/uploads/2018/05/jak-na-bitcoin-karel-fillner-aktualizace.pdf>.
- Finex Media. 2021.** Kryptoměnové peněženky. *finex.cz*. [Online] 2021. [Citace: 19. 6 2021.] <https://finex.cz/rubrika/kryptomeny/penezenky/>.
- Finex. 2021.** Zdanění kryptoměn. *finex.cz*. [Online] 4. 6 2021. [Citace: 18. 6 2021.] <https://finex.cz/zdaneni-kryptomen-kompletni-navod/>.
- FRED. 2021.** M2 and Components. *fred.stlouisfed.org*. [Online] 28. 12 2021. [Citace: 10. 1 2022.] <https://fredaccount.stlouisfed.org/datalists/273545/download>.
- Frue, Keisha. 2018.** SWOT Analysis of Bitcoin. *pestleanalysis.com*. [Online] 24. 10 2018. [Citace: 19. 6 2021.] <https://pestleanalysis.com/swot-analysis-of-bitcoin/>.
- GameKyuubi. 2013.** I AM HODLING. *bitcointalk.org*. [Online] 18. 12 2013. [Citace: 19. 6 2021.] <https://bitcointalk.org/index.php?topic=375643.0>.
- General Bytes. 2021.** BATMFour. *generalbytes.com*. [Online] 2021. [Citace: 27. 6 2021.] <https://www.generalbytes.com/res/crc-1771206473/products/images/519x650/q90/f-Sinc/603478-vx-batmfoura.png>.
- Generální finanční ředitelství. 2018.** Zdanění kryptoměn. *simpletax.cz*. [Online] 2018. [Citace: 28. 6 2021.] https://www.simpletax.cz/files/vyjadreni_gfr_kryptomeny.pdf.
- Hamilton, David. 2020.** The Lightning Network and Atomic Swaps. *bitcoinlightning.com*. [Online] 5. 12 2020. [Citace: 26. 6 2021.] <https://www.bitcoinlightning.com/how-the-lightning-network-will-change-the-way-we-exchange-crypto/>.
- Chainalysis. 2021.** Know what happens on blockchains. *chainalysis.com*. [Online] 2021. [Citace: 27. 6 2021.] <https://www.chainalysis.com/company/>.

- IMF. 2021.** Comodity prices. *imf.org*. [Online] 2021. [Citace: 23. 1 2022.] <https://www.imf.org/-/media/Files/Research/CommodityPrices/Monthly/external-datadecember.ashx>.
- Insider Inc. 2021.** One of the world's biggest bitcoin exchanges has been hacked. *businessinsider.com*. [Online] 2021. [Citace: 24. 6 2021.] <https://www.businessinsider.com/south-korean-bitcoin-exchange-bithumb-hacked-ethereum-2017-7>.
- Investing. 2021.** S&P 500 (SPX). *investing.com*. [Online] 2021. [Citace: 5. 11 2021.] <https://www.investing.com/indices/us-spx-500-historical-data>.
- Investopedia. 2021.** How to Buy Bitcoin. *investopedia.com*. [Online] 1. 6 2021. [Citace: 14. 6 2021.] <https://www.investopedia.com/articles/investing/082914/basics-buying-and-investing-bitcoin.asp>.
- . **2021.** Mt. Gox. *investopedia.com*. [Online] 26. 3 2021. [Citace: 25. 6 2021.] <https://www.investopedia.com/terms/m/mt-gox.asp>.
- Janda, Aleš. 2021.** Bitcoinový block explorer. *walletexplorer.com*. [Online] 2021. [Citace: 18. 6 2021.] <https://www.walletexplorer.com/>.
- Kohout, Martin. 2021.** Poradíme, jak Bitcoin bezpečně uchovat. *freebit.cz*. [Online] 5. 3 2021. [Citace: 17. 6 2021.] <https://freebit.cz/poradime-jak-bitcoin-bezpecne-uchovat/>.
- Krause, Tomáš. 2021.** Peněženky na bitcoiny a další kryptoměny. *bitcoinvkapse.cz*. [Online] 2021. [Citace: 22. 6 2021.] <https://bitcoinvkapse.cz/penezenky-bitcoiny-kryptomeny/>.
- KryptoHodler.cz. 2021.** Hardwarová peněženka. *krypthodler.cz*. [Online] 2021. [Citace: 18. 6 2021.] <https://krypthodler.cz/navod-pro-novacky-jak-si-mam-zalozit-hardwarovou-penezenku-trezor-nebo-leger-2-dil/>.
- Ledger SAS. 2021.** Getting Started. *ledger.com*. [Online] 2021. [Citace: 17. 6 2021.] <https://www.ledger.com/start>.
- Maverick, J. B. 2022.** What Is the Average Annual Return for the S&P 500? *investopedia.com*. [Online] 13. 1 2022. [Citace: 15. 1 2022.] <https://www.investopedia.com/ask/answers/042415/what-average-annual-return-sp-500.asp>.
- Mempool.space. 2021.** Mempool.space. *Mempool.space*. [Online] 2021. [Citace: 27. 6 2021.] <https://mempool.space/cs/>.
- Mikulášek, Filip. 2021.** Bitcoin FOMO. *finex.cz*. [Online] 6. 5 2021. [Citace: 17. 6 2021.] <https://finex.cz/bitcoin-fomo-jak-zachovat-chladnou-hlavu/>.
- Nakamoto, Satoshi. 2014.** Bitcoin open source implementation of P2P currency. *p2pfoundation.ning.com*. [Online] 7. 3 2014. [Citace: 3. 6 2021.] http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source?commentId=2003008%3AComment%3A52186&_xg_source=activity.
- . **2008.** Bitcoin: A Peer-to-Peer Electronic Cash System. *bitcoin.org*. [Online] 31. 10 2008. <https://bitcoin.org/bitcoin.pdf>.
- . **2009.** Summary. *bitcointalk.org*. [Online] 2009. <https://bitcointalk.org/index.php?action=profile;u=3>.

- Ogino, Ozora. 2021.** Proof-of-stake (PoS). *ethereum.org*. [Online] 16. 4 2021. [Citace: 23. 6 2021.] <https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/>.
- Osato, Avan-Nomayo. 2021.** Bitcoin Taproot locked in to improve privacy and introduce smart contracts. *coinelegraph.com*. [Online] 26. 6 2021. [Citace: 28. 6 2021.] <https://coinelegraph.com/news/bitcoin-taproot-locked-in-to-improve-privacy-and-introduce-smart-contracts>.
- Rajput, Vinita. 2020.** The SWOT Analysis of Crypto-currency and Bitcoin. *researchgate.net*. [Online] 2020. [Citace: 26. 6 2021.] https://www.researchgate.net/publication/347439921_The_SWOT_Analysis_of_Crypto-currency_and_Bitcoin.
- SatoshiLabs. 2018.** 7 Years of Hardware Wallets. *blog.trezor.io*. [Online] 6. 12 2018. [Citace: 18. 6 2021.] <https://blog.trezor.io/7-years-of-hardware-wallets-the-success-story-of-czech-crypto-enthusiasts-creating-a-brand-new-6648769d373a>.
- , **2021.** Do you need to pay tax on crypto? *blog.trezor.io*. [Online] 30. 3 2021. [Citace: 17. 6 2021.] <https://blog.trezor.io/do-you-need-to-pay-tax-on-crypto-a9c6ca8c8c91>.
- , **2021.** Welcome to Trezor. *trezor.io*. [Online] 2021. [Citace: 16. 6 2021.] <https://trezor.io/start/>.
- Slush Pool. 2021.** Introduction to mining. *SlushPool.com*. [Online] 2021. [Citace: 8. 6 2021.] <https://help.slushpool.com/en/support/solutions/articles/77000417314-introduction-to-mining-%E2%98%85>.
- Soukup, Tomáš. 2021.** Lightning Network. *finex.cz*. [Online] 26. 6 2021. [Citace: 25. 6 2021.] <https://finex.cz/lightning-network/>.
- Thoma, Mike a Vaughan, Brooks. 2021.** CORE Report: Bitcoin (Abridged). *cryptoeq.io*. [Online] 15. 6 2021. [Citace: 26. 6 2021.] <https://www.cryptoeq.io/corereports/bitcoin-abridged>.
- Wolf, Karel. 2021.** Centralizovaně, nebo decentralizovaně: jak kupovat kryptoměny? *lupa.cz*. [Online] 18. 1 2021. [Citace: 18. 6 2021.] <https://www.lupa.cz/clanky/centralizovane-nebo-decentralizovane-jak-kupovat-kryptomeny/>.
- Wuille, Pieter. 2020.** BIP 341: Taproot: SegWit version 1 spending rules. *bips.dev*. [Online] 19. 1 2020. [Citace: 28. 6 2021.] <https://bips.dev/341/>.
- Zhang, Ren. 2017.** On the Necessity of a Prescribed Block Validity Consensus: Analyzing Bitcoin Unlimited Mining Protoco. *researchgate.net*. [Online] 2017. [Citace: 8. 6 2021.] https://www.researchgate.net/figure/An-example-in-which-two-blocks-are-orphaned-by-one-Alices-block-Carol-switches-to-Chain_fig2_321234622.

7 Přílohy

Příloha 1: Podkladová data, Model 1 (1/2)	87
Příloha 2: Podkladová data, Model 1 (2/2)	88
Příloha 3: Podkladová data, Model 2 (1/2)	89
Příloha 4: Podkladová data, Model 2 (2/2)	90
Příloha 5: Odhad Modelu 2	91
Příloha 6: Odhad Modelu 3	92
Příloha 7: Instrumentální proměnné pro Model 3	93
Příloha 8: Odebrání statisticky nevýznamných proměnných, OLS	94
Příloha 9: Odebrání statisticky nevýznamných proměnných, OLS, HACC errors.....	95
Příloha 10: Odebrání statisticky nevýznamných proměnných, Cochrane-Orcutt (1/2).....	96
Příloha 11: Odebrání statisticky nevýznamných proměnných, Cochrane-Orcutt (2/2).....	97
Příloha 12: Odhad Modelu 4, Možnost 1, OLS, HACC errors	98
Příloha 13: Odhad Modelu 4, Možnost 2, Cochrane-Orcutt	99
Příloha 14: Odhad Modelu 4, Možnost 3, Modifikace Just and Pope, 1.krok	100
Příloha 15: Odhad Modelu 4, Možnost 3, Modifikace Just and Pope, 3.krok	101

Příloha 1: Podkladová data, Model 1 (1/2)

Datum	BTC cena	JV	M2 USA	SPX	STOXX50E	SSEC	BCOMAG	METALS
	1*10 ³ USD/kus		1*10 ¹² USD	1*10 ³ USD/kus	1*10 ³ EUR/kus	1*10 ³ CNY/kus	USD/kus	1*10 ³ USD/kus
Označení	y_{1t}	x_{0t}	x_{1t}	x_{2t}	x_{3t}	x_{4t}	x_{5t}	x_{6t}
01.07.2016	0,678	1	12,889	2,174	2,991	2,979	55,573	10,415
01.08.2016	0,607	1	12,968	2,171	3,023	3,085	52,900	10,530
01.09.2016	0,572	1	13,027	2,168	3,002	3,005	55,131	10,342
01.10.2016	0,615	1	13,100	2,126	3,055	3,100	56,829	10,134
01.11.2016	0,731	1	13,174	2,199	3,052	3,250	55,187	10,721
01.12.2016	0,754	1	13,214	2,239	3,291	3,104	53,918	10,606
01.01.2017	0,997	1	13,289	2,279	3,231	3,159	55,684	10,870
01.02.2017	0,988	1	13,359	2,364	3,320	3,242	55,503	11,414
01.03.2017	1,228	1	13,429	2,363	3,501	3,223	52,237	11,314
01.04.2017	1,090	1	13,487	2,384	3,560	3,155	51,560	10,943
01.05.2017	1,437	1	13,537	2,412	3,555	3,117	50,402	10,583
01.06.2017	2,400	1	13,565	2,423	3,442	3,192	51,912	10,567
01.07.2017	2,412	1	13,622	2,470	3,449	3,273	52,305	10,823
01.08.2017	2,727	1	13,671	2,472	3,421	3,361	48,673	11,507
01.09.2017	4,918	1	13,714	2,519	3,595	3,349	48,631	11,592
01.10.2017	4,382	1	13,768	2,575	3,674	3,393	48,137	11,361
01.11.2017	6,726	1	13,802	2,648	3,570	3,317	48,281	11,459
01.12.2017	10,809	1	13,855	2,674	3,504	3,307	47,509	11,587
01.01.2018	13,465	1	13,872	2,824	3,609	3,481	48,088	12,201
01.02.2018	9,040	1	13,915	2,714	3,439	3,259	50,294	12,227
01.03.2018	10,924	1	13,971	2,641	3,362	3,169	48,815	11,931
01.04.2018	6,805	1	14,001	2,648	3,537	3,082	49,438	12,031
01.05.2018	9,072	1	14,066	2,705	3,407	3,095	49,646	11,935
01.06.2018	7,520	1	14,126	2,718	3,396	2,847	44,375	11,904
01.07.2018	6,361	1	14,155	2,816	3,525	2,876	45,492	11,301
01.08.2018	7,597	1	14,198	2,902	3,393	2,725	42,703	11,059
01.09.2018	7,192	1	14,228	2,914	3,399	2,821	41,741	11,028
01.10.2018	6,562	1	14,236	2,712	3,198	2,603	42,560	11,269
01.11.2018	6,343	1	14,255	2,760	3,173	2,588	42,658	11,213
01.12.2018	4,148	1	14,374	2,507	3,001	2,494	41,552	11,189
01.01.2019	3,808	1	14,443	2,704	3,159	2,585	42,725	11,471
01.02.2019	3,445	1	14,486	2,784	3,298	2,941	40,982	12,081
01.03.2019	3,811	1	14,534	2,834	3,352	3,091	39,995	12,111
01.04.2019	4,138	1	14,569	2,946	3,515	3,078	38,577	12,192
01.05.2019	5,315	1	14,668	2,752	3,280	2,899	41,412	12,116
01.06.2019	8,555	1	14,787	2,942	3,474	2,979	41,551	12,534
01.07.2019	10,570	1	14,858	2,980	3,467	2,933	39,345	13,073
01.08.2019	10,400	1	14,935	2,926	3,427	2,886	37,295	12,691
01.09.2019	9,763	1	15,027	2,977	3,569	2,905	38,792	12,868
01.10.2019	8,315	1	15,153	3,038	3,604	2,929	39,409	12,684
01.11.2019	9,251	1	15,251	3,141	3,704	2,872	39,184	12,345
01.12.2019	7,418	1	15,326	3,231	3,745	3,050	41,381	12,611
01.01.2020	7,171	1	15,407	3,226	3,641	2,977	39,124	13,115
01.02.2020	9,382	1	15,470	2,954	3,329	2,880	38,457	12,942
01.03.2020	8,542	1	16,011	2,585	2,787	2,750	37,188	12,455
01.04.2020	6,643	1	17,039	2,912	2,928	2,860	35,075	12,534
01.05.2020	8,856	1	17,889	3,044	3,050	2,852	34,755	12,960
01.06.2020	10,199	1	18,176	3,100	3,234	2,985	35,372	13,567
01.07.2020	9,241	1	18,317	3,271	3,174	3,310	36,265	14,391
01.08.2020	11,798	1	18,379	3,500	3,273	3,396	38,257	15,470
01.09.2020	11,970	1	18,602	3,363	3,194	3,218	39,571	15,473
01.10.2020	10,607	1	18,748	3,270	2,958	3,225	41,122	15,318
01.11.2020	13,737	1	18,959	3,622	3,493	3,392	43,486	15,541
01.12.2020	18,821	1	19,130	3,756	3,553	3,473	48,013	16,612
01.01.2021	29,381	1	19,393	3,714	3,481	3,483	50,317	17,169
01.02.2021	33,570	1	19,665	3,811	3,636	3,509	52,204	17,187
01.03.2021	49,634	1	19,913	3,973	3,919	3,442	51,273	17,128
01.04.2021	58,819	1	20,139	4,181	3,975	3,447	58,475	17,789
01.05.2021	57,864	1	20,403	4,204	4,039	3,615	57,926	19,249
01.06.2021	36,661	1	20,430	4,298	4,064	3,591	57,816	19,496

Zdroj: (Vlastní zprac. na základě podkladů z CoinMetrics, FRED, Investing, IMF, 2021)

Příloha 2: Podkladová data, Model 1 (2/2)

Datum	BTC_zasoba	BTC_hash_rate	BTC_trz_kap	BTC_tx_pop	BTC_odmena	BTC_mista	ETH_cena	LTC_cena
	$1 \cdot 10^6$ kusů	EH/s	$1 \cdot 10^{10}$ USD	USD/tx	BTC/blok	$1 \cdot 10^3$ míst	$1 \cdot 10^1$ USD/kus	USD/kus
Označení	X_{1t}	X_{2t}	X_{3t}	X_{4t}	X_{5t}	X_{6t}	X_{7t}	X_{8t}
01.07.2016	15,722	1,614	1,065	0,187	12,500	8,576	1,186	3,810
01.08.2016	15,790	1,624	0,958	0,192	12,500	8,658	1,163	3,980
01.09.2016	15,848	1,536	0,907	0,153	12,500	8,787	1,330	3,840
01.10.2016	15,905	1,883	0,979	0,169	12,500	8,873	1,096	4,360
01.11.2016	15,962	1,815	1,166	0,234	12,500	8,993	0,862	4,070
01.12.2016	16,018	2,045	1,207	0,338	12,500	9,142	0,800	3,850
01.01.2017	16,077	2,464	1,603	0,380	12,500	9,309	1,071	7,250
01.02.2017	16,139	3,751	1,594	0,442	12,500	9,528	1,586	16,200
01.03.2017	16,192	3,155	1,989	0,905	12,500	9,623	4,972	25,880
01.04.2017	16,249	3,278	1,770	0,821	12,500	9,739	8,351	39,490
01.05.2017	16,305	3,892	2,343	1,114	12,500	9,945	21,834	42,270
01.06.2017	16,366	5,036	3,928	4,283	12,500	10,168	27,562	73,230
01.07.2017	16,422	5,802	3,962	2,756	12,500	10,337	20,081	55,260
01.08.2017	16,483	6,372	4,495	1,537	12,500	10,723	38,730	55,410
01.09.2017	16,538	7,682	8,134	6,595	12,500	11,094	30,344	85,820
01.10.2017	16,598	7,134	7,274	2,558	12,500	11,498	30,369	227,170
01.11.2017	16,659	11,266	11,205	5,621	12,500	12,025	43,221	163,879
01.12.2017	16,714	12,254	18,066	6,379	12,500	12,667	73,677	202,010
01.01.2018	16,776	14,924	22,589	26,594	12,500	13,129	111,808	116,340
01.02.2018	16,840	20,704	15,223	7,642	12,500	13,428	85,249	148,327
01.03.2018	16,894	24,667	18,455	2,390	12,500	13,693	39,396	118,462
01.04.2018	16,952	28,152	11,535	0,918	12,500	13,933	67,007	81,272
01.05.2018	17,010	31,590	15,432	1,453	12,500	14,224	57,787	78,961
01.06.2018	17,069	35,541	12,836	0,734	12,500	14,413	45,267	62,033
01.07.2018	17,126	37,103	10,895	0,689	12,500	14,686	43,150	61,224
01.08.2018	17,184	44,362	13,054	0,672	12,500	14,854	28,194	49,943
01.09.2018	17,244	50,496	12,403	0,641	12,500	15,093	23,280	32,228
01.10.2018	17,300	56,178	11,352	0,587	12,500	15,317	19,859	29,893
01.11.2018	17,354	54,989	11,008	0,391	12,500	15,705	11,377	31,428
01.12.2018	17,402	41,011	7,219	0,515	12,500	15,842	13,190	45,820
01.01.2019	17,457	41,616	6,648	0,182	12,500	16,056	10,671	60,785
01.02.2019	17,514	45,670	6,034	0,321	12,500	16,195	13,547	74,235
01.03.2019	17,566	48,897	6,694	0,326	12,500	16,327	14,179	114,479
01.04.2019	17,622	43,128	7,293	0,710	12,500	16,449	16,180	122,993
01.05.2019	17,677	54,004	9,396	0,778	12,500	16,657	26,799	98,781
01.06.2019	17,736	55,994	15,173	4,010	12,500	16,789	29,221	64,271
01.07.2019	17,792	56,404	18,805	4,038	12,500	16,925	21,723	55,961
01.08.2019	17,852	63,627	18,566	1,432	12,500	17,121	17,162	58,429
01.09.2019	17,910	76,105	17,486	0,692	12,500	17,261	18,035	47,523
01.10.2019	17,968	90,704	14,940	1,174	12,500	17,355	18,237	41,287
01.11.2019	18,025	88,479	16,675	1,167	12,500	17,490	15,195	68,044
01.12.2019	18,078	89,642	13,410	0,585	12,500	17,581	12,921	58,078
01.01.2020	18,136	112,930	13,004	0,281	12,500	17,681	17,991	39,078
01.02.2020	18,195	116,092	17,070	0,546	12,500	17,772	21,752	46,400
01.03.2020	18,247	136,265	15,586	0,395	12,500	17,979	13,286	45,611
01.04.2020	18,300	105,814	12,157	0,639	12,500	18,014	20,622	41,196
01.05.2020	18,356	111,857	16,255	2,859	6,250	18,060	23,181	58,156
01.06.2020	18,392	100,837	18,758	2,639	6,250	18,099	22,563	60,957
01.07.2020	18,420	127,111	17,023	1,516	6,250	18,198	34,651	46,258
01.08.2020	18,449	114,737	21,765	4,989	6,250	18,235	43,390	55,730
01.09.2020	18,477	134,413	22,118	3,988	6,250	18,293	35,939	87,664
01.10.2020	18,505	119,057	19,628	3,656	6,250	18,349	38,642	124,162
01.11.2020	18,531	124,259	25,456	8,900	6,250	18,396	61,592	129,400
01.12.2020	18,560	144,751	34,930	7,323	6,250	18,461	73,594	165,119
01.01.2021	18,588	137,764	54,612	5,470	6,250	18,516	131,273	196,661
01.02.2021	18,617	123,182	62,496	15,538	6,250	20,270	141,876	271,080
01.03.2021	18,642	140,389	92,529	22,161	6,250	20,530	191,799	188,169
01.04.2021	18,671	157,607	109,820	17,088	6,250	20,636	277,278	144,150
01.05.2021	18,696	158,216	108,183	21,976	6,250	20,843	270,847	270,847
01.06.2021	18,724	148,573	68,645	7,321	6,250	21,465	227,384	227,384

Zdroj: (Vlastní zpracování na základě podkladů z CoinMetrics, Investing, 2021)

Příloha 3: Podkladová data, Model 2 (1/2)

Datum	BTC cena	JV	M2_USA	SPX	STOXX50E	SSEC	BCOMAG	METALS	BTC zasoba	BTC hash rate	BTC tx pop	BTC místa	ETH cena	LTC cena
	1*10 ³ USD/kus		1*10 ¹² USD	1*10 ³ USD/kus	1*10 ³ EUR/kus	1*10 ³ CNY/kus	USD/kus	1*10 ³ USD/kus	1*10 ³ kusů	EH/s	USD/tx	1*10 ³ míst	1*10 ³ USD/kus	USD/kus
Označení	y _{t1}	x _{0t}	x _{t1}	x _{t1}	x _{t1}	x _{t1}	x _{t1}	x _{t1}	x _{t1}	x _{t1}	x _{0t}	x _{t1}	x _{t1}	x _{t1}
01.01.2011	0,000	1	8,820	1,286	2,954	2,791	94,425	16,921	5,030	0,000	0,000	0,000	0,000	0,000
01.02.2011	0,001	1	8,884	1,327	3,013	2,905	95,311	17,507	5,287	0,000	0,001	0,000	0,000	0,000
01.03.2011	0,001	1	8,941	1,326	2,911	2,928	93,490	17,099	5,563	0,000	0,000	0,000	0,000	0,000
01.04.2011	0,001	1	9,002	1,364	3,011	2,912	93,521	17,663	5,811	0,000	0,002	0,000	0,000	0,000
01.05.2011	0,003	1	9,073	1,345	2,862	2,743	91,869	17,284	6,065	0,000	0,009	0,000	0,000	0,000
01.06.2011	0,010	1	9,148	1,321	2,849	2,762	84,364	17,121	6,403	0,000	0,036	0,000	0,000	0,000
01.07.2011	0,015	1	9,314	1,292	2,670	2,702	86,716	17,555	6,715	0,000	0,027	0,000	0,000	0,000
01.08.2011	0,013	1	9,505	1,219	2,302	2,567	94,705	17,973	6,960	0,000	0,012	0,000	0,000	0,000
01.09.2011	0,008	1	9,526	1,131	2,180	2,359	76,740	17,626	7,177	0,000	0,007	0,000	0,000	0,000
01.10.2011	0,005	1	9,560	1,253	2,385	2,468	79,693	15,924	7,386	0,000	0,003	0,000	0,000	0,000
01.11.2011	0,003	1	9,610	1,247	2,330	2,333	74,767	15,847	7,573	0,000	0,003	0,000	0,000	0,000
01.12.2011	0,003	1	9,658	1,258	2,317	2,199	77,781	15,452	7,782	0,000	0,002	0,000	0,000	0,000
01.01.2012	0,005	1	9,732	1,312	2,417	2,293	77,254	15,893	8,010	0,000	0,004	0,000	0,000	0,000
01.02.2012	0,006	1	9,789	1,366	2,512	2,428	79,978	16,500	8,246	0,000	0,004	0,000	0,000	0,000
01.03.2012	0,005	1	9,837	1,408	2,477	2,263	80,242	16,250	8,464	0,000	0,005	0,000	0,000	0,000
01.04.2012	0,005	1	9,890	1,398	2,306	2,396	79,962	16,046	8,697	0,000	0,003	0,000	0,000	0,000
01.05.2012	0,005	1	9,935	1,310	2,119	2,372	72,045	15,244	8,909	0,000	0,003	0,000	0,000	0,000
01.06.2012	0,005	1	9,998	1,362	2,265	2,225	82,033	14,963	9,129	0,000	0,003	0,000	0,000	0,000
01.07.2012	0,007	1	10,055	1,379	2,326	2,104	93,749	14,754	9,355	0,000	0,003	0,000	0,000	0,000
01.08.2012	0,010	1	10,115	1,407	2,441	2,048	94,228	14,304	9,594	0,000	0,006	0,000	0,000	0,000
01.09.2012	0,010	1	10,193	1,441	2,454	2,086	90,050	14,990	9,839	0,000	0,009	0,000	0,000	0,000
01.10.2012	0,012	1	10,257	1,412	2,504	2,069	87,039	15,270	10,072	0,000	0,008	0,000	0,000	0,000
01.11.2012	0,011	1	10,320	1,416	2,575	1,980	84,586	15,162	10,303	0,000	0,009	0,000	0,000	0,000
01.12.2012	0,013	1	10,452	1,426	2,636	2,269	80,808	15,494	10,513	0,000	0,010	0,000	0,000	0,000
01.01.2013	0,013	1	10,477	1,498	2,703	2,385	83,294	16,001	10,618	0,000	0,011	0,000	0,000	0,000
01.02.2013	0,020	1	10,489	1,515	2,634	2,366	80,188	15,965	10,729	0,000	0,018	0,001	0,000	0,000
01.03.2013	0,035	1	10,556	1,569	2,624	2,237	78,237	15,147	10,845	0,000	0,037	0,003	0,000	0,000
01.04.2013	0,104	1	10,590	1,598	2,712	2,178	77,946	14,386	10,980	0,000	0,085	0,037	0,000	1,517
01.05.2013	0,116	1	10,630	1,631	2,770	2,301	77,970	13,722	11,103	0,000	0,102	0,054	0,000	4,350
01.06.2013	0,129	1	10,683	1,606	2,603	1,979	74,725	13,079	11,229	0,000	0,098	0,068	0,000	2,823
01.07.2013	0,083	1	10,729	1,686	2,768	1,994	72,502	13,034	11,358	0,000	0,049	0,121	0,000	2,667
01.08.2013	0,097	1	10,784	1,633	2,721	2,098	74,215	13,675	11,493	0,000	0,072	0,187	0,000	2,743
01.09.2013	0,131	1	10,835	1,682	2,893	2,175	72,774	13,557	11,640	0,001	0,070	0,301	0,000	2,429
01.10.2013	0,128	1	10,949	1,757	3,068	2,142	71,124	13,436	11,779	0,001	0,087	0,426	0,000	2,305
01.11.2013	0,203	1	10,954	1,806	3,087	2,221	71,226	13,289	11,935	0,004	0,157	1,007	0,000	2,400
01.12.2013	0,964	1	11,020	1,848	3,109	2,116	69,224	13,121	12,064	0,007	0,251	1,758	0,000	34,948
01.01.2014	0,752	1	11,077	1,783	3,014	2,033	68,901	13,066	12,205	0,012	0,164	2,386	0,000	23,871
01.02.2014	0,813	1	11,169	1,859	3,149	2,056	76,830	13,071	12,341	0,021	0,170	2,767	0,000	22,311
01.03.2014	0,568	1	11,208	1,872	3,162	2,033	80,643	12,859	12,463	0,027	0,111	3,289	0,000	13,841
01.04.2014	0,479	1	11,260	1,884	3,198	2,026	83,451	12,591	12,591	0,043	0,092	3,637	0,000	13,080
01.05.2014	0,460	1	11,326	1,924	3,245	2,039	77,453	12,715	12,717	0,070	0,084	3,945	0,000	11,303
01.06.2014	0,630	1	11,377	1,960	3,228	2,048	72,593	12,522	12,843	0,091	0,123	4,213	0,000	11,057
01.07.2014	0,643	1	11,434	1,931	3,116	2,202	67,281	12,884	12,970	0,111	0,121	4,496	0,000	8,267
01.08.2014	0,597	1	11,463	2,003	3,173	2,217	65,767	12,757	13,089	0,146	0,095	4,768	0,000	7,743
01.09.2014	0,475	1	11,497	1,972	3,226	2,364	59,489	12,513	13,217	0,185	0,074	4,938	0,000	4,776
01.10.2014	0,383	1	11,559	2,018	3,113	2,420	64,790	11,717	13,336	0,267	0,063	5,146	0,000	4,456
01.11.2014	0,324	1	11,595	2,068	3,251	2,683	64,050	11,413	13,452	0,284	0,059	5,329	0,000	3,552
01.12.2014	0,379	1	11,674	2,059	3,146	3,235	62,818	11,177	13,562	0,260	0,053	5,538	0,000	3,561
01.01.2015	0,315	1	11,744	1,995	3,351	3,210	59,215	11,095	13,676	0,333	0,043	5,752	0,000	2,710
01.02.2015	0,227	1	11,872	2,105	3,599	3,310	60,524	10,775	13,789	0,318	0,032	5,880	0,000	1,831
01.03.2015	0,261	1	11,888	2,068	3,697	3,748	57,273	10,452	13,894	0,325	0,041	6,069	0,000	1,905
01.04.2015	0,247	1	11,928	2,086	3,616	4,442	56,971	10,415	14,007	0,307	0,035	6,192	0,000	1,668
01.05.2015	0,233	1	11,958	2,107	3,571	4,612	54,974	10,721	14,114	0,350	0,032	6,302	0,000	1,409
01.06.2015	0,223	1	12,003	2,063	3,424	4,277	62,017	10,376	14,225	0,312	0,037	6,638	0,000	1,602
01.07.2015	0,258	1	12,052	2,104	3,601	3,664	55,124	9,657	14,335	0,332	0,038	6,862	0,000	3,949
01.08.2015	0,282	1	12,101	1,972	3,270	3,206	53,000	9,524	14,450	0,403	0,063	7,031	0,000	4,208
01.09.2015	0,228	1	12,155	1,920	3,101	3,053	54,177	9,549	14,565	0,415	0,044	7,187	0,136	2,824
01.10.2015	0,238	1	12,193	2,079	3,418	3,383	55,034	9,577	14,676	0,445	0,051	7,297	0,065	2,999
01.11.2015	0,330	1	12,277	2,080	3,506	3,445	53,535	8,864	14,791	0,473	0,059	7,451	0,099	3,871
01.12.2015	0,363	1	12,340	2,044	3,268	3,539	52,985	8,578	14,907	0,604	0,064	7,520	0,086	3,438
01.01.2016	0,435	1	12,471	1,940	3,045	2,738	52,545	8,633	15,033	0,697	0,069	7,595	0,092	3,521
01.02.2016	0,371	1	12,552	1,932	2,946	2,688	51,069	9,231	15,155	0,961	0,095	7,659	0,217	3,042
01.03.2016	0,433	1	12,617	2,060	3,005	3,004	53,320	9,800	15,269	1,146	0,094	7,740	0,753	3,408
01.04.2016	0,417	1	12,697	2,065	3,028	2,938	57,056	9,911	15,383	1,267	0,106	7,844	1,163	3,254
01.05.2016	0,455	1	12,764	2,097	3,063	2,917	59,000	9,833	15,495	1,377	0,082	8,008	0,878	3,728
01.06.2016	0,538	1	12,831	2,099	2,865	2,930	60,038	9,844	15,610	1,417	0,130	8,106	1,391	4,725
01.07.2016	0,678	1	12,889	2,174	2,991	2,979	55,573	10,415	15,722	1,614	0,187	8,191	1,228	4,290
01.08.2016	0,607	1	12,968	2,171	3,023	3,085	52,900	10,530	15,790	1,624	0,192	8,273	1,101	3,857
01.09.2016	0,572	1	13,027	2,168	3,002	3,005	55,131	10,342	15,848	1,536	0,153	8,402	1,212	3,816
01.10.2016	0,615	1	13,100	2,126	3,055	3,100	56,829	10,134	15,905	1,883	0,169	8,488	1,324	3,845
01.11.2016	0,731	1	13,174	2,199	3,052	3,250	55,187	10,721	15,962	1,815	0,234	8,608	1,081	4,094
01.12.2016	0,754	1	13,214	2,239	3,291	3,104	53,918	10,606	16,018	2,045	0,338	8,757	0,846	3,896

Zdroj: (Vlastní zprac. na základě podkladů z CoinMetrics, FRED, Investing, IMF, 2021)

Příloha 4: Podkladová data, Model 2 (2/2)

Datum	BTC cena	JV	M2 USA	SPX	STOXX50E	SSEC	BCOMAG	METALS	BTC zasoba	BTC hash rate	BTC tx pop	BTC mista	ETH cena	LTC cena
	1*10 ³ USD/kus		1*10 ¹² USD	1*10 ³ USD/kus	1*10 ³ EUR/kus	1*10 ³ CNY/kus	USD/kus	1*10 ³ USD/kus	1*10 ³ kusů	EH/s	USD/tx	1*10 ³ mist	1*10 ³ USD/kus	USD/kus
Označení	y _t	x _{0t}	x _{1t}	x _{2t}	x _{3t}	x _{4t}	x _{5t}	x _{6t}	x _{7t}	x _{8t}	x _{9t}	x _{10t}	x _{11t}	x _{12t}
01.01.2017	0,997	1	13,289	2,279	3,231	3,159	55,684	10,870	16,077	2,464	0,380	8,924	0,818	4,475
01.02.2017	0,988	1	13,359	2,364	3,320	3,242	55,503	11,414	16,139	3,751	0,442	9,143	1,072	4,048
01.03.2017	1,228	1	13,429	2,363	3,501	3,223	52,237	11,314	16,192	3,155	0,905	9,238	1,727	3,854
01.04.2017	1,090	1	13,487	2,384	3,560	3,155	51,560	10,943	16,249	3,278	0,821	9,354	5,069	7,603
01.05.2017	1,437	1	13,537	2,412	3,555	3,117	50,402	10,583	16,305	3,892	1,114	9,560	7,837	16,107
01.06.2017	2,400	1	13,565	2,423	3,442	3,192	51,912	10,567	16,366	5,036	4,283	9,783	22,099	27,302
01.07.2017	2,412	1	13,622	2,470	3,449	3,273	52,305	10,823	16,422	5,802	2,756	9,952	26,122	38,116
01.08.2017	2,727	1	13,671	2,472	3,421	3,361	48,673	11,507	16,483	6,372	1,537	10,338	22,574	43,123
01.09.2017	4,918	1	13,714	2,519	3,595	3,349	48,631	11,592	16,538	7,682	6,595	10,709	39,160	87,876
01.10.2017	4,382	1	13,768	2,575	3,674	3,393	48,137	11,361	16,598	7,134	2,558	11,113	30,292	54,721
01.11.2017	6,726	1	13,802	2,648	3,570	3,317	48,281	11,459	16,659	11,266	5,621	11,640	29,052	53,286
01.12.2017	10,809	1	13,855	2,674	3,504	3,307	47,509	11,587	16,714	12,254	6,379	12,282	46,159	98,665
01.01.2018	13,465	1	13,872	2,824	3,609	3,481	48,088	12,201	16,776	14,924	26,594	12,744	75,607	224,817
01.02.2018	9,040	1	13,915	2,714	3,439	3,259	50,294	12,227	16,840	20,704	7,642	13,043	101,917	141,184
01.03.2018	10,924	1	13,971	2,641	3,362	3,169	48,815	11,931	16,894	24,667	2,390	13,308	86,930	209,269
01.04.2018	6,805	1	14,001	2,648	3,537	3,082	49,438	12,031	16,952	28,152	0,918	13,548	37,807	114,629
01.05.2018	9,072	1	14,066	2,705	3,407	3,095	49,646	11,935	17,010	31,590	1,453	13,839	67,153	147,990
01.06.2018	7,520	1	14,126	2,718	3,396	2,847	44,375	11,904	17,069	35,541	0,734	14,028	57,883	119,946
01.07.2018	6,361	1	14,155	2,816	3,525	2,876	45,492	11,301	17,126	37,103	0,689	14,301	45,180	79,894
01.08.2018	7,597	1	14,198	2,902	3,393	2,725	42,703	11,059	17,184	44,362	0,672	14,469	41,902	77,566
01.09.2018	7,192	1	14,228	2,914	3,399	2,821	41,741	11,028	17,244	50,496	0,641	14,708	29,494	66,280
01.10.2018	6,562	1	14,236	2,712	3,198	2,603	42,560	11,269	17,300	56,178	0,587	14,932	22,992	60,014
01.11.2018	6,343	1	14,255	2,760	3,173	2,588	42,658	11,213	17,354	54,989	0,391	15,320	19,782	50,108
01.12.2018	4,148	1	14,374	2,507	3,001	2,494	41,552	11,189	17,402	41,011	0,515	15,457	11,697	33,763
01.01.2019	3,808	1	14,443	2,704	3,159	2,585	42,725	11,471	17,457	41,616	0,182	15,671	13,915	31,646
01.02.2019	3,445	1	14,486	2,784	3,298	2,941	40,982	12,081	17,514	45,670	0,321	15,810	10,663	32,535
01.03.2019	3,811	1	14,534	2,834	3,352	3,091	39,995	12,111	17,566	48,897	0,326	15,942	13,486	46,995
01.04.2019	4,138	1	14,569	2,946	3,515	3,078	38,577	12,192	17,622	43,128	0,710	16,064	14,130	60,384
01.05.2019	5,315	1	14,668	2,752	3,280	2,899	41,412	12,116	17,677	54,004	0,778	16,272	15,822	72,498
01.06.2019	8,555	1	14,787	2,942	3,474	2,979	41,551	12,534	17,736	55,994	4,010	16,404	26,514	112,711
01.07.2019	10,570	1	14,858	2,980	3,467	2,933	39,345	13,073	17,792	56,404	4,038	16,540	29,386	122,677
01.08.2019	10,400	1	14,935	2,926	3,427	2,886	37,295	12,691	17,852	63,627	1,432	16,736	21,735	98,841
01.09.2019	9,763	1	15,027	2,977	3,569	2,905	38,792	12,868	17,910	76,105	0,692	16,876	17,121	66,297
01.10.2019	8,315	1	15,153	3,038	3,604	2,929	39,409	12,684	17,968	90,704	1,174	16,970	17,664	55,766
01.11.2019	9,251	1	15,251	3,141	3,704	2,872	39,184	12,345	18,025	88,479	1,167	17,105	18,336	58,372
01.12.2019	7,418	1	15,326	3,231	3,745	3,050	41,381	12,611	18,078	89,642	0,585	17,196	15,138	47,739
01.01.2020	7,171	1	15,407	3,226	3,641	2,977	39,124	13,115	18,136	112,930	0,281	17,296	12,996	41,416
01.02.2020	9,382	1	15,470	2,954	3,329	2,880	38,457	12,942	18,195	116,092	0,546	17,387	18,356	70,725
01.03.2020	8,542	1	16,011	2,585	2,787	2,750	37,188	12,455	18,247	136,265	0,395	17,594	21,862	57,878
01.04.2020	6,643	1	17,039	2,912	2,928	2,860	35,075	12,534	18,300	105,814	0,639	17,629	13,585	39,332
01.05.2020	8,856	1	17,889	3,044	3,050	2,852	34,755	12,960	18,356	111,857	2,859	17,675	21,271	47,143
01.06.2020	10,199	1	18,176	3,100	3,234	2,985	35,372	13,567	18,392	100,837	2,639	17,714	24,907	48,407
01.07.2020	9,241	1	18,317	3,271	3,174	3,310	36,265	14,391	18,420	127,111	1,516	17,813	23,115	41,803
01.08.2020	11,798	1	18,379	3,500	3,273	3,396	38,257	15,470	18,449	114,737	4,989	17,850	38,719	61,691
01.09.2020	11,970	1	18,602	3,363	3,194	3,218	39,571	15,473	18,477	134,413	3,988	17,908	48,075	63,070
01.10.2020	10,607	1	18,748	3,270	2,958	3,225	41,122	15,318	18,505	119,057	3,656	17,964	35,236	46,168
01.11.2020	13,737	1	18,959	3,622	3,493	3,392	43,486	15,541	18,531	124,259	8,900	18,011	39,558	55,539
01.12.2020	18,821	1	19,130	3,756	3,553	3,473	48,013	16,612	18,560	144,751	7,323	18,076	58,825	85,295
01.01.2021	29,381	1	19,393	3,714	3,481	3,483	50,317	17,169	18,588	137,764	5,470	18,131	73,091	126,167
01.02.2021	33,570	1	19,666	3,811	3,636	3,509	52,204	17,187	18,617	123,182	15,538	19,885	136,995	132,619
01.03.2021	49,634	1	19,913	3,973	3,919	3,442	51,273	17,128	18,642	140,389	22,161	20,145	156,324	175,665
01.04.2021	58,819	1	20,139	4,181	3,975	3,447	58,475	17,789	18,671	157,607	17,088	20,251	197,124	202,667
01.05.2021	57,864	1	20,403	4,204	4,039	3,615	57,926	19,249	18,696	158,216	21,976	20,458	294,932	277,167
01.06.2021	36,661	1	20,429	4,298	4,064	3,591	57,816	19,496	18,724	148,573	7,321	21,080	262,620	183,131

Zdroj: (Vlastní zprac. na základě podkladů z CoinMetrics, FRED, Investing, IMF, 2021)

Příloha 5: Odhad Modelu 2

Model 2: OLS, za použití pozorování 2011:04-2021:06 (T = 123)

Závisle proměnná: BTC_cena

	koeficient	směr. chyba	t-podíl	p-hodnota	
const	-25,6655	5,33209	-4,813	4,59e-06	***
M2_USA_3	1,92785	0,376260	5,124	1,23e-06	***
SPX_2	-2,70446	1,58861	-1,702	0,0914	*
BCOMAG	0,0684213	0,0367849	1,860	0,0655	*
METALS_2	0,311685	0,186118	1,675	0,0967	*
BTC_hash_rate_2	-0,0366893	0,0160416	-2,287	0,0240	**
ETH_cena_1	-0,125983	0,0158754	-7,936	1,60e-012	***
LTC_cena	0,0502558	0,00776198	6,475	2,49e-09	***
BTC_cena_1	1,13577	0,0821127	13,83	3,84e-026	***
Střední hodnota závisle proměnné		5,132637			
Sm. odchylka závisle proměnné		10,15079			
Součet čtverců reziduí		502,6466			
Sm. chyba regrese		2,099805			
Koeficient determinace		0,960014			
Adjustovaný koeficient determinace		0,957208			
F(8, 114)		342,1286			
P-hodnota (F)		6,17e-76			
Logaritmus věrohodnosti		-261,1032			
Akaikovo kritérium		540,2063			
Schwarzovo kritérium		565,5160			
Hannan-Quinnovo kritérium		550,4871			
rho (koeficient autokorelace)		0,287727			
Durbinovo h		7,724139			

zde je poznámka o zkratkách statistik modelu

Whiteův test heteroskedasticity -

Nulová hypotéza: není zde heteroskedasticita

Testovací statistika: LM = 121,156

s p-hodnotou = $P(\text{Chi-kvadrát}(44) > 121,156) = 3,89989e-09$

Test normality reziduí -

Nulová hypotéza: chyby jsou normálně rozdělené

Testovací statistika: Chi-kvadrát(2) = 69,1756

s p-hodnotou = $9,52152e-16$

LM test pro autokorelaci až do řádu 12 -

Nulová hypotéza: žádná autokorelace

Testovací statistika: LMF = 5,01799

s p-hodnotou = $P(F(12, 102) > 5,01799) = 1,69037e-06$

Test RESET pro specifikaci -

Nulová hypotéza: specifikace je adekvátní

Testovací statistika: F(2, 112) = 29,519

s p-hodnotou = $P(F(2, 112) > 29,519) = 5,04676e-11$

Zdroj: (Vlastní zpracování na základě podkladových dat v SW Gretl, 2022)

Příloha 6: Odhad Modelu 3

Model 3: OLS, za použití pozorování 2015:09-2021:06 (T = 70)
 Závisle proměnná: l_BTC_cena

	koeficient	směr. chyba	t-podíl	p-hodnota	
const	-4,81604	1,25930	-3,824	0,0003	***
l_M2_USA	1,44991	0,603699	2,402	0,0193	**
l_SPX	0,953743	0,495813	1,924	0,0590	*
l_STOXX50E_1	0,348124	0,379326	0,9177	0,3623	
l_METALS_1	-0,313274	0,498060	-0,6290	0,5317	
l_ETH_cena	0,0596268	0,0346803	1,719	0,0905	*
l_LTC_cena	0,293608	0,0595526	4,930	6,46e-06	***
l_BTC_cena_1	0,410256	0,0703972	5,828	2,17e-07	***
Střední hodnota závisle proměnné		1,363260			
Sm. odchylka závisle proměnné		1,442252			
Součet čtverců reziduí		1,703853			
Sm. chyba regrese		0,165775			
Koeficient determinace		0,988129			
Adjustovaný koeficient determinace		0,986788			
F(7, 62)		737,2361			
P-hodnota(F)		3,66e-57			
Logaritmus věrohodnosti		30,72042			
Akaikovo kritérium		-45,44083			
Schwarzovo kritérium		-27,45287			
Hannan-Quinnovo kritérium		-38,29579			
rho (koeficient autokorelace)		0,263748			
Durbinovo h		2,730544			

zde je poznámka o zkratkách statistik modelu

Pomine-li se konstanta, p-hodnota byla nejvyšší pro proměnnou 22 (l_METALS_1)

Whiteův test heteroskedasticity -

Nulová hypotéza: není zde heteroskedasticita

Testovací statistika: LM = 43,7953

s p-hodnotou = $P(\text{Chi-kvadrát}(35) > 43,7953) = 0,146299$

Test normality reziduí -

Nulová hypotéza: chyby jsou normálně rozdělené

Testovací statistika: Chi-kvadrát(2) = 1,30304

s p-hodnotou = 0,521253

LM test pro autokorelaci až do řádu 12 -

Nulová hypotéza: žádná autokorelace

Testovací statistika: LMF = 1,65522

s p-hodnotou = $P(F(12, 50) > 1,65522) = 0,106432$

CUSUM test pro stabilitu parametrů -

Nulová hypotéza: žádná změna v parametrech

Testovací statistika: Harvey-Collier $t(61) = -1,112$

s p-hodnotou = $P(t(61) > -1,112) = 0,270503$

Test RESET pro specifikaci -

Nulová hypotéza: specifikace je adekvátní

Testovací statistika: $F(2, 60) = 0,817156$

s p-hodnotou = $P(F(2, 60) > 0,817156) = 0,446541$

Zdroj: (Vlastní zpracování na základě podkladových dat v SW Gretl, 2022)

Příloha 7: Instrumentální proměnné pro Model 3

Model 4: TSLS, za použití pozorování 2015:09-2021:06 (T = 70)
 Závisle proměnná: l_BTC_cena
 Instrumentální proměnné: const l_M2_USA l_SPX l_STOXX50E_l l_METALS_l
 l_ETH_cena l_LTC_cena l_BTC_cena_l

	koeficient	směr. chyba	t-podíl	p-hodnota	
const	-4,27739	0,985234	-4,341	5,14e-05	***
l_M2_USA	1,07944	0,446278	2,419	0,0184	**
l_SPX	1,03299	0,435090	2,374	0,0206	**
l_ETH_cena	0,0504665	0,0326603	1,545	0,1272	
l_LTC_cena	0,308096	0,0569111	5,414	9,90e-07	***
l_BTC_cena_l	0,406581	0,0696078	5,841	1,89e-07	***

Střední hodnota závisle proměnné 1,363260
 Sm. odchylka závisle proměnné 1,442252
 Součet čtverců reziduí 1,729502
 Sm. chyba regrese 0,164388
 Koeficient determinace 0,987950
 Adjustovaný koeficient determinace 0,987009
 F(5, 64) 1049,435
 P-hodnota(F) 5,53e-60
 Logaritmus věrohodnosti 30,19747
 Akaikovo kritérium -48,39494
 Schwarzovo kritérium -34,90397
 Hannan-Quinnovo kritérium -43,03616
 rho (koeficient autokorelace) 0,277615
 Durbinovo h 2,857233

zde je poznámka o zkratkách statistik modelu

Sarganův test pro nadbytečnou identifikaci -
 Nulová hypotéza: všechny instrumentální proměnné jsou platné
 Testovací statistika: LM = 1,03812
 s p-hodnotou = P(Chi-kvadrát(2) > 1,03812) = 0,59508

Pesaran-Taylorův test heteroskedasticity -
 Nulová hypotéza: není zde heteroskedasticita
 Asymptotická testovací statistika: z = 1,27017
 s p-hodnotou = 0,204022

Test normality reziduí -
 Nulová hypotéza: chyby jsou normálně rozdělené
 Testovací statistika: Chi-kvadrát(2) = 1,45375
 s p-hodnotou = 0,483417

LM test pro autokorelaci až do řádu 12 -
 Nulová hypotéza: žádná autokorelace
 Testovací statistika: LMF = 1,98849
 s p-hodnotou = P(F(12, 52) > 1,98849) = 0,0518471

Zdroj: (Vlastní zpracování na základě podkladových dat v SW Gretl, 2022)

Příloha 8: Odebrání statisticky nevýznamných proměnných, OLS

Model 7: OLS, za použití pozorování 2013:04-2021:06 (T = 99)

Závisle proměnná: 1_BTC_cena

	koeficient	směr. chyba	t-podíl	p-hodnota	
const	-5,18726	0,915082	-5,669	1,57e-07	***
1_M2_USA	1,25047	0,429765	2,910	0,0045	***
1_SPX	1,33023	0,409390	3,249	0,0016	***
1_LTC_cena	0,396746	0,0375109	10,58	1,10e-017	***
1_BTC_cena_1	0,364337	0,0555527	6,558	2,92e-09	***

Střední hodnota závisle proměnné	0,602565
Sm. odchylka závisle proměnné	1,735892
Součet čtverců reziduí	3,410210
Sm. chyba regrese	0,190470
Koeficient determinace	0,988452
Adjustovaný koeficient determinace	0,987961
F(4, 94)	2011,470
P-hodnota (F)	4,11e-90
Logaritmus věrohodnosti	26,25821
Akaikovo kritérium	-42,51643
Schwarzovo kritérium	-29,54083
Hannan-Quinnovo kritérium	-37,26648
rho (koeficient autokorelace)	0,335938
Durbinovo h	4,010953

zde je poznámka o zkratkách statistik modelu

Breusch-Paganův test heteroskedasticity -

Nulová hypotéza: není zde heteroskedasticita

Testovací statistika: LM = 13,9106

s p-hodnotou = $P(\text{Chí-kvadrát}(4) > 13,9106) = 0,00758608$

Whiteův test heteroskedasticity -

Nulová hypotéza: není zde heteroskedasticita

Testovací statistika: LM = 28,7826

s p-hodnotou = $P(\text{Chí-kvadrát}(14) > 28,7826) = 0,0111809$

Test normality reziduí -

Nulová hypotéza: chyby jsou normálně rozdělené

Testovací statistika: Chí-kvadrát(2) = 7,90718

s p-hodnotou = 0,0191857

LM test pro autokorelaci až do řádu 12 -

Nulová hypotéza: žádná autokorelace

Testovací statistika: LMF = 2,65368

s p-hodnotou = $P(F(12, 82) > 2,65368) = 0,00470527$

Zdroj: (Vlastní zpracování na základě podkladových dat v SW Gretl, 2022)

Příloha 9: Odebrání statisticky nevýznamných proměnných, OLS, HACC errors

Model 9: OLS, za použití pozorování 2013:04-2021:06 (T = 99)
 Závisle proměnná: l_BTC_cena
 HAC standardní chyby, šířka okénka 3 (Bartlettovo jádro)

	koeficient	směr. chyba	t-podíl	p-hodnota	
const	-5,18726	0,877058	-5,914	5,35e-08	***
l_M2_USA	1,25047	0,363844	3,437	0,0009	***
l_SPX	1,33023	0,389326	3,417	0,0009	***
l_LTC_cena	0,396746	0,0630584	6,292	9,87e-09	***
l_BTC_cena_l	0,364337	0,0876191	4,158	7,08e-05	***

Střední hodnota závisle proměnné 0,602565
 Sm. odchylka závisle proměnné 1,735892
 Součet čtverců reziduí 3,410210
 Sm. chyba regrese 0,190470
 Koeficient determinace 0,988452
 Adjustovaný koeficient determinace 0,987961
 F(4, 94) 1416,404
 P-hodnota(F) 4,71e-83
 Logaritmus věrohodnosti 26,25821
 Akaikovo kritérium -42,51643
 Schwarzovo kritérium -29,54083
 Hannan-Quinnovo kritérium -37,26648
 rho (koeficient autokorelace) 0,335938
 Durbinovo h 6,823404

zde je poznámka o zkratkách statistik modelu

Whiteův test heteroskedasticity -

Nulová hypotéza: není zde heteroskedasticita

Testovací statistika: LM = 28,7826

s p-hodnotou = $P(\text{Chí-kvadrát}(14) > 28,7826) = 0,0111809$

Breusch-Paganův test heteroskedasticity -

Nulová hypotéza: není zde heteroskedasticita

Testovací statistika: LM = 13,9106

s p-hodnotou = $P(\text{Chí-kvadrát}(4) > 13,9106) = 0,00758608$

Test normality reziduí -

Nulová hypotéza: chyby jsou normálně rozdělené

Testovací statistika: Chí-kvadrát(2) = 7,90718

s p-hodnotou = 0,0191857

Zdroj: (Vlastní zpracování na základě podkladových dat v SW Gretl, 2022)

Příloha 10: Odebrání statisticky nevýznamných proměnných, Cochrane-Orcutt (1/2)

Model 10: Cochrane-Orcutt, za použití pozorování 2013:05–2021:06 (T = 98)

Závisle proměnná: l_BTC_cena

rho = 0,760876

	koeficient	směr. chyba	t-podíl	p-hodnota	
const	-11,0904	0,468154	-23,69	3,57e-041	***
l_M2_USA	3,63379	0,856390	4,243	5,21e-05	***
l_SPX	0,650251	0,480786	1,352	0,1795	
l_LTC_cena	0,547309	0,0432642	12,65	6,31e-022	***
l_BTC_cena_1	0,0597401	0,0672637	0,8881	0,3768	

Statistika založená na rho-diferencovaných datech:

Součet čtverců reziduí	2,628668
Sm. chyba regrese	0,168123
Koeficient determinace	0,990880
Adjustovaný koeficient determinace	0,990488
F(4, 93)	172,6175
P-hodnota(F)	3,85e-42
rho (koeficient autokorelace)	0,009954
Durbinovo h	0,132079

zde je poznámka o zkratkách statistik modelu

Statistika založená na původních datech:

Střední hodnota závisle proměnné	0,631850
Sm. odchylka závisle proměnné	1,720059

zde je poznámka o zkratkách statistik modelu

Pomine-li se konstanta, p-hodnota byla nejvyšší pro proměnnou 15 (l_BTC_cena_1)

Test normality reziduí -

Nulová hypotéza: chyby jsou normálně rozdělené

Testovací statistika: Chi-kvadrát(2) = 11,5569

s p-hodnotou = 0,00309352

Zdroj: (Vlastní zpracování na základě podkladových dat v SW Gretl, 2022)

Příloha 11: Odebrání statisticky nevýznamných proměnných, Cochrane-Orcutt (2/2)

Prováděn interativní výpočet rho...

ITER	RHO	ESS
1	0,33594	2,79015
2	0,45898	2,70588
3	0,53574	2,66984
4	0,58630	2,65278
5	0,62143	2,64386
6	0,64713	2,63875
7	0,66673	2,63561
8	0,68218	2,63356
9	0,69465	2,63218
10	0,70489	2,63121
11	0,71340	2,63052
12	0,72055	2,63002
13	0,72658	2,62966
14	0,73170	2,62940
15	0,73605	2,62920
16	0,73975	2,62906
17	0,74292	2,62896
18	0,74561	2,62888
19	0,74792	2,62882
20	0,74989	2,62878
21	0,75157	2,62875
22	0,75300	2,62873
23	0,75423	2,62871
24	0,75527	2,62870
25	0,75617	2,62869
26	0,75693	2,62869
27	0,75758	2,62868
28	0,75814	2,62868
29	0,75861	2,62867
30	0,75901	2,62867
31	0,75936	2,62867
32	0,75965	2,62867
33	0,75990	2,62867
34	0,76012	2,62867
35	0,76030	2,62867
36	0,76045	2,62867
37	0,76059	2,62867
38	0,76070	2,62867
39	0,76079	2,62867
40	0,76088	2,62867

Zdroj: (Vlastní zpracování na základě podkladových dat v SW Gretl, 2022)

Příloha 12: Odhad Modelu 4, Možnost 1, OLS, HACC errors

Model 28: OLS, za použití pozorování 2013:04-2021:06 (T = 99)

Závisle proměnná: l_BTC_cena

HAC standardní chyby, šířka okénka 3 (Bartlettovo jádro)

	koeficient	směr. chyba	t-podíl	p-hodnota	
const	-9,93159	0,792356	-12,53	7,56e-022	***
l_M2_USA	3,34784	0,322743	10,37	2,64e-017	***
l_LTC_cena	0,612771	0,0366809	16,71	5,02e-030	***
l_BTC_cena_6	0,163492	0,0309806	5,277	8,26e-07	***

Střední hodnota závisle proměnné 0,602565
 Sm. odchylka závisle proměnné 1,735892
 Součet čtverců reziduí 4,775627
 Sm. chyba regrese 0,224209
 Koeficient determinace 0,983828
 Adjustovaný koeficient determinace 0,983317
 F(3, 95) 1060,475
 P-hodnota (F) 7,05e-73
 Logaritmus věrohodnosti 9,589012
 Akaikovo kritérium -11,17802
 Schwarzovo kritérium -0,797545
 Hannan-Quinnovo kritérium -6,978066
 rho (koeficient autokorelace) 0,688339
 Durbinovo h 7,199473

zde je poznámka o zkratkách statistik modelu

Whiteův test heteroskedasticity -

Nulová hypotéza: není zde heteroskedasticita

Testovací statistika: LM = 7,06091

s p-hodnotou = $P(\text{Chí-kvadrát}(9) > 7,06091) = 0,630778$

Test normality reziduí -

Nulová hypotéza: chyby jsou normálně rozdělené

Testovací statistika: Chí-kvadrát(2) = 3,6051

s p-hodnotou = 0,164878

LM test pro autokorelaci až do řádu 12 -

Nulová hypotéza: žádná autokorelace

Testovací statistika: LMF = 9,05286

s p-hodnotou = $P(F(12, 83) > 9,05286) = 7,72887e-11$

Zdroj: (Vlastní zpracování na základě podkladových dat v SW Gretl, 2022)

Příloha 13: Odhad Modelu 4, Možnost 2, Cochrane-Orcutt

Prováděn interaktivní výpočet rho...

ITER	RHO	ESS
1	0,68834	2,43445
2	0,71645	2,42975
3	0,72188	2,42957
4	0,72305	2,42956
5	0,72331	2,42956
6	0,72337	2,42956
7	0,72338	2,42956

Model 23: Cochrane-Orcutt, za použití pozorování 2013:05-2021:06 (T = 98)

Závisle proměnná: 1_BTC_cena

rho = 0,723382

	koeficient	směr. chyba	t-podíl	p-hodnota	
const	-10,4875	0,364090	-28,80	1,97e-048	***
1_M2_USA	3,61619	0,512920	7,050	2,97e-010	***
1_LTC_cena	0,557319	0,0374021	14,90	1,73e-026	***
1_BTC_cena_6	0,167100	0,0475810	3,512	0,0007	***

Statistika založená na rho-diferencovaných datech:

Součet čtverců reziduí	2,429560
Sm. chyba regrese	0,160768
Koeficient determinace	0,991551
Adjustovaný koeficient determinace	0,991282
F(3, 94)	322,4572
P-hodnota(F)	2,47e-49
rho (koeficient autokorelace)	0,090245
Durbinovo h	1,012764

zde je poznámka o zkratkách statistik modelu

Statistika založená na původních datech:

Střední hodnota závisle proměnné	0,631850
Sm. odchylka závisle proměnné	1,720059

zde je poznámka o zkratkách statistik modelu

Test normality reziduí -

Nulová hypotéza: chyby jsou normálně rozdělené

Testovací statistika: Chí-kvadrát(2) = 2,58149

s p-hodnotou = 0,275066

Zdroj: (Vlastní zpracování na základě podkladových dat v SW Gretl, 2022)

Příloha 14: Odhad Modelu 4, Možnost 3, Modifikace Just and Pope, 1.krok

Model 29: OLS, za použití pozorování 2013:04-2021:06 (T = 99)

Závisle proměnná: l_BTC_cena

	koeficient	směr. chyba	t-podíl	p-hodnota	
const	-9,93159	0,646299	-15,37	1,68e-027	***
l_M2_USA	3,34784	0,251436	13,31	1,91e-023	***
l_LTC_cena	0,612771	0,0246827	24,83	2,58e-043	***
l_BTC_cena_6	0,163492	0,0261016	6,264	1,09e-08	***
Střední hodnota závisle proměnné		0,602565			
Sm. odchylka závisle proměnné		1,735892			
Součet čtverců reziduí		4,775627			
Sm. chyba regrese		0,224209			
Koeficient determinace		0,983828			
Adjustovaný koeficient determinace		0,983317			
F(3, 95)		1926,471			
P-hodnota(F)		6,41e-85			
Logaritmus věrohodnosti		9,589012			
Akaikovo kritérium		-11,17802			
Schwarzovo kritérium		-0,797545			
Hannan-Quinnovo kritérium		-6,978066			
rho (koeficient autokorelace)		0,688339			
Durbinovo h		7,092245			
zde je poznámka o zkratkách statistik modelu					

Zdroj: (Vlastní zpracování na základě podkladových dat v SW Gretl, 2022)

Příloha 15: Odhad Modelu 4, Možnost 3, Modifikace Just and Pope, 3.krok

Model 30: OLS, za použití pozorování 2013:05-2021:06 (T = 98)
 Závisle proměnná: l_BTC_cena

	koeficient	směr. chyba	t-podíl	p-hodnota	
const	-9,79635	0,642835	-15,24	5,07e-027	***
l_M2_USA	3,28987	0,250245	13,15	6,28e-023	***
l_LTC_cena	0,608130	0,0244812	24,84	7,86e-043	***
sq_uhat29_1	0,533267	0,296416	1,799	0,0753	*
l_BTC_cena_6	0,175201	0,0265865	6,590	2,62e-09	***
Střední hodnota závisle proměnné		0,631850			
Sm. odchylka závisle proměnné		1,720059			
Součet čtverců reziduí		4,561199			
Sm. chyba regrese		0,221461			
Koeficient determinace		0,984106			
Adjustovaný koeficient determinace		0,983423			
F(4, 93)		1439,609			
P-hodnota (F)		1,06e-82			
Logaritmus věrohodnosti		11,24574			
Akaikovo kritérium		-12,49148			
Schwarzovo kritérium		0,433362			
Hannan-Quinnovo kritérium		-7,263646			
rho (koeficient autokorelace)		0,690867			
Durbinovo h		7,089174			
zde je poznámka o zkratkách statistik modelu					

Zdroj: (Vlastní zpracování na základě podkladových dat v SW Gretl, 2022)