

Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra ekonomiky



Diplomová práce

Ekonometrická analýza Bitcoinu

David Steiner

© 2022 ČZU v Praze

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. David Steiner

Hospodářská politika a správa
Podnikání a administrativa

Název práce

Ekonometrická analýza Bitcoinu

Název anglicky

Econometric analysis of Bitcoin

Cíle práce

Hlavním cílem práce je konstrukce modelu zaměřeného na simulaci hodnoty kryptoměny Bitcoin s následnou prognózou vývoje.

Díličí cíle:

- identifikace determinant působících na cenu Bitcoinu
- specifikace ekonometrického modelu
- kvantifikace, verifikace a aplikace modelu
- ex-ante prognóza hodnoty Bitcoinu

Metodika

Teoretická část diplomové práce bude založena na studiu odborné literatury zaměřené na kryptoměny s cílem vypracovat adekvátní literární rešerši zvoleného tématu.

V praktické části práce budou s využitím statistického aparátu identifikovány vhodné determinanty vývoje hodnoty Bitcoinu, přičemž v navazující části bude na základě dosažených poznatků koncipován vhodný ekonometrický model, který bude dále využit i pro kvantifikaci ex-post a ex-ante prognózy.

Doporučený rozsah práce

70 stran

Klíčová slova

peníze, kryptoměny, bitcoin, ekonometrický model, prognóza

Doporučené zdroje informací

- Grabowski, Mark. Cryptocurrencies : A Primer on Digital Money. Milton: Taylor & Francis Group, 2019. ISBN 978-04-295-1014-4.
- HUŠEK, R. – VYSOKÁ ŠKOLA EKONOMICKÁ V PRAZE. *Ekonometrická analýza*. Praha: Oeconomica, 2007. ISBN 978-80-245-1300-3.
- Chowdhury, Niaz. Inside Blockchain, Bitcoin, and Cryptocurrencies. Milton: Auerbach Publishers, Incorporated, 2019. ISBN 978-10-005-0770-6.
- LANSKY, Jan. Possible State Approaches to Cryptocurrencies. *Journal of Systems Integration*, 2018. ISSN 18042724.
- STROUKAL, D. – SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti : historie, ekonomie a technologie kryptoměn, stručná příručka pro úplné začátečníky*. Praha: Grada Publishing, 2018. ISBN 978-80-271-0742-1.

Předběžný termín obhajoby

2021/22 LS – PEF

Vedoucí práce

doc. Ing. Michal Malý, Ph.D.

Garantující pracoviště

Katedra ekonomiky

Elektronicky schváleno dne 15. 2. 2022

prof. Ing. Miroslav Svatoš, CSc.

Vedoucí katedry

Elektronicky schváleno dne 21. 2. 2022

doc. Ing. Tomáš Šubrt, Ph.D.

Děkan

V Praze dne 16. 03. 2022

Čestné prohlášení

Prohlašuji, že svou diplomovou práci *Ekonometrická analýza Bitcoinu* jsem vypracoval(a) 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 30. 3. 2022

Poděkování

Rád bych touto cestou poděkoval vedoucímu práce, panu doc. Ing. Michalovi Malému, Ph.D., za cenné rady, odborný dohled a věnovaný čas při psaní této diplomové práce.

Ekonometrická analýza Bitcoinu

Abstrakt

Předkládaná diplomová práce se zabývá ekonometrickou analýzou kryptoměny bitcoin. Metodická část práce obsahuje seznámení s principy ekonometrické analýzy, na kterých je založena vlastní část práce. V rámci teoretické části je představena problematika kryptoměn. Předmětem vlastní práce je konstrukce ekonometrického modelu, která sestává z několika fází. První fází je identifikace vhodných determinant, následuje sestavení ekonomického modelu, který je poté převeden na model ekonometrický. V další fázi následuje sběr a zpracování vstupních dat. Data jsou získána z volně dostupných zdrojů v podobě googlefinance, macrotrends a blockchain.com. Před samotným odhadem parametrů modelu jsou vstupní časové řady otestovány na stacionaritu a neexistenci perfektní multikolinearity mezi proměnnými. Odhad parametrů ekonometrického modelu je proveden s využitím softwaru gretl. Po odhadu parametrů je model podroben ekonomické, statistické a ekonometrické verifikaci. Poslední fází ekonometrické analýzy je aplikace modelu v podobě simulování scénářů, kdy je zkoumán 10% nárůst hodnoty regresorů na vysvětlovanou proměnou a odvození ex-ante prognózy. V rámci krátkodobé a střednědobé prognózy se modelu dařilo předpovídat budoucí hodnoty relativně dobře, nicméně čím byl prognostický horizont delší, začala se, vzhledem ke zmíněným okolnostem v závěru práce, prognóza se skutečnými hodnotami rozcházet.

Klíčová slova: peníze, kryptoměny, blockchain, bitcoin, ekonomie, determinanty, ekonometrie, ekonometrický model, lineární regresní model, prognóza

Econometric analysis of Bitcoin

Abstract

The presented thesis deals with the econometric analysis of the cryptocurrency bitcoin. The methodological part of the thesis includes an introduction to the principles of econometric analysis, on which the actual part of the thesis is based. The theoretical part introduces the issues of cryptocurrencies. The subject of the actual work is the construction of the econometric model, which consists of several stages. The first stage is the identification of appropriate determinants, followed by the construction of an economic model, which is then converted into an econometric model. The next stage is the collection and processing of input data. The data is obtained from freely available sources in the form of googlefinance, macrotrends and blockchain.com. Before the actual estimation of the model parameters, the input time series are tested for stationarity and the absence of perfect multicollinearity among the variables. The estimation of the econometric model parameters is performed using gretl software. After estimation of the parameters, the model is subjected to economic, statistical and econometric verification. The last stage of the econometric analysis is the application of the model in the form of scenario simulations, where a 10% increase in the value of the regressors on the explained variable is examined and an ex-ante forecast is derived. In the short- and medium-term forecasts, the model was able to predict future values relatively well; however, the longer the forecast horizon, the forecast began to diverge from the actual values, given the circumstances mentioned at the end of the paper.

Keywords: currencies, cryptocurrencies, blockchain, bitcoin, economics, determinants, econometrics, econometric model, linear regression model, prognosis

Obsah

1 Úvod.....	12
2 Cíl práce.....	13
3 Metodika	14
3.1 Konstrukce ekonometrického modelu.....	16
3.1.1 Ekonomická teorie a tvorba ekonomického modelu.....	16
3.1.2 Odhad parametrů ekonometrického modelu.....	18
3.1.3 Běžná metoda nejmenších čtverců.....	21
3.2 Verifikace ekonometrického modelu	24
3.2.1 Ekonomická verifikace	25
3.2.2 Statistická verifikace odhadnutých parametrů.....	25
3.2.3 Ekonometrická verifikace modelu.....	27
3.3 Aplikace ekonometrického modelu.....	36
3.3.1 Prognostika	36
4 Teoretická východiska	40
4.1 Historie peněz.....	40
4.1.1 Barterova směna	40
4.1.2 Mince	40
4.1.3 Bankovky	41
4.1.4 Fiat měny	42
4.2 Virtuální měny	42
4.2.1 Základní charakteristika.....	42
4.2.2 Historie virtuálních měn	44
4.3 Blockchain	46
4.3.1 Hashovací funkce.....	47
4.3.2 Mechanismus konsenzu	48
4.3.2.1 Proof of work.....	48
4.3.2.2 Alternativní algoritmy	49
4.4 Transakce	50
4.4.1 Životní cyklus transakce	52
4.4.2 Transakční poplatek.....	53
4.5 Těžba virtuálních měn.....	53
4.5.1 Proces těžby	53
4.5.2 Technologie těžby.....	56
4.5.3 Možnosti těžby.....	58
4.6 Bitcoin.....	61

4.6.1	Satoshi Nakamoto	61
4.6.2	Co je Bitcoin?.....	62
4.6.3	Regulace.....	64
4.7	Determinanty	66
4.7.1	Makroekonomické a finanční ukazatele	66
4.7.2	Technologické (blockchainové) ukazatele.....	67
5	Vlastní práce	69
5.1	Deklarace proměnných a očekávané vztahy	69
5.2	Formulace ekonomického a ekonometrického modelu.....	71
5.3	Odhad parametrů modelu	72
5.3.1	Stacionarita časových řad a multikolinearita	72
5.3.2	Odhad parametrů.....	74
5.3.3	Ekonomická verifikace a interpretace odhadnutých parametrů	76
5.3.4	Statistická verifikace	79
5.3.5	Ekonometrická verifikace	81
5.3.6	Aplikace modelu	83
6	Zhodnocení výsledků.....	95
7	Závěr.....	97
8	Seznam použitých zdrojů.....	101
	Přílohy	105

Seznam obrázků

Obrázek 1	Ekonometrie	15
Obrázek 2	Běžná metoda nejmenších čtverců	21
Obrázek 3	Testování autokorelace dle Durbin-Watsona	32
Obrázek 4	Transakce.....	52
Obrázek 5	Deskriptivní statistiky.....	71
Obrázek 6	Korelační matice.....	74
Obrázek 7	Odhad parametrů modelu	75
Obrázek 8	Test heteroskedasticity	81
Obrázek 9	Test autokorelace reziduí.....	82
Obrázek 10	Test normality reziduí.....	83
Obrázek 11	Prognóza ex-post	86
Obrázek 12	Prognóza ex-ante	92

Seznam tabulek

Tabulka 1	Deklarace proměnných	69
Tabulka 2	Stacionarita časových řad	73
Tabulka 3	Statistická verifikace odhadnutých parametrů	80

Tabulka 4 Odhadnuté hodnoty pro prognózu ex-ante	89
Tabulka 5 Prognóza ex-ante – absolutní hodnoty v USD.....	93
Tabulka 6 Porovnání – prognóza vs. skutečnost v USD.....	95

Seznam grafů

Graf 1 Hash rate Bitcoinové sítě na logaritmické křivce.....	58
Graf 2 Hashrate distribuce napříč největšími mining pooly k 23.9.2021	60
Graf 3 Prognóza ex-post	87
Graf 4 Vývoj a trend – miners revenue.....	89
Graf 5 Vývoj a trend – Ether	90
Graf 6 Vývoj a trend – hash rate.....	90
Graf 7 Prognóza ex-ante	91
Graf 8 Porovnání – prognóza vs. skutečnost	95

1 Úvod

Virtuální měny lze jednoznačně považovat za jeden z nejžhavějších trendů současnosti. Pravděpodobně na planetě Zemi neexistuje člověk s přístupem na internet, který by se nesetkal s pojmy jako kryptoměny či bitcoin. Kryptoměny ovšem nepředstavují jen potenciální měnový systém ať už blízké, či vzdálené budoucnosti. Za kryptoměnami především stojí vyspělá technologie s obrovským potenciálem a možnost vysokých a rychlých výdělků. Jak tomu ale na finančních trzích běžně bývá s vysokými zisky však kauzálně souvisejí i vysoké ztráty.

Vnímání kryptoměn z pohledu odborné i laické veřejnosti se velmi různí. Jedni považují kryptoměny za technologii budoucnosti a oproštění od nedůvěryhodných konvenčních měnových systémů, jiní zase vnímají kryptoměny pouze jako investiční instrument, do kterého mají možnost vložit své prostředky a přijít k potenciálnímu zhodnocení své investice. Samozřejmě existuje i velká skupina odpůrců kryptoměn, která vnímá kryptoměny jako jeden velký podvod.

Pravděpodobně v myslí každého jedince, který se rozhodne do kryptoměn investovat, probíhá myšlenka, zda existuje možnost predikovat vývoj hodnoty dané kryptoměny, a na základě toho určit svou vstupní či výstupní pozici dané investice. Na tuto otázku se pokusí nalézt odpověď tato diplomová práce.

2 Cíl práce

Hlavním cílem diplomové práce je konstrukce modelu zaměřeného na simulaci hodnoty kryptoměny Bitcoin s následnou prognózou vývoje.

Dílčí cíle diplomové práce:

- Identifikace determinant působících na hodnotu bitcoinu
- Specifikace ekonometrického modelu
- Kvantifikace, verifikace a aplikace modelu
- Ex-ante prognóza hodnoty bitcoinu

3 Metodika

Diplomová práce bude rozdělena na tři samostatné části. V první metodické části bude detailně prostudována a popsána ekonometrická analýza, na základě které pak bude zpracována vlastní část práce. V rámci kapitoly ekonometrické analýzy budou taktéž využity znalosti a poznatky získané během studia předmětu Ekonometrie vyučovaného na ČZU. Literární rešerše bude vycházet ze studia odborné, převážně zahraniční, literatury a vědeckých článků. První část literární rešerše bude zaměřena na historii prostředků směny a následného vývoje měn, jak je známe dnes. V další části literární rešerše bude detailně probrána problematika kryptoměn a představení principu a filozofie kryptoměny, kterou se tato diplomová práce zabývá – tedy Bitcoinu.

Vlastní část práce bude zaměřena na specifikaci, konstrukci a aplikaci ekonometrického modelu. K tomu bude využit veřejně dostupný SW Gretl, který je rovněž využíván při výuce předmětu Ekonometrie na České zemědělské univerzitě. Model bude zkonstruován s využitím volně dostupných vstupních dat. Převážně se bude jednat o data získána z googlefinance.com a blockchain.com.

V následujících kapitolách budou popsány avizované principy ekonometrické analýzy.

Autorka Hančlová ve své publikaci Ekonometrické modelování z roku 2012 cituje několik autorů a jejich pohled na definování ekonometrie:

„Metody ekonometrického výzkumu se zaměřují především na souvislosti ekonomické teorie a reálného měření prostřednictvím teorie a metod statistického odvozování jako společného pilíře.“ (Haavelmo, 1944)

„Ekonometrie je kvantitativní analýza reálných ekonomických jevů na základě současného teoretického vývoje a pozorování s využitím vhodných metod dedukce.“ (Samuelson, 1954)

„Ekonometrie je sociální věda, ve které jsou na ekonomické jevy aplikovány nástroje ekonomické teorie, matematiky a statistické inference.“ (Goldberger, 1964)

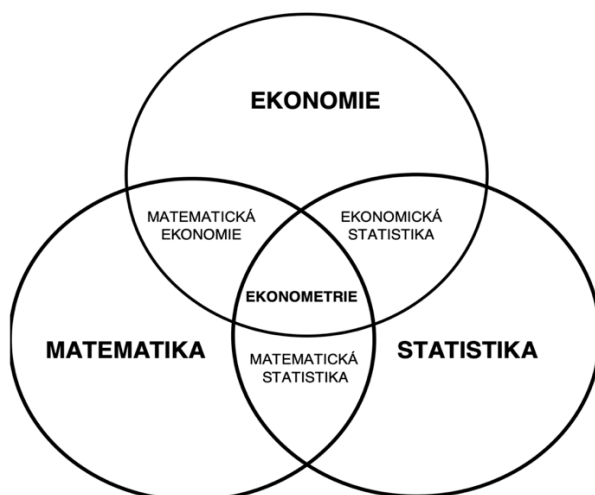
„*Ekonometrie je výsledkem pohledu ekonomie, který vychází z aplikace matematické statistiky na ekonomických datech jako empirické podpory modelů, které jsou konstruovány prostřednictvím matematické ekonomie a slouží k získání empirických výsledků.*“ (Gujarati, 2003)

„*Ekonometrická analýza vychází ze spojení ekonomické teorie, matematiky, statistiky a v poslední době stále více i z využívání informatiky za účelem vyhledávání, měření a empirického ověřování či testování především ekonomických, ale i jiných společenských jevů. Protože úkolem ekonometrie je mj. dát ekonomické teorii alespoň aproximativně empirických obsah, je předmět jejího zkoumání poměrně široký a zahrnuje tyto oblasti:*

- *Matematickou a statistickou formulaci ekonomické pomoci modelového přístupu (ekonometrické modelování).*
- *Rozvoj ekonometrické teorie spočívající v navrhování, popř. modifikaci odhadových a testovacích metod i výpočetních technik, vhodných pro ekonometrické modely a empirická data (ekonometrické metody).*
- *Aplikaci ekonometrických modelů a metod v jednotlivých oblastech ekonomické teorie a praxe, resp. výzkumu (aplikovaná ekonometrie).*“ (Hušek, 2007)

Z výše uvedených definic lze tedy ekonometrii jako vědní disciplínu vyjádřit následujícím diagramem:

Obrázek 1 Ekonometrie



(zdroj: Hančlová, 2013)

3.1 Konstrukce ekonometrického modelu

Konstrukce ekonometrického modelu obsahuje několik fází jejichž počet a struktura se napříč autory liší. Pro účely této diplomové práce budeme vycházet z postupu, jenž se vyučuje na České zemědělské univerzitě.

- 1) Ekonomická teorie
- 2) Tvorba ekonomického modelu
- 3) Tvorba ekonometrického modelu
- 4) Sběr, zpracování a analýza vstupních dat
- 5) Odhad parametrů ekonometrického modelu
- 6) Ekonomické ověření modelu
- 7) Statistické a ekonometrické ověření modelu
- 8) Aplikace ekonometrického modelu, nebo jeho zamítnutí

3.1.1 Ekonomická teorie a tvorba ekonomického modelu

V této fázi je důležité formulovat problém, který chceme řešit, vymezit teoretický rámec a klasifikovat ekonomické veličiny. (Cipra, 2013) (Hančlová, 2012)

Z nastudované ekonomické teorie nelze přímo kvantifikovat námi zvolený problém. Ekonomický model tedy slouží jako abstrakce reálného světa, a ačkoliv se nezdá jako důležitý prvek při konstrukci ekonometrického modelu, své opodstatnění má v tom, že pomocí nějž vyjádříme vztah mezi námi zvolenými proměnnými. (Hušek, 2007)

V ekonometrii máme dva základní druhy proměnných, a to endogenní a exogenní proměnné. Endogenní neboli vysvětlované proměnné, jsou takové proměnné jejichž hodnoty jsou generovány systémem (modelem), zatímco exogenní (vysvětlující) proměnné vysvětlují zvolené endogenní proměnné. (Hušek, 2007)

Nyní už se můžeme podívat na samotný ekonomický model. Ekonomický model lze vyjádřit následujícím vztahem:

$$y = fce(x_1; x_2; x_3) \quad (3.1)$$

kde:

yendogenní proměnná

x_1exogenní proměnná 1

x_2exogenní proměnná 2

x_3exogenní proměnná 3

Tvorba ekonometrického modelu:

Ekonometrický model oproti ekonomickému obsahuje navíc tři veličiny – náhodnou (stochastickou) složku, parametry a funkční formu.

Ekonometrický model s lineární funkční formou pak můžeme vyjádřit následujícím vztahem:

$$\beta y_t = \gamma_1 x_{1t} + \gamma_2 x_{2t} + \gamma_3 x_{3t} + u_t \quad (3.2)$$

kde:

βparametr beta

y_tendogenní proměnná v čase t

$\gamma_{1;2;3}$parametry gama 1; 2; 3

$x_{1;2;3}$exogenní proměnné 1; 2; 3 v čase t

u_tnáhodná (stochastická) složka v čase t

Stochastická složka představuje náhodné chyby, které vznikají při konstrukci ekonometrických modelů. Může se jednat například o vynechání či opomenutí podstatné vysvětlující proměnné, zvolení nevhodné funkční formy, chyby a nepřesnosti v datech a další. (Hušek, 2007)

Dynamizace modelu:

Modely nezohledňující časové hledisko jsou označovány jako modely statické. Zahrnutím časového hlediska do modelu pak vzniká model dynamický. Ekonomická data jsou ovšem často generována procesy, které mají dynamický charakter. Při specifikaci ekonometrického modelu je pak běžnou metodou zahrnutí zpožděných exogenních i endogenních proměnných do množiny vysvětlujících proměnných – tím nám vzniká model dynamický. (Hušek, 2007)

Dynamizace modelu lze docílit následujícími způsoby:

1. Zahrnutím zpožděných exogenních i endogenních proměnných
2. Převedením proměnných do postupných či relativních diferencí
3. Implikací časového vektoru jako samostatné exogenní proměnné
4. Zahrnutí „dummy“ proměnné

Dummy proměnná zpravidla nabývá hodnot od 0 do 1 a vyjadřuje okamžik, kdy nastane či nenastane určitý jev, který je svým způsobem významný pro specifikaci ekonometrického modelu, avšak nelze jej jiným způsobem kvantifikovat. Učebnicovým příkladem využití dummy proměnné může být sezónnost.

Dynamizujeme-li model hovoříme o exogenních proměnných jako o predeterminovaných. Predeterminované proměnné pak tedy představují všechny exogenní proměnné, zpožděné exogenní proměnné a zpožděné endogenní proměnné. Dynamický ekonometrický model lze pak vyjádřit následujícím vztahem:

$$\beta y_t = \beta_1 y_{t-1} + \gamma_1 x_{1t} + \gamma_2 x_{2t-2} + u_t \quad (3.3)$$

kde:

βparametr beta

y_tendogenní proměnná v čase t

y_{t-1}predeterminovaná endogenní proměnná zpožděná o 1 období

$\gamma_{1;2}$parametry gama 1; 2

x_{1t}predeterminovaná exogenní proměnná 1 v čase t

x_{2t-2}predeterminovaná exogenní proměnná 2 zpožděná o 2 období

u_tnáhodná (stochastická) složka v čase t

3.1.2 Odhad parametrů ekonometrického modelu

Pro účely této diplomové práce se budeme zabývat pouze odhadem parametrů jednorovnicového lineárního regresního modelu. K tomuto účelu nejlépe poslouží odhadová technika nazývaná jako BMNČ – Běžná metoda nejmenších čtverců. Její podstatou se budeme zabývat v následující kapitole.

Abychom pomocí BMNČ dosáhli nejlepších, nestranných a konzistentních odhadů parametrů, je prvně zapotřebí, aby model splňoval jisté předpoklady.

Specifikační předpoklady:

1. Neopomenutí podstatné vysvětlující proměnné
2. Vypuštění nepodstatných vysvětlujících proměnných
3. Neexistence perfektní multikolinearity
4. Volba správné funkční formy modelu
5. Stabilní odhadnuté parametry, časová invariantnost
6. Respektování simultánních vztahů mezi proměnnými

Předpoklady o stochastické složce:

1. Nulový průměr náhodné složky u - $E(u_t) = 0$
2. Homoskedasticita (stejnorozptylovost) – rozptyl náhodné složky by měl být konstantní a konečný - $var(u_t) = \sigma^2 < \infty$
3. Nepřítomnost autokorelace reziduí - $cov(u_t, u_{t-p}) = 0$
4. Normální rozdělení náhodné složky - $u_t \sim N(0, \sigma^2)$
5. Nepřítomnost kovariance mezi vysvětlujícími proměnnými a náhodnou složkou

Dalším předpokladem je stacionarita časových řad.

Stacionarita časových řad:

Stacionárnost časových řad je důležitým prvkem pro kvalitu ekonometrické analýzy i predikce. Před samotným odhadem modelu je tedy důležité otestovat, zda jsou vstupní data stacionární. (Hušek, 2007)

K objasnění stacionarity je nejprve potřeba se zaměřit na stochastický proces. *Stochastický proces je v čase uspořádaná řada náhodných veličin $\{X(s, t), s \in S, t \in T\}$, kde S je výběrový prostor a T je indexní řada. Pro každé $t \in T$ je $X(.,t)$ náhodná veličina definovaná na výběrovém prostoru S . Pro každé $s \in S$ je $X(s,.)$ realizace stochastického procesu na indexní řadě T , tj. uspořádaná řada čísel, z níž každé odpovídá jedné hodnotě indexní řady. Časovou řadu lze tedy chápat jako realizaci stochastického procesu.* (Arlt, Arltová, 2003)

Stochastický proces se tedy označuje jako stacionární, jsou-li charakteristiky jeho náhodných veličin v čase neměnné. (Arlt, Arltová, 2009)

K otestování, zda je časová řada stacionární lze použít například Dickey – Fuller test, který lze dle Huška (2007) vyjádřit následujícím vztahem pro specifikovanou rovnici:

$$Y_t = \gamma + \delta t + \alpha Y_{t-1} + \alpha_1 \Delta Y_{t-1} + u_t \quad (3.4)$$

kde:

$$u_t \sim N(0, \sigma^2)$$

$$\Delta Y_{t-1} = Y_{t-1} - Y_{t-2}$$

Prvním krokem je odečtení Y_{t-1} na obou stranách rovnice, čímž dostaneme rovnici:

$$Y_t - Y_{t-1} = \gamma + \delta t + (\alpha - 1)Y_{t-1} + \alpha_1 \Delta Y_{t-1} + u_t \quad (3.5)$$

Rovnici nazveme **neomezenou regresí** ve srovnání s **omezenou regresí**

$$Y_t - Y_{t-1} = \gamma + \alpha_1 \Delta Y_{t-1} + u_t \quad (3.6)$$

Rovnice s omezenou regresí je pak zvláštním případem, kdy $\delta = 0$ a $\alpha = 1$, tj. platí nulová hypotéza, že časová řada není stacionární.

Dalším krokem je odhad parametrů výše zmíněných rovnic z výběru o rozsahu T . Součástí je i spočítat odhadnuté standardní chyby jednotlivých parametrů a nevysvětlené součty čtverců.

Třetím krokem je spočtení příslušné F statistiky, která je vyjádřena následujícím vztahem:

$$F(0,1) = \frac{(NS\check{C}_O - NS\check{C}_N)/q}{NS\check{C}/(T-m)} \quad (3.7)$$

kde:

$NS\check{C}_O$nevysvětlený součet čtverců omezené regrese

$NS\check{C}_N$nevysvětlený součet čtverců neomezené regrese

qpočet omezení parametrů v omezené regresi

mpočet odhadnutých parametrů v neomezené regresi

Vyhodnocení testů spočívá v porovnání spočtené hodnoty statistiky s kritickými hodnotami. Nicméně podíl $F(0,1)$ nemá charakteristiku standardního F rozdělení, je potřeba použít kritické hodnoty uváděné samotnými autory testu - Dickeym a Fullerem.

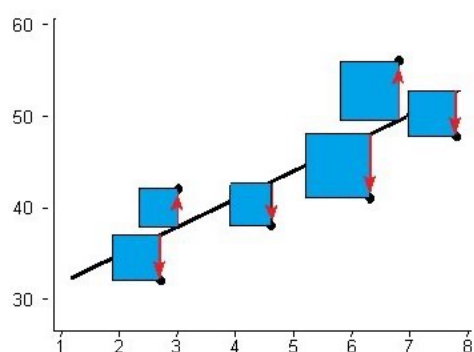
V případě, že časové řady nejsou stacionární, musíme původní časové řady transformovat. K transformaci můžeme dle Huška (2007) využít následující způsoby:

1. Zahrnutím časového vektoru jako samostatné vysvětlující proměnné do regresního modelu.
2. Nahrazením původních dat prvními nebo vyššími diferencemi.

3.1.3 Běžná metoda nejmenších čtverců

Podstatou běžné metody nejmenších čtverců je kritérium minimalizace součtů čtvercových odchylek napozorovaných hodnot od regresní přímky.

Obrázek 2 Běžná metoda nejmenších čtverců



(zdroj: <https://www.statisticshowto.com/probability-and-statistics/statistics-definitions/least-squares-regression-line/>)

Vertikální vzdálenost mezi každým bodem a regresní přímkou se nazývá odchylka. Podle kritéria metody BMNČ je nejlepší regresní přímka ta přímka, která minimalizuje součet čtverců těchto odchylek. Při regresi se odchylky čtvercují (hodnoty se umocňují na druhou mocninu), takže kladné a záporné odchylky se navzájem nevyruší, což je velmi důležitým aspektem BMNČ, neboť jediná přímka, která nám poskytne nejmenší součet čtvercových odchylek od přímky, je podle metody BMNČ nejlepší přímkou. (Wilson, 2013)

Minimalizační kritérium metody BMNČ lze vyjádřit následujícím vztahem:

$$\min \sum_{t=1}^n (y_t - \hat{y}_t)^2 \quad (3.8)$$

kde:

y_tskutečné hodnoty y

\hat{y}_tteoretické hodnoty y

Samotný odhad parametrů metodou BMNČ pak probíhá dle následujícího vztahu:

$$\gamma = (X^T \cdot X)^{-1} \cdot X^T \cdot y \quad (3.9)$$

kde:

γvektor odhadovaných parametrů

Xmatice X napozorovaných hodnot vysvětlujících proměnných

yvektor y napozorovaných hodnot vysvětlované proměnné

Koeficient determinace:

Po odhadnutí modelu lineární regrese následuje jeho verifikace, kterou se budeme zabývat v následujících kapitolách. Pro lepší orientaci a zjištění, zda je model kompatibilní s použitými daty nám poslouží takzvaný koeficient determinace, jenž je jedním ze statistických testů aplikovaných na ekonometrické modely. (Cipra, 2013)

Princip koeficientu determinace spočívá v rozložení úplného součtu čtverců pozorované a střední hodnoty y na část reziduální a vysvětlenou regresí, jenž se následně využívají ke zjištění vzájemných podílů. (Hančlová, 2013)

Nyní si objasníme základní pojmy a vztahy, které jsou nezbytné k vypočtení koeficientu determinace.

Úplný součet čtverců (Total Sum of Squares) představuje součet čtverců rozdílu pozorovaných hodnot endogenní proměnné od průměrné hodnoty a lze jej vyjádřit následujícím vztahem:

$$TSS = \sum (y_t - \bar{y})^2 \quad (3.10)$$

kde:

TSS Celkový součet čtverců

y_t napozorované hodnoty y

\bar{y} průměrná hodnota y

Úplný součet čtverců lze pak vyjádřit i pomocí dvou komponentů, jimiž jsou Residuální součet čtverců a Vysvětlený součet čtverců.

Residuální součet čtverců (Residual Sum of Squares) již známe, neboť na jeho principu je založeno minimalizační kritérium BMNČ. Lze tedy konstatovat, že čím je hodnota RSS menší, tím je odhadnutý model přijatelnější. (Cipra, 2013)

RSS lze vyjádřit následujícím vztahem:

$$RSS = \sum (y_t - \hat{y}_t)^2 \quad (3.11)$$

kde:

RSS Residuální součet čtverců

y_t napozorované hodnoty y

\hat{y}_t teoretické (odhadnuté) hodnoty y

Vysvětlený součet čtverců (Explained Sum of Squares) pak představuje vysvětlení regresní přímkou a lze jej vyjádřit pomocí následujícího vztahu:

$$ESS = \sum (\hat{y}_t - \bar{y})^2 \quad (3.12)$$

kde:

ESS Vysvětlený součet čtverců

\hat{y}_t teoretické (odhadnuté) hodnoty y

\bar{y} průměrná hodnota y

Pomocí aplikace Pythagorovy věty, lze pak Celkový součet čtverců vyjádřit následovně:

$$TSS = ESS + RSS \quad (3.13)$$

Nyní už se můžeme přesunout k samotnému koeficientu determinace, který je definován následujícím vztahem:

$$R^2 = \frac{ESS}{TSS} = 1 - \frac{RSS}{TSS} \quad (3.14)$$

„Koeficient determinace vyjadřuje stupeň vysvětlení celkové změny vysvětlované proměnné y regresí, tj. působením lineárního vztahu vysvětlující proměnné. Jedná se tedy o kritérium shody napozorovaných dat a odhadů prostřednictvím regresní přímky.“ (Hančlová, 2013)

Hodnota koeficientu determinace se pohybuje v intervalu od 0 do 1. V případě, že je jeho hodnota vysoká a blíží se 1, můžeme konstatovat, že odhadnutý model daným datům padne dobře – jinými slovy zvolené vysvětlující proměnné dobře reflektují změny vysvětlované proměnné. V opačném případě, kdy se hodnota R^2 blíží 0, není odhadnutý model vhodný pro vybraná data. (Cipra, 2013)

Ačkoliv koeficient determinace poskytuje na první pohled obecný přehled nad odhadnutým modelem, v praxi se ovšem častěji lze setkat s jeho modifikací. Hlavním nedostatkem obecného koeficientu determinace je, že pokud do modelu implikujeme další a další regresory (vysvětlující proměnné), jenž se zkoumaným jevem nemusí ani souviset, jeho hodnota se bude postupně zvyšovat. Z tohoto důvodu se využívá takzvaný korigovaný koeficient determinace, jehož hlavním přínosem je, že zahrnutí nevýznamných regresorů penalizuje. Korigovaný koeficient determinace pak vyjadřuje následující vztah:

$$\bar{R}^2 = 1 - (1 - R^2) \frac{n-1}{n-p} \quad (3.15)$$

kde:

R^2koeficient determinace

n.....počet pozorování

p.....počet odhadovaných parametrů

Pro korigovaný koeficient determinace platí taktéž, že jeho hodnoty náleží v intervalu od 0 do 1 a interpretuje se analogicky, jako obecný koeficient determinace.

3.2 Verifikace ekonometrického modelu

Po odhadu parametrů a ověření, zda je získaná regresní funkce kompatibilní s daty pomocí koeficientu determinace následuje fáze verifikace modelu, kdy se ověřují zejména

ekonomické, statistické a ekonometrické charakteristiky ekonometrického modelu před jeho aplikací.

3.2.1 Ekonomická verifikace

Fáze ekonomické verifikace spočívá v posouzení a ověření správnosti znamének (směru) a numerických hodnot (intenzity působení) odhadnutých parametrů. V případě, že jsou odhadnuté parametry v souladu s deklarovanou ekonomickou teorií čili parametry vysvětlujících proměnných působí na vysvětlovanou proměnnou správným směrem a přiměřenou intenzitou, lze ekonometrický model považovat za adekvátní, byť abstrahující, zobrazení zkoumaného ekonomického problému. V opačném případě je potřeba model specifikovat odlišným způsobem, případně zvolit jinou ekonomickou teorii. (Hušek, 2007)

3.2.2 Statistická verifikace odhadnutých parametrů

Statistická verifikace slouží k posouzení statistické reálnosti jednotlivých odhadnutých parametrů. Provádí se prostřednictvím statistických testů, pomocí nichž ověřujeme významnost výsledků kvantifikace. Nejpoužívanějšími metodami statistické verifikace jsou standardní chyby odhadnutých parametrů, koeficient vícenásobné determinace a t a F testy statistické významnosti odhadů. (Hušek, 2007)

Využívané statistické testy jsou založeny na předpokladu dvou hypotéz, kdy

- Nulová hypotéza označována jako H_0 představuje tvrzení, které má být testováno
- Alternativní hypotéza označována jako H_1 zahrnuje zbývající tvrzení (Cipra, 2013)

Základní principy testování hypotéz lze pak dle Hančlové, 2013 shrnout do tří fází:

- Formulace nulové a alternativní hypotézy
- Výpočet testovací statistiky
- Rozhodovací pravidlo o přijetí či zamítnutí nulové hypotézy pro stanovenou hladinu významnosti. Tato fáze představuje nalezení rozdělení testovací statistiky za předpokladu platnosti H_0 , volba hladiny významnosti (běžnou praxí jsou tři hladiny významnosti – 1 %, 5 % a 10 %), stanovení kritické hodnoty a porovnání vypočtené statistiky s kritickou hodnotou. Existují tři způsoby, jakými je možné provést

statistický test, a to pomocí kritického oboru testovací statistiky, pomocí intervalu spolehlivosti či případně pomocí p-hodnoty.

Statistická verifikace odhadnutých parametrů prostřednictvím t -testu dle metodiky vyučované na ČZU pak probíhá následovně:

Prvně je zapotřebí vypočítat matici pro ověření statistické významnosti parametrů (mimoходом známe již z odhadu parametrů pomocí BMNČ)

$$(X^T \cdot X)^{-1} \quad (3.16)$$

Následuje výpočet korigovaného reziduálního rozptylu, jenž získáme následujícím vztahem:

$$\bar{S}_u^2 = \frac{\sum_{t=1}^n (y_t - \hat{y}_t)^2}{n-p} \quad (3.17)$$

kde:

$(n - p)$počet stupňů volnosti

Poté vypočteme rozptyl odhadnutých parametrů vynásobením korigovaného reziduálního rozptylu a matice:

$$S_{ii} = \bar{S}_u^2 (X^T \cdot X)^{-1} \quad (3.18)$$

Rozptyl odhadnutých parametrů se pak nachází na hlavní diagonále výsledné matice.

Dalším krokem je výpočet standardní chyby odhadnutých parametrů:

$$S_{bi} = \sqrt{S_{ii}} \quad (3.19)$$

Předposledním krokem je výpočet testovacího kritéria pomocí následujícího vztahu:

$$t - \text{hodnota} = \frac{\text{hodnota parametru}}{\text{chyba odhadu}} = \frac{|y_{it}|}{S_{bi}} \quad (3.20)$$

Po vypočtení testovacího kritéria pro jednotlivé parametry následuje porovnání vypočtené t -hodnoty s tabulkovou hodnotou t -testu na zvolené hladině významnosti s ohledem na počet stupňů volnosti t_α .

Porovnání pak probíhá následovně:

Je-li $t > t_{\alpha}$, zamítá se nulová hypotéza o statistické nevýznamnosti parametru.

Je-li $t < t_{\alpha}$, přijímá se nulová hypotéza o statistické nevýznamnosti parametru na hladině významnosti α .

3.2.3 Ekonometrická verifikace modelu

Posledním, za to však nejobsáhlejším, krokem před samotnou aplikací ekonometrického modelu je ekonometrická verifikace modelu. V rámci ekonometrické verifikace ověřujeme, zda se v odhadnutém modelu nevyskytuje heteroskedasticita, multikolinearita, autokorelace reziduí a normalita reziduí.

Heteroskedasticita:

Heteroskedasticita se týká rozptylů rozdělení pravděpodobnosti reziduální složky. Slovo „hetero“ znamená různý, slovo „skedasticita“ pak odkazuje na rozptyl rozdělení. Heteroskedasticita tedy znamená, že rozptyl rozdělení reziduální složky se liší od pozorování k pozorování. (Westhoff, 2013)

O náhodné veličině se říká, že je heteroskedastická, jestliže její rozptyl může být pro různá pozorování různý. Naopak se říká, že je homoskedastická, pokud je její rozptyl konstantní a konečný pro všechna pozorování. Nejběžnějším rámcem, v němž se Heteroskedasticita v ekonometrii studuje, je obecný lineární model. (Baltagi, 2001)

Předpoklad konečného a konstantního rozptylu náhodné složky je jedním ze specifikačních předpokladů ekonometrického modelu odhadovaného běžnou metodou nejmenších čtverců. Z toho plyne, že homoskedasticita je v odhadnutém modelu žádoucí, heteroskedasticita pak nikoliv.

Příčiny výskytu heteroskedasticity v modelu jsou dle Woolridge (2008) následující:

- Průřezové regresní analýzy nehomogenních jednotek, kdy se mezi průřezovými jednotkami vyskytují značně velké rozdíly.
- Odlehlá pozorování.

- Chybná specifikace regresního modelu, a to zejména ve formě špatné funkční formy a vynechání podstatné vysvětlující proměnné.
- Výskyt chyby měření dat.
- Nevhodná transformace dat nebo neadekvátní způsob nahrazení chybějících hodnot.
- Nevhodné použití kombinace průřezové a časové analýzy v panelových modelech.

Výskyt heteroskedasticity v reziduální složce odhadnutého modelu má za následek negativní dopad na odhady regresních parametrů a vlastnosti odhadových funkcí. V případě malých výběrových souborů jsou odhadnuté parametry lineární a nevychýlené, rozptyl je však zkreslený a není vydatný, což má za následek nespolehlivost využití konfidenčních intervalů při testování hypotéz. Pro velké výběrové soubory pak v případě výskytu heteroskedasticity platí, že odhady regresních parametrů jsou asymptoticky nestranné a konzistentní, nejsou však asymptoticky vydatné. (Hančlová, 2013)

Detekovat heteroskedasticitu lze například prostřednictvím Whiteova, případně Breusch-Paganova testu. Whiteův test vychází z možnosti získat konzistentní odhad kovarianční matice pomocí BMNČ i v případě nesplnění požadavku homoskedasticity. Nicméně vyžaduje minimální počet 30 pozorování a správnou specifikaci modelu. White v tomto testu nahrazuje požadavek konečného a konstantního rozptylu slabším požadavkem, že čtverce reziduí nejsou zkorelovány s žádným z regresorů x_1 , s jeho čtvercem x_1^2 a ani s párovými součiny regresorů x_1x_2 . (Hušek, 2007)

Na modelové situaci si ukážeme, jak dle Huška (2007) Whiteův test probíhá. Představme si lineární regresní model o 3 vysvětlujících proměnných, kdy jedna proměnná (x_1) představuje konstantu. Nejprve je potřeba si model převést do tzv. pomocné regrese čtverců reziduí. Whiteova testovací pomocná regrese čtverců reziduí e_t^2 má následující tvar:

$$e_t^2 = \alpha_1 + \alpha_2 x_{2t} + \alpha_3 x_{3t} + \alpha_4 x_{2t}^2 + \alpha_5 x_{3t}^2 + \alpha_6 x_{2t} x_{3t} + v_i \quad (3.21)$$

Za normální situace by v pomocné regresi mělo být 9 regresorů. Pracujeme-li však s konstantou platí, že $1^2 = 1$ a párové součiny $1x_{2t}$, $1x_{3t}$, jsou shodné s x_{2t} , x_{3t} – tím pádem se tyto tři proměnné opakují a jsou zbytečné.

O náhodné složce v_t se v pomocné regresi předpokládá, že je nezávislá na náhodné složce u_t , přičemž $v_t \sim N(0, \sigma^2)$.

Testovací LM statistika je pak vyjádřena následujícím vztahem:

$$LM = nR_e^2 \quad (3.22)$$

Kde R_e^2 představuje koeficient vícenásobné determinace získaný z pomocné regrese.

Testovací statistika má v případě nulové hypotézy homoskedasticity asymptotické rozdělení $\chi^2(p)$, kde p představuje počet stupňů volnosti, který je dán počtem vysvětlujících proměnných v pomocné regresi zmenšených o jednotku.

Samotný test heteroskedasticity pak probíhá tak, že na zvolené hladině významnosti např. 5 % porovnáváme kritickou hodnotu z tabulky $\chi^2(p)$ rozdělení se spočtenou hodnotou R_e^2 . Nulovou hypotézu homoskedasticity pak akceptujeme tehdy, platí-li $\chi_{0,05}^2(p) > nR_e^2$. V opačném případě nulovou hypotézu zamítáme a můžeme konstatovat, že model obsahuje heteroskedasticitu. Přijetí nulové hypotézy tedy znamená, že všechny parametry v pomocné regresi jsou rovny 0, čili statisticky nevýznamné. V případě, že je alespoň jeden parametr nenulový se tento parametr systematicky mění v závislosti na některém regresoru.

Autokorelace reziduí:

Autokorelace (někdy též sériová korelace) reziduí znamená nastává, když hodnota reziduální složky jednoho pozorování umožňuje předpovědět hodnotu reziduální složky dalšího pozorování. Pokud k tomu dojde, je reziduum jednoho pozorování korelován s reziduem dalšího pozorování. (Westhoff, 2013)

K autokorelaci reziduí dochází často v případě, kdy je model kvantifikovaný pomocí dat ve tvaru časových řad. Nicméně korelovanost v čase u veličin s časovým uspořádáním je

poměrně obvyklá. Předpona „auto“ znamená, že se tato korelovanost odehrává v rámci jedné časové řady. Nicméně autokorelace reziduí se může vyskytovat i při použití průřezových dat. Obecně však platí, že výskyt autokorelace je méně pravděpodobný, čím delší jsou intervaly pozorování – z toho plyne, že s autokorelací se častěji setkáme u analýzy dat v měsíčních či čtvrtletních intervalech než v případě ročních časových řad. (Cipra, 2013)(Hušek, 2007)

Příčiny výskytu autokorelace reziduí jsou dle Cipry (2013) a Huška (2007) následující:

- Opomenutí regresorů, jejichž časové řady vykazují autokorelovanost a ta se tím pádem přesune do reziduální složky.
- Nedostatečně specifikovaná dynamika modelu – mezi regresory měly být zařazeny zpožděné hodnoty vysvětlované/vysvětlujících proměnné/proměnných.
- Přirozená značná setrvačnost některých ekonomických veličin – pozorování za několik po sobě jdoucích období nejsou nezávislá, nýbrž sériově zkorelována. Může se jednat například o HDP, disponibilní důchod, cenové indexy, investice, nezaměstnanost a další. V takovém případě jsou hodnoty v jednom období více či méně determinovány svými hodnotami v předcházejících obdobích.
- Hrubá aproximace nelineární funkční závislosti lineárním vztahem. V takovém případě se chybná specifikace analytické formy modelu stává součástí reziduální složky, která pak vykazuje autokorelaci.
- Odhad modelu z upravených dat. Pod upravenými daty si můžeme představit data, které obsahují zprůměrované, vyrovnané, interpolované či extrapolované údaje. V takovém případě mohou úpravy dat systematicky ovlivňovat náhodné složky a způsobovat tak jejich autokorelaci.

Výskyt autokorelace má v odhadnutém modelu nepříznivé důsledky obdobně jako v případě heteroskedasticity. Odhadnuté parametry jsou sice nestranné a konzistentní, nemají však minimální rozptyl a nejsou asymptoticky vydatné. V takovém případě jsou odhadnuté rozptyly a standardní chyby odhadnutých parametrů vychýlené a nemůžeme se tím pádem spolehnout na spočtené intervaly spolehlivosti, ani na běžné testovací postupy. Dojde-li k pozitivní autokorelaci reziduí, odhady rozptylu reziduí a standardní chyby odhadnutých parametrů jsou podhodnoceny – vychýlené směrem k nule, což má za následek nadhodnocení koeficientu determinace R^2 . (Hančlová, 2013)(Hušek, 2007)

Dle Hančlové (2013) je nejjednodušším typem autokorelace modelování reziduální složky jako autoregresního modelu prvního řádu (AR(1)) dle následujícího vztahu:

$$u_t = \rho u_{t-1} + \varepsilon_t \quad (3.23)$$

kde u_t představuje náhodnou složku, která je závislá na své zpožděné hodnotě o jedno období u_{t-1} , ρ je regresní parametr jehož hodnota leží v intervalu $(-1;1)$, ε_t je takzvaný *bílý šum* a vyjadřuje časovou řadu navzájem nekorelovaných veličin s nulovou střední hodnotou a konstantním rozptylem. Důležitou roli zde hraje znaménko regresního parametru ρ pro nějž platí, že:

- a) $\rho > -1$ se jedná o negativní autokorelaci
- b) $\rho = 0$ se nejedná o autokorelaci
- c) $\rho < 1$ se jedná o pozitivní autokorelaci

Z autoregresního modelu pak dle Hančlové (2013) vychází samotné testování autokorelace reziduí prvního řádu prostřednictvím Durbin-Watsonova testu autokorelace. Samotný proces testu je pak následující:

Formulace hypotéz:

$H_0: \rho = 0$ (autokorelace prvního řádu není významná)

$H_1: \rho \neq 0$ (autokorelace prvního řádu je významná a dle znaménka ρ se jedná o pozitivní/negativní autokorelaci)

Výpočet Durbin-Watsonovi testovací statistiky, která se chová podle d rozdělení:

$$DW = \frac{\sum_{t=2}^n (\hat{u}_t - \hat{u}_{t-1})^2}{\sum_{t=1}^n \hat{u}_t^2} \sim d_{n,k} \quad (3.24)$$

Durbin-Watsonova statistika se dá rovněž přibližně vyjádřit pomocí odhadnutého regresního parametru z autoregresního modelu:

$$DW \doteq 2(1 - \hat{\rho}) \quad (3.25)$$

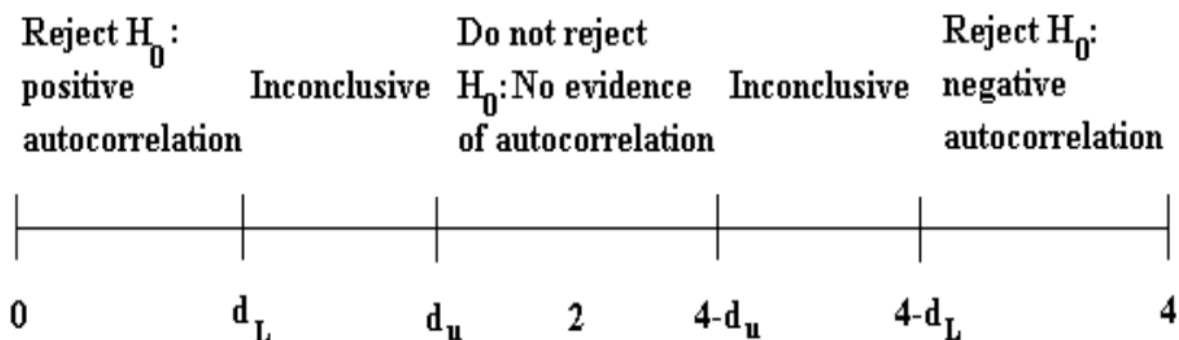
V takovém případě platí, že:

- a) $\hat{\rho} = -1 \Rightarrow DW = 4$
- b) $\hat{\rho} = +1 \Rightarrow DW = 0$

$$c) \hat{\rho} = 0 \Rightarrow DW = 2$$

Následuje rozhodnutí o zamítnutí či přijetí nulové hypotézy H_0 na zvolené hladině významnosti α . Hodnota DW statistiky se chová podle nestandardního d rozdělení a pohybuje se v intervalu $<0;4>$ a je symetrická se střední hodnotou. Za předpokladu bílého šumu náhodné složky u_t má d -rozdělení dvě kritické hodnoty d_L a d_U pro daný počet pozorování n a počet vysvětlujících proměnných $k-1$ a při dané významnosti α . Tyto kritické hodnoty je možné použít pouze v případě, že regresní model obsahuje úroňovou konstantu, reziduální složka má normální rozdělení a v modelu se nevyskytují zpožděné vysvětlované proměnné. Přijetí či zamítnutí nulové hypotézy se pak řídí dle následujícího obrázku:

Obrázek 3 Testování autokorelace dle Durbin-Watsona



(zdroj:<https://itfeature.com/time-series-analysis-and-forecasting/autocorrelation/durbin-watson-test>)

Závěry testu jsou pak následující:

- Jestliže $DW < d_L$ nebo $DW > 4 - d_L$ zamítáme nulovou hypotézu H_0 o nepřítomnosti autokorelace reziduí prvního řádu.
- Pokud DW leží v jednom z intervalů $< d_L; d_U >$ / $< 4 - d_U; 4 - d_L >$, je test neprůkazný a nemůžeme tedy rozhodnout, zda se v modelu vyskytuje autokorelace reziduí prvního řádu.
- Nulovou hypotézu o nepřítomnosti autokorelace reziduí pak přijímáme v případě, že DW leží v intervalu $< d_U; 4 - d_U >$.

Pro testy autokorelace vyšších řádů je zapotřebí použít jinou formu testu. Nabízí se například Breusch-Godfreyův test autokorelace reziduí, který je hojně využíván i napříč

ekonometrickými softwary. Dle Cipry (2013) tento test při modelování reziduální složky u_t vychází z autoregresního modelu AR(p) vyššího řádu $p \geq 1$ jenž vypadá následovně:

$$u_t = \rho_1 u_{t-1} + \rho_2 u_{t-2} + \rho_p u_{t-p} + \varepsilon_t \quad (3.26)$$

Následuje průběh samotného testu, na jehož počátku je formulace hypotéz:

$$H_1: \rho_1 = \rho_2 = \rho_p = 0$$

$$H_1: \rho_1 \neq 0 \text{ nebo } \rho_2 \neq 0 \text{ nebo } \rho_p \neq 0$$

Poté Breusch-Godfrey test odhadne následující pomocný model:

$$\hat{u}_t = \gamma_1 + \gamma_2 x_{2t} + \gamma_k x_{kt} + \rho_1 \hat{u}_{t-1} + \rho_2 \hat{u}_{t-2} + \rho_p \hat{u}_{t-p} + \varepsilon_t \quad (3.27)$$

Dalším krokem je aplikace χ^2 testu na koeficient determinace R^2 získaného z pomocného modelu. Porovnání příslušného kritického oboru proti alternativě na hladině významnosti α je pak následující:

$$(n - p) \cdot R^2 \geq \chi_{1-\alpha}^2(p) \quad (3.28)$$

Vyhodnocení testu dle Hančlové (2013) probíhá tak, že pokud $(n - p) \cdot R^2 > \chi_{1-\alpha}^2(p)$, zamítáme nulovou hypotézu o neautokorelovanosti reziduální složky až do řádu p na hladině významnosti α . Stanovení řádu p bývá problematickým prvkem tohoto testu, doporučený postup je zvolit p v případě kvartálních dat 4, u měsíčních časových řad pak 12.

Multikolinearita:

Předposledním předpokladem pro odhad parametrů ekonometrického modelu je neexistence multikolinearity. Ten spočívá v tom, že hodnota matice X je rovna počtu vysvětlujících proměnných (k) a lze jej dle Hančlové (2013) vyjádřit následujícím vztahem:

$$h(X) = k \quad (3.29)$$

Z pohledu statistiky představuje multikolinearita vysokou vzájemnou korelovanost regresorů. Nejjednodušeji lze tedy multikolinearitu detekovat pomocí vysoké hodnoty (kladné či záporné) korelačního koeficientu mezi dvěma regresory. Obecně se za vysokou hodnotu považuje 0,8 popř. 0,9. Je nutné podotknout, že vysoká hodnota párového korelačního koeficientu mezi vysvětlovanou a vysvětlující proměnnou se za žádnou

multikolinearitu nepovažuje, ba naopak, jedná se o žádoucí jev při odhadu ekonometrických modelů. (Cipra, 2013)

Příčiny multikolinearity dle Huška (2007) jsou následující:

- Nejčastější příčinou multikolinearity je samotná tendence časových řad některých ukazatelů vyvíjet se stejným směrem, přičemž vykazují i obdobné přírůstky. Velmi často se jedná o makroúdaje jakými jsou HDP, spotřeba, investice, důchody, úspory atd.
- Zahrnutí mezi regresory zpožděné hodnoty jedné z vysvětlovaných/vysvětlujících proměnných.
- Multikolinearita se také může objevit v případě použití dummy proměnné, která je pak následně silně korelována s úrovnovou konstantou.

Multikolinearita má negativní důsledky na odhadnuté parametry, které jsou dle Hančlové (2013) následující:

- Odhadnuté parametry zůstávají nezkreslené a vydatné, mají však velký rozptyl a kovarianci, což negativně ovlivňuje testování hypotéz o statistické významnosti parametrů.
- Nemožnost oddělit vliv korelovaných vysvětlujících proměnných na vysvětlovanou proměnnou, což vede k problémům při interpretaci regresních parametrů.
- Vysoké rozptyly parametrů mohou znamenat nízké hodnoty t-statistiky, což následně vede k chybenému vyhodnocení samotného testu o statistické významnosti parametrů. Pokud se jedná o více regresních parametrů, bývá koeficient determinace velmi vysoký i přesto, že většina regresních parametrů jsou statisticky nevýznamné.
- Odhady parametrů a jejich rozptyly jsou citlivé na malé změny v podkladových datech (např. rozšíření výběrového souboru o další pozorování).

Dle Huška (2007) lze multikolinearitu detekovat například prostřednictvím Farrar – Glauberova testu, který je založený na vytvoření korelační matice pomocí vztahu kde X představuje matici normovaných vektorů vysvětlující proměnné:

$$X^T X. \quad (3.30)$$

Normování vektorů se pak řídí následujícím vztahem:

$$\frac{(x_{it} - \bar{x}_i)}{\left(\frac{s_{xi}}{\sqrt{n}}\right)} \quad (3.31)$$

kde:

x_{it} hodnota i-té vysvětlující proměnné v čase t

\bar{x}_i průměr i-té vysvětlující proměnné

s_{xi} směrodatná odchylka i-té vysvětlující proměnné

n..... počet pozorování

Normalita reziduí:

Posledním předpokladem, který v rámci ekonometrické verifikace ověřujeme před samotnou aplikací ekonometrického modelu, je normální rozdělení náhodné složky. Dle Hančlové (2013) se předpoklad o normálním rozdělení náhodné složky využívá při specifikaci pravděpodobnostního rozdělení reziduální složky a následném testování hypotéz v modelu i konstrukci konfidenčních intervalů.

Pro normální rozdělení je charakteristické, že je určeno střední hodnotou a rozptylem. Nicméně je také charakteristické šikmostí a špičatostí. (Cipra, 2013)

Testovat normální rozdělení náhodné složky lze dvěma způsoby. Prvním z nich je grafická analýza, kdy se porovnává histogram rozdělení četností reziduí s Gaussovou teoretickou křivkou. Druhým jsou pak neparametrické testy, kam patří například χ^2 test dobré shody, Kolmogorov – Smirnov test a Jarque – Bera test. (Hančlová, 2013)

Právě poslední zmíněný test je hojně využíván v ekonometrické praxi napříč různými softwary. Dle Cipry (2013) test pracuje s testovou statistikou a probíhá dle následujícího vztahu:

$$W = T \left(\frac{\hat{\gamma}_1^2}{6} + \frac{\hat{\gamma}_2^2}{24} \right) \quad (3.33)$$

kde:

γ_1 koeficient šikmosti

γ_2 koeficient špičatosti

Testovací statistika je založena na koeficientech šikmosti a špičatosti v případě normálního rozdělení. Platí-li nulová hypotéza o normálním rozdělení náhodné složky, má tato statistika asymptoticky rozdělení $\chi^2(2)$ (chí-kvadrát se dvěma stupni volnosti). Vyhodnocení testu pak spočívá v porovnání výsledné statistiky s kritickým oborem na hladině významnosti α a řídí se následujícím vztahem:

$$W \geq \chi_{1-\alpha}^2(2) \quad (3.34)$$

Vyjde-li výsledná testovací statistika vyšší než $\chi_{1-\alpha}^2(2)$, zamítáme nulovou hypotézu o normálním rozdělení náhodné složky. (Hančlová, 2013)

3.3 Aplikace ekonometrického modelu

Pokud odhadnutý regresní model splňuje specifikační předpoklady a prošel všemi testy, můžeme přejít k aplikaci ekonometrického modelu, což je poslední fázi ekonometrické analýzy. Ekonometrické modely se uplatňují zejména v následujících oblastech:

- Simulace efektů
- Strukturální analýza
- Prognostika

V rámci prvních dvou zmíněných oblastí je oblíbenou metodou využití koeficientů elasticity. Koeficienty elasticity se udávají v procentech, tím pádem vyjadřují působení zvolených regresorů na vysvětlovanou proměnnou relativně. Z toho plyne, že za pomoci koeficientů elasticity lze srovnávat působení jednotlivých regresorů na vysvětlovanou proměnnou mezi sebou. Výpočet koeficientu elasticity probíhá dle následujícího vztahu:

$$E = \frac{\partial y}{\partial x_i} \frac{x_i}{\hat{y}} \quad (3.35)$$

kde:

y.....pravá strana regresní rovnice

x_ii-tá vysvětlující proměnná

\hat{y}teoretická hodnota y

3.3.1 Prognostika

Pod pojmem prognóza (předpověď, predikce) si můžeme z pohledu ekonometrie představit situaci, kdy se odhadnutý ekonometrický model využívá pro extrapolaci modelu do

budoucná. Nicméně existuje i možnost, kdy užití modelu spočívá v extrapolaci do minulosti, tedy do období, před začátkem pozorování. V takovém případě hovoříme o retropolaci. (Hušek, 2007)

Zpravidla rozlišujeme dvě možnosti předpovědi, a to ex-post a ex-ante. Ex-post prognóza představuje situaci, kdy s jistotou známe všechny hodnoty všech vysvětlujících proměnných pro predikované období. Ex-ante prognóza pak představuje podmíněnou předpověď, podmíněnou proto, protože s jistotou neznáme hodnoty vysvětlujících proměnných – ty jsou pak předmětem odhadu. (Hančlová, 2013)

Prognózy pak dále klasifikujeme na tzv. bodovou prognózu a intervalovou prognózu. V případě bodové prognózy se jedná o odhad jedné konkrétní hodnoty vybrané proměnné. Intervalová prognóza pak představuje období intervalu spolehlivosti odhadu, který obsahuje predikovanou hodnotu s určitou mírou pravděpodobnosti. (Hušek, 2007)

Prognostický horizont:

Prognózy můžeme také členit dle délky prognostického horizontu. Klasifikace je pak následující:

- a) Krátkodobé prognózy (1 – 3 období)
- b) Střednědobé prognózy (3 – 5 období)
- c) Dlouhodobé prognózy (5 a více období)

Doporučuje se i maximální délka prognostického horizontu, ten by neměl přesáhnout jednu třetinu délky podkladových údajů.

Prognóza ex-post:

V ekonometrické praxi se prognózy ex-post tvoří stejně často, jako samotné ex-ante prognózy. Hlavním přínosem ex-post prognózy je ověření prognostických vlastností odhadnutého modelu. Prognóza ex-post probíhá tak, že do odhadnutého modelu dosadíme za jednotlivé regresory jejich skutečné hodnoty z námi zvoleného období a tím získáme teoretickou hodnotu endogenní proměnné y . Pokud se výsledná teoretická hodnota y blíží

skutečné hodnotě y , můžeme předpokládat, že model bude správně fungovat i v případě ex-ante prognózy.

Bodová prognóza ex-ante:

K provedení ex-ante prognózy musíme nejprve odhadnout (extrapolovat) hodnoty regresorů pro následující období. Regresory můžeme odhadnout například pomocí trendových funkcí, kde regresory figurují v pozici vysvětlované proměnné. Při odhadu trendových funkcí můžeme použít již známou metodu nejmenších čtverců. Odhadnutou lineární trendovou funkci můžeme dle Cipry (2007) vyjádřit následujícím vztahem:

$$\hat{x}_{it} = \beta_1 + \beta_2 t \quad (3.36)$$

kde:

\hat{x}_{it}teoretická hodnota regresoru

β_1neznámý parametr 1 (konstanta)

β_2neznámý parametr 2

tčasový vektor

Tímto způsobem odhadneme hodnoty pro všechny regresory. Jakmile odhadneme budoucí hodnoty regresorů, můžeme zjištěné hodnoty dosadit do regresní funkce našeho ekonometrického modelu, provedeme součin jednotlivých parametrů s odhadnutými hodnotami regresorů a zjistíme teoretickou hodnotu naší vysvětlující proměnné, která je předmětem predikce. Je však dobré podotknout, že pokud se v modelu vyskytují zpožděné predeterminované proměnné a pohybujeme se v prognostickém horizontu, pro nějž hodnoty těchto proměnných existují, není nutné hodnoty těchto proměnných odhadovat.

Intervalová prognóza ex-ante:

Intervalová prognóza vysvětlované proměnné představuje stanovení intervalu spolehlivosti pro danou hladinu významnosti, ve kterém se bude pravděpodobně predikovaná hodnota nacházet. Dle Hančlové (2012) lze získat intervalovou prognózu následujícím způsobem, který si představíme na modelové situaci pro rovnici $y_0 = \beta_1 + \beta_2 x_0 + u_0$. Prvně je

zapotřebí stanovit chybu predikce a odhadnout variabilitu a směrodatnou odchylku, kterou následně využijeme ke konstrukci konfidenčního intervalu. Chybu predikce lze vyjádřit následujícím vztahem:

$$y_0 - \hat{y}_0 = \beta_1 + \beta_2 x_0 + u_0 - (\hat{\beta}_1 + \hat{\beta}_2 x_0) = (\hat{\beta}_1 - \beta_1) + (\hat{\beta}_2 - \beta_2) \cdot x_0 + u_0 \quad (3.37)$$

Střední hodnota chyby predikce je nulová, což znázorňuje následující rovnice:

$$E(y_0 - \hat{y}_0) = E(\hat{\beta}_1 - \beta_1) + E(\hat{\beta}_2 - \beta_2) \cdot x_0 + E(u_0) = 0 \quad (3.38)$$

Za předpokladu, že $\hat{\beta}_1$ a $\hat{\beta}_2$ jsou nestranné odhady regresních parametrů, x_0 je fixní číslo a průměr náhodné složky u_0 je nulový, můžeme odvozením rovnice získat variabilitu chyby predikce. Variabilitu chyby predikce lze vyjádřit následujícím způsobem:

$$\text{var}[y_0 - \hat{y}_0] = \sigma^2 \cdot \left[1 + \frac{1}{n} + \frac{(x_0 - \bar{x})^2}{\sum_{t=1}^n (x_t - \bar{x})^2}\right] \quad (3.39)$$

Předposledním krokem je výpočet t statistiky:

$$t = \frac{y_0 - \hat{y}_0}{\sqrt{\text{var}(y_0 - \hat{y}_0)}} \quad (3.40)$$

Nyní už můžeme sestavit $(1-\alpha)\%$ interval spolehlivosti pro individuální predikovanou hodnotu y_0 :

$$\hat{y}_0 - t_{1-\alpha} \cdot \sqrt{\text{var}(y_0 - \hat{y}_0)} \leq \frac{y_0}{x_0} \leq \hat{y}_0 + t_{1-\alpha} \cdot \sqrt{\text{var}(y_0 - \hat{y}_0)} \quad (3.41)$$

4 Teoretická východiska

4.1 Historie peněz

4.1.1 Barterova směna

Dle historiků byly peníze (ať už v jakékoliv formě) využívány již před 3200 lety. Barterova směna představuje systém, kdy docházelo k výměně jednoho druhu zboží za jiný. Koncept barterovy směny spočívá v tom, že jedna osoba musí mít větší množství jednoho druhu zboží, než potřebuje, a na druhé straně, v ten stejný okamžik, musí být druhá osoba, která má stejné dilema s jiným druhem zboží. Je tedy patrné, že obchodování muselo být velmi obtížné, neboť lidé museli najít ideálního obchodního partnera, který byl ochoten přijmout jimi nabízené zboží za svoje. Další překážkou v barterově směně představovalo množství zboží, které bylo prostředkem směny za jiné. (Naghshpour, 2013)

Tyto překážky vedly ke vzniku takzvaných komoditních peněz. Komoditní peníze představovaly zboží, které se stalo všeobecně přijímaným a výrazně tak usnadnilo proces směny. Jako komoditní peníze se využíval například med, obilí, kožešiny, plátno, dobytek. (Jílek, 2013)

4.1.2 Mince

V případě mincovního systému můžeme již hovořit o vzniku plnohodnotných peněz. Mince byly zpočátku raženy ze vzácných kovů – zlata a stříbra. Přirozené vlastnosti těchto kovů přímo vybízely k tomuto využití. Zlato a stříbro jsou snadno dělitelné, dělením neztrácejí svou hodnotu, dají se znovu slévat a vytvořit tak nové mince a nekazí se. Mince se dostávaly do oběhu pomocí ražby, kterou měl v gesci panovník dané země a mince tak představovaly symbol dané země. Předností mincovního systému bylo to, že hodnota drahého kovu obsaženého v dané minci a náklady na ražbu zpravidla refletovaly kupní cenu mince. Panovník určoval výši ražebného. Ražebné představovalo rozdíl mezi jmenovitou hodnotou mince a celkovými náklady na ražbu. (Jílek, 2013)

Plnohodnotné mince, které obsahovaly pouze drahý kov, nevydržely příliš dlouho. Po jistém čase používání docházelo k odlamování, ošoupaní a dalšímu opotřebení jednotlivých mincí. Dochází tedy k rozdílu mezi jmenovitou hodnotou a kupní silou mince a vznikají tak

„neplnohodnotné mince“. Neplnohodnotné mince se však dále používaly, neboť panovníci přesvědčili lid, že peníze se využívají bez ohledu na jejich vnitřní hodnotu. Je zjevné, že panovníci této skutečnosti využili a začali tak mince šidit. Při ražbě nových mincí se začaly přimíchávat běžně dostupné kovy. (Černohorský, 2011)

4.1.3 Bankovky

Za předchůdce bankovek jsou považovány poukázky, které vydávali zlatníci. Aby došlo k urychlení oběhu mincí došlo k jejich ukládání u zlatníků. Zlatníci přebrali mince a vystavili poukázku, která obsahovala informace o uložených mincích a jejich ryzosti. Poukázku pak bylo možné použít buď k vybrání mincí, nebo jako prostředek směny s jiným obchodníkem. Tento systém představoval pravý zlatý standard. (Jílek, 2013)

Díky dosavadnímu vývoji formy placení a směny dochází k obrovskému rozvoji obchodu a ten již není možné financovat pouze z mincí a drahých kovů. V této souvislosti se začínají používat obchodní směňky. Směňky byly velmi dobře právně upraveny a byly tak vymahatelné. Dlužník musel být známý a solventní, a částka na směnce musela odpovídat ceně při transakci. Vzhledem k tomu, že směňka byla splatná až v určitý okamžik, věřitelé raději prodávali směňky bance. Banky na odkupu směnek vydělávaly, neboť ji nikdy neodkoupily za jmenovitou hodnotu, ale část si strhly jako provizi. Tato provize se dodnes nazývá diskont. V den splatnosti směňky si banka nechala směňku proplatit od dlužníka v celé jmenovité hodnotě. (Černohorský, 2011)

Banky později nahradily roli zlatníků, kteří zastavovali mince a drahé kovy. Potvrzení o uložení mincí a drahých kovů tak přechází do rukou bankéřů. Princip byl stejný – na základě množství a ryzosti mincí byla vystavena poukázka. V tomto případě už však hovoříme o **bankovkách**. Netrvalo dlouho a bankéři přišli na zajímavý trik, jak zvýšit své zisky. Začali vydávat poukázky, které nebyly kryty žádným drahým kovem. Zcela správně a racionálně uvažovali, že si všichni klienti nepřijdou vybrat všechny drahé kovy najednou. Tento okamžik je de facto považován za vznik úvěrové emise, neboť banka neposkytovala bankovky, které předtím někdo přinesl, ale v bance vznikly nové a nekryté peníze. Důsledkem toho bylo, že banka emitovala více poukázek na drahý kov, než ve skutečnosti držela. Vznikají tak neplnohodnotné peníze. Později banky zjistily, že při úvěrové emisi

drahé kovy již vůbec nepotřebují a drahé kovy tak byly nahrazeny nekrytými papírovými a kovovými penězi – neboli fiat měny. (Jílek, 2013)

4.1.4 Fiat měny

Fiat měny neboli měny s nuceným oběhem (například Dolar, Euro, Česká koruna) dnes představují většinu peněz. Fiat měny nemají žádnou vnitřní hodnotu, neboť nejsou kryty žádným vzácným kovem ani ničím jiným. Název fiat měny plyne z podstaty těchto měn, jelikož jsou nařízeny vládou jednotlivých států/společenství (fiat = nařízení, rozkaz). Míra přijímání fiat měn závisí na důvěře a očekáváníích ve společnosti. Pokud by došlo ke ztrátě důvěry, zpravidla z důsledku nezodpovědné monetární politiky, může dojít k úplnému zastavení přijímání měny a občanským nepokojům. Ze zkušeností víme, že ponechání monetární politiky v rukou výkonných orgánů není to nejvhodnější řešení, neboť vlády by tak mohly být pobízeny k neustálému zvyšování peněz v oběhu k řešení finančních problémů a docházelo by tak k vysoké inflaci a ztrátě důvěry v danou měnu. Vhodnějším řešením je svěřit oblast monetární politiky nezávislé instituci – centrální bance. Centrální banka má tak za úkol vykonávat měnovou politiku. Vykonává tak pomocí cílů, jakými jsou například ekonomický růst a stabilita cenové hladiny. (Franco, 2014)

4.2 Virtuální měny

4.2.1 Základní charakteristika

Kryptoměny by se zjednodušeně daly definovat, jako digitální (virtuální) finanční systém, který je vytvořen tak, aby fungoval jako zprostředkovatel výměny aktiv. Celý systém je založen na silné kryptografii, aby všechny finanční transakce v rámci systému byly maximálně chráněny. Všechny transakce jsou zaznamenávány do veřejně přístupné databáze odborně nazývané jako „ledger“. V praxi to znamená, že všechny transakce jsou zpětně dohledatelné, ačkoliv virtuální adresa příjemce i plátce je zašifrována ve formě nahodilých znaků, čili není možné přiřadit konkrétní adresu konkrétní osobě. (Chowdhury, 2019)

Autor Jan Lánský ve své studii z roku 2018 stanovil šest podmínek, které definují kryptoměnu. Kryptoměnu definuje jako systém, který splňuje všech šest níže uvedených podmínek:

- 1) Systém nevyžaduje centrální autoritu. Jeho stav udržují uživatelé sítě.

- 2) Systém si udržuje dohled na jednotlivé kryptoměny a jejich vlastnictví.
- 3) Systém určí, zda nové kryptoměny mohou být vytvořeny. Pokud dojde k vytvoření nové kryptoměny, systém určí okolnosti jejich vzniku a jak určit vlastnictví těchto nových jednotek.
- 4) Vlastnictví kryptoměny může být prokázáno pouze pomocí kryptografie.
- 5) Systémem projdou transakce, ve kterých dojde k výměně mezi dvěma zašifrovanými jednotkami. Transakci může uskutečnit pouze subjekt, který prokazuje vlastnictví jednotky.
- 6) Pokud jsou zadány dvě rozdílné transakce souběžně, systémem projde alespoň jedna z nich.

Kryptoměny jsou jedinou měnou, které mají následující tři vlastnosti – zajišťují pseudo-anonymitu, nezávislost na centrální autoritě a ochrana proti dvojnásobné úhradě. Touto problematikou se ve světě financí zabývali lidé již v osmdesátých letech minulého století, avšak ke splnění všech třech podmínek došlo až v roce 2008, kdy Satoshi Nagamoto představil esej s názvem „A peer to peer electronic cash system“. 3. ledna roku 2009 pak stejný autor/skupina autorů představil/a první (a dodnes nejznámější) kryptoměnu bitcoin.

Nyní k výše uvedeným třem podmínkám. **Zajištění pseudo-anonymity** lze chápat tak, že pokud uživatel, který se řídí elementárními pravidly při provádění transakcí, nemůže být jednoduše identifikován. Nicméně uživatelé mohou svoji identitu vědomě i nevědomě odhalit. Případně může dojít k odhalení identity i pomocí vnějších informací. *(Např. si představme situaci, kdy provedeme transakci s osobou, kterou známe a na jejíž adresu zašleme nějaký obnos kryptoměny. Známe tedy adresu a dokážeme k ní i přiřadit určitou osobu, můžeme se pak tedy podívat do ledgeru a zobrazit si výpis všech transakcí, ve kterých figurovala námi vybraná adresa. pozn. autora).* **Nezávislost na centrální autoritě** je jedním z pilířů kryptoměn a zároveň i důvod, proč kryptoměny dnes existují. Znamená to, že v systému neexistuje jedna autorita, která by byla oprávněna jakkoliv změnit pravidla, na kterých je daná kryptoměna založena. Ke změně pravidel lze docílit pouze v případě, že se většina uživatelů (75 - 95 %) dohodne. Je však nutné podotknout, že takové změny jsou spíše raritou. (Lánský, 2018). **Ochrana proti dvojitě úhradě** představuje ochranný prvek, který zamezuje přesunout obnos kryptoměny na dvě adresy současně. V případě, že jsou kryptoměny převedeny na jednu adresu, systém automaticky vyhodnotí druhou transakci

jako neplatnou. Pro konvenční měny tento problém v podstatě neexistuje, neboť pokud někomu předáme fyzické peníze, je logické, že je nemůžeme předat již žádné jiné osobě. V případě kryptoměn bylo tuto skutečnost náročně eliminovat. (Rosenfeld, 2012)

4.2.2 Historie virtuálních měn

70. a 80. léta

Pravděpodobně nikoho nepřekvapí, že původ virtuálních měn sahá do období, kdy vznikl Internet. Internet - vynález, který změnil celý svět jako nic před ním. Přeci jen, kdyby zde neexistovala globální síť počítačů, nic jako kryptoměny by nemohlo fungovat. Údajně první transakce na internetu proběhla v roce 1972, kdy název internet ještě neexistoval. Místo něj bylo používáno označení Arpanet. V té době byl Arpanet využíván pouze armádou a akademiky. Studenti z MIT a Stanfordské univerzity chtěli prostřednictvím Arpanetu uskutečnit obchod s marihuanou. Vzhledem k tomu, že se jednalo o nelegální činnost, peníze nebyly nikdy převedeny. I přesto tato událost představuje první obchod uskutečněný na internetu, a co je hlavní, nastínila transakční potenciál internetu. (Grabowski, 2019)

V roce 1983 představil David Chaum myšlenku digitálních peněz, kdy během konference posluchačům vysvětloval, že za pomoci digitálních peněz bude možné si například koupit přístup do databáze, pořídit si software nebo noviny prostřednictvím emailu, zahrát si počítačovou hru online, obdržet dlužné peníze od kamaráda, nebo si například objednat pizzu. Řekl: „Možnosti jsou skutečně neomezené“. David Chaum je mnohdy považován za zakladatele anonymní komunikace, jelikož vynalezl mnoho šifrovacích protokolů, na jejichž základech stavíme dodnes a jsou i nezbytnou součástí virtuálních měn. (Grabowski, 2019)

90. léta

Komerčního využití se virtuální měny dočkaly až v roce 1990, kdy výše zmíněný David Chaum založil společnost DigiCash, Inc. Společnost vyvinula systém eCash, pomocí nějž bylo možné převádět peníze online i offline na základě šifrovaných protokolů. Systém eCash byl používán napříč různými bankami například ve Spojených státech a Finsku. Až do roku 1999 byl systém eCash vlastněn společností DigiCash. V roce 1999 pak společnost InfoSpace přebrala kontrolu nad společností a systém eCash byl upozaděn. (Lee, 2015)

V druhé polovině devadesátých let, konkrétně roku 1996, přichází E-gold, neboli elektronické zlato. Název E-gold nebyl zvolen jen tak. Důvodem k tomuto označení bylo to, že systém byl krytý fyzickým zlatem. E-gold byl platební systém, který byl v porovnání s dosavadními tradičními platebními systémy unikátní. Jeho unikátnost spočívala v čistě digitální podobě a absolutní nezvratnosti transakcí. Systém se stal velmi rychle populárním a byl využíván více než pět milióny uživatelů. Nicméně systém se stal médiem pro kriminální činnost (hackerské útoky, internetové podvody) a byl následně shozen vládou Spojených států. (Grabowski, 2019)

Před tím, než byl podán návrh na zabavení a likvidaci zlatých rezerv e-Gold dle zákona o propadnutí majetku z roku 2008, objem transakcí jenž procházely systémem e-Gold dosahoval více než 2 miliardy amerických dolarů. (Lee, 2015)

Přesuneme-li se o pár let dále, zjistíme, že nadšenci ze Silicon Valley se snažili najít nové způsoby, jak realizovat transakce online. Zlom přišel roku 1998, kdy Elon Musk a Peter Thiel spolu s dalšími založili PayPal. PayPal představoval celosvětový platební systém, který podporoval převody peněz na internetu, jako alternativu k tradičním způsobům v podobě šeků a poštovních poukázek (složenek). Na rozdíl od e-Gold je PayPal hojně využíván dodnes a představuje velmi populární způsob, jak převádět peníze v kybernetickém prostoru. (Grabowski, 2019)

Doposud jsme se zabývali pouze způsoby, jakými se převáděly peníze v minulosti. Ve skutečnosti e-Gold ani PayPal nenaplňovaly charakteristiky kryptoměny, neboť sloužily pouze za účelem přesunu peněz. V případě e-Gold se jednalo o jakési virtuální přesuny elektronického zlata, PayPal zase představoval přesuny klasických fiat měn ve virtuálním prostředí. Samy o sobě neměly žádnou hodnotu a byly centrálně řízeny, nenaplňovaly tak podstatu kryptoměny. (pozn. autora)

2008

Uprostřed probíhající globální finanční krize vzkvétá zájem o kryptoměny v podobě, v jaké je známe dnes. Nick Szabo se na svém blogu domníval, že kryptoměny by měly potenciál vyřešit hned několik problémů spojených s konvenčním finančním systémem. Na blogu tak

představil myšlenku jakéhosi digitálního zlata (*nikoliv však e-Gold, digitálním zlatem je dnes označován Bitcoin. Anglický ekvivalent, který použil, zněl bit gold – bit jako základní datová jednotka. pozn. autora*). Ze zvoleného názvu lze tedy odvodit, že zlatem myslel jakousi komoditu, kterou je potřeba vytěžit a bit jakožto záznam ve virtuálním rejstříku (ledger). Celé jeho pojednání bylo velmi technické, zjednodušeně lze však říci, že měl na mysli jednoduchý protokol, který vyžadoval investovat zdroje (výpočetní technika) a jako odměnu uživatelé obdrželi digitální zlato. Proces těžby spočíval v ověřování záznamů ve veřejné databázi. Ještě tentýž rok vznikla první masově využívaná a rozšířená kryptoměna bitcoin. (Lee, 2015)

4.3 Blockchain

„Blockchain je decentralizovaná a distribuovaná účetní kniha (DLT – Distributed ledger technology), která nemá centrální autoritu. Je využíván k zaznamenávání a uchování stejné informace uchované v bloku napříč množinou počítačů. Tyto bloky jsou navzájem propojeny a tvoří vlastní síť. Záznam, který byl do sítě vložen, nemůže být následně upraven, pokud se na tom neshodne většina uživatelů sítě.“ (Alman, Hirsch, 2019)

Na technologii blockchainu stojí většina dnešních kryptoměn. Dalo by se říci, že blockchain vznikl společně s první kryptoměnou bitcoin v roce 2008. Bitcoin byl tehdy prvním a nejlepším využitím blockchainu vůbec. (Grabowski, 2019)

Blockchain je stále rostoucí řetězec bloků. Každý blok obsahuje skupinu nových transakcí a spojení s předešlým blokem v síti. Nové transakce v síti jsou shromážděny do bloku, který je následně zanesen do blockchainu. Je důležité zmínit, že již provedené transakce z blockchainu nezmizely, jsou uchovány v předešlých blocích, na které jsou napojeny nově vznikající bloky. (Franco, 2014)

Každý záznam, který je zanesen do blockchainu obsahuje unikátní digitální podpis, který je vytvořen kryptografickou hashovací funkcí. Můžeme říci, že se jedná o jakýsi digitální otisk prstu. Kromě klasické hashovací funkce každý blok v blockchainu obsahuje navíc ještě informace o hashi předcházejícího bloku, čas jeho vzniku a data o dosažení konsenzu, neboli proof-of-work, což je algoritmus, pomocí nějž jsou nové bloky vytvořeny a ověřeny. Díky

zmíněným vlastnostem je blockchain velmi obtížné prolomit. Pokud by se někdo pokusil změnit jakoukoliv informaci obsaženou v jakémkoliv bloku, dojde ke změně hashe a následně zprůtrhání celé sítě. Proto tedy název blockchain – řetězec bloků. (Alman, Hirsch, 2019)

K zabezpečení decentralizované databáze využívá blockchain metodu konsenzu proof-of-work. To znamená, že blockchain je vůči vnějším útokům zabezpečen výpočetním výkonem, který byl použit k jeho vytvoření. Útočník, který by se snažil změnit informaci obsaženou v blockchainu by musel vynaložit minimálně stejné množství výpočetního výkonu, jaké bylo doposud vynaloženo v rámci daného blockchainu. (Franco, 2014)

4.3.1 Hashovací funkce

Hashovací funkce je matematická funkce, která má následující tři vlastnosti – vstupem může být informace jakékoliv délky, výsledkem je výstup fixní délky a je efektivně vypočitatelná. (Narayanan, 2016)

Kvalitní hashovací funkce by měla distribuovat vstupní hodnoty do hash hodnot proporcionálně, aby bylo docíleno toho, že každá hash hodnota je propojena s přibližně stejným počtem možných výstupních hodnot. Jednou z cest, jak proporcionálního rozdělení docílit je nechat se hashovací funkci chovat tak náhodně, jak jen je to možné. Ačkoliv se hashovací funkce chová náhodně, je pořád deterministická, neboť z jednoho vstupu vzejde vždy stejný výstup. (Franco, 2014)

Klíčovou vlastností hashovacích funkcí je jejich nezvratnost. Hashovací funkce nemůže být tedy zpětně rozšifrována. (Abbatemarco, 2018)

Kryptografické hashovací funkce

Většina kryptoměn využívá kryptografické hashovací funkce (někdy nazývané jako „secure hash functions“). Například Bitcoin využívá kryptografickou hashovací funkci SHA256². Kryptografické hashovací funkce rozšiřují běžné hashovací funkce o další vlastnosti:

- **Jednosměrnost** – Vezmeme-li hodnotu hash, musí být výpočetně nemožné zjistit vstupní informaci.
- **Slabá odolnost vůči kolizi** – Vzhledem ke vstupu je výpočetně nemožné najít jiný vstup se stejnou hash hodnotou.
- **Silná odolnost vůči kolizi** – Je výpočetně nemožné najít dvojice vstupní data, která by vyústila ve stejnou hash hodnotu. (Franco, 2014)

4.3.2 Mechanismus konsenzu

4.3.2.1 Proof of work

Jedním z problémů decentralizovaných sítí bývá dosažení celkové spolehlivosti systému. To často vyžaduje, aby se jednotlivé uzly sítě dohodly na nějaké hodnotě, která je potřebná během výpočtů. Metoda, která této shody uživatelů docílí, se nazývá konsenzus. Zjednodušeně by se dalo říci, že konsenzus je dynamický způsob dosažení shody ve skupině. Zatímco obecný systém hlasování zvýhodňuje větší skupinu a upozaduje menšinu, konsenzus vyvolává dohodu, která by mohla být přínosem pro všechny zúčastněné. (Chowdhury, 2019)

Nejnámější metoda k dosažení konsenzu v rámci blockchainu je algoritmus Proof-of-Work (PoW). PoW nevyžaduje, aby všechny uzly v síti našly nové bloky k dosažení konsenzu. Místo toho PoW využívá hashovací funkci k vytvoření podmínek, za kterých může jeden uživatel oznámit nalezení nového bloku. Následně tento nově nalezený blok může každý uživatel sítě vidět a následně ověřit jeho validitu. V praxi funguje PoW blockchain následovně: uzel vytvoří „kandidátský blok“ naplněný informacemi, poté vypočítá jeho hash hodnotu, která musí odpovídat bezpečnostnímu standardu definovaného blockchainovým protokolem, aby mohl hostovat nový blok. (Abbatemarco, 2018)

Odměnou pro těžaře, který úspěšně vytvoří nový blok je speciální transakce v daném bloku. Tato transakce je označována jako „coin-creation transaction“. Těžař má rovněž možnost si vybrat adresu, kam bude nově získaný obnos kryptoměny připsán (zpravidla jeho vlastní adresa). Tato odměna by se v podstatě dala nazvat jako platba těžaři za vytvoření nového bloku, díky kterému může blockchainová síť fungovat. (Narayanan, 2016)

4.3.2.2 Alternativní algoritmy

Ačkoliv je PoW algoritmus velmi bezpečný a odolný vůči útokům, má však bohužel i jednu velkou nevýhodu. Nedostatkem algoritmu PoW je nadbytečné a neefektivní využívání elektrické energie, která je zapotřebí k zajištění funkčnosti blockchainu postaveného na algoritmu PoW. Kritici bitcoinu a virtuálních měn obecně využívají tohoto argumentu a jsou znepokojeni, že kryptoměny nejsou energeticky udržitelné. Existují však i další algoritmy, které budou představeny v následujících řádcích. (Chowdhury, 2019).

Proof of Stake (PoS)

Tento algoritmus funguje na myšlence, že uživatel již disponuje určitým množstvím kryptoměny. V tomto případě uživatel již vynaložil a zainvestoval prostředky do sítě a tím pádem by jakýkoliv pokus o útok tímto uživatelem na síť pro něj osobně nepřevažoval nad výhodami, které pro něj plynou z jeho současné pozice. Tento algoritmus byl poprvé představen kryptoměnou Peercoin a v budoucnu bude využit v nové verzi blockchainu Etherea nazývané Serenity. Dalším významnou myšlenkou PoS je „stáří mince“ (coin age). Coin age představuje kritérium odvozené od množství času a počtu mincí, které nebyly doposud utraceny (neboli jak dlouho dané mince daný uživatel drží). V tomto modelu se šance na navrhování a podepsání nového bloku zvyšují se stářím mince. (Bashir, 2018)

Pro PoS existuje ještě nadstavba nazývaná „Delegated Proof of Stake“. DPoS představuje inovaci oproti standardnímu PoS, kdy každý uživatel, který drží určitý objem kryptoměny, může delegovat ověření transakce jiným uživatelům prostřednictvím hlasování. (Bashir, 2018)

Proof of Burn (PoB)

PoB je další distribuovaný mechanismus konsenzu a je tak alternativou PoW a PoS. Spočívá v tom, že těžaři odešlou (spálí) určitý obnos jiné kryptoměny na ověřenou adresu, ze které nebudou následně utraceny. Z pohledu těžařů tento systém vypadá draze. Výhodou ovšem je, že nedochází k žádné spotřebě zdrojů, kromě podkladového aktiva. (Chowdhury, 2019)

Proof of Importance (PoI)

PoI představuje významnou a zároveň odlišnou myšlenku od algoritmu PoS. Algoritmus PoI spočívá v tom, že nespolehá pouze na objem kryptoměny vlastněné uživatelem, jako tomu je v případě PoS, ale také monitoruje, jak daný uživatel kryptoměnu využívá a kam ji přesouvá. Pomocí tohoto monitorování dokáže systém stanovit úroveň důvěry a důležitosti daného uživatele. (Bashir, 2018)

Proof of Space (PoSpace)

Proof of Space, někdy též nazývaný jako Proof of Capacity, znamená, že uživatel, který má zájem o určitou službu, alokuje nepodstatné množství paměti, nebo místa na disku k vyřešení určitého problému zadaného poskytovatelem služby. PoSpace je velmi podobný algoritmu PoW, až na to, že místo výpočtů se používá úložiště. (Grabowski, 2019)

Proof of Activity (PoA)

Tento algoritmus je kombinací PoW a PoS. Stojí na tom, že uživatel, který vytěží blok, je vybírán pseudonáhodným, ale jednotným způsobem. Tento mechanismus je v porovnání s PoW energeticky efektivnější. Využívá nový koncept nazvaný „Follow the Satoshi“. V případě PoA dochází ke kombinaci algoritmů PoW a PoS k dosažení konsenzu a zároveň k vysoké úrovni zabezpečení. Algoritmus PoW je využit pouze v první fázi mechanismu, poté dojde k přepnutí na PoS, který spotřebovává pouze zanedbatelné množství energie. Díky tomu je tedy docíleno vyšší energetické úspornosti a zároveň požadované úrovně zabezpečení. (Bashir, 2019)

4.4 Transakce

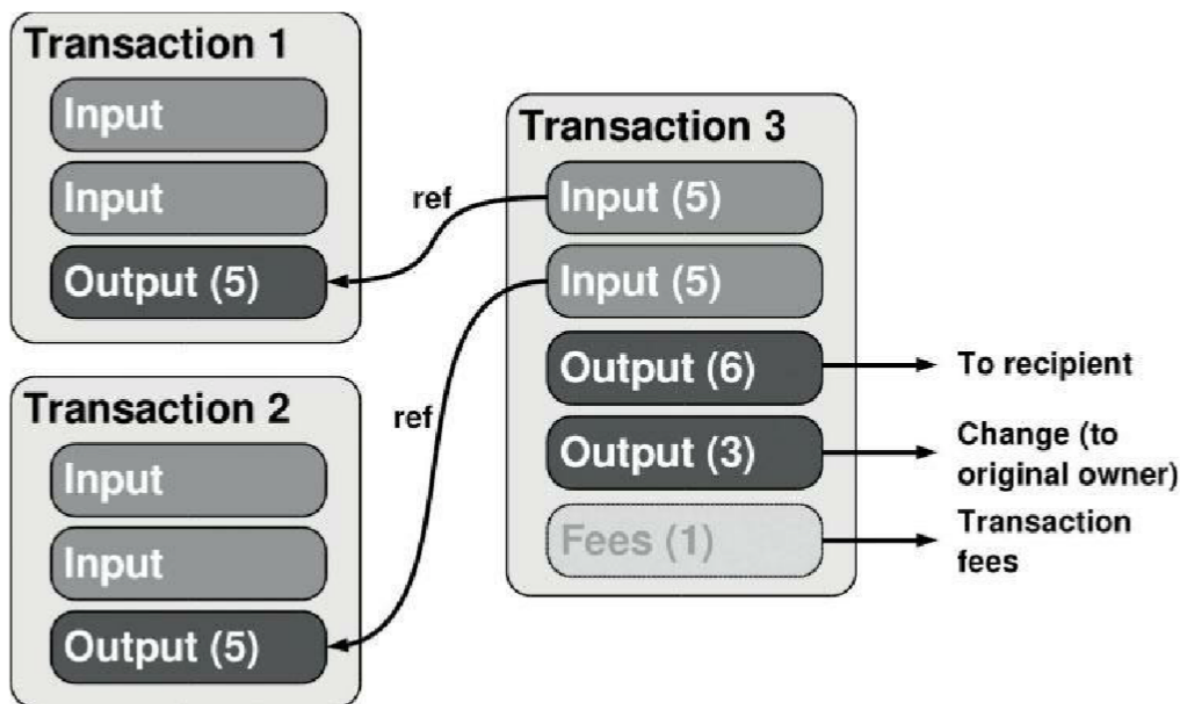
Kryptoměny nejsou uloženy v počítači uživatelů, ale jsou „pouze“ záznamy v distribuované databázi nazývané blockchain. Na rozdíl od centralizovaných fiat měn blockchain neuchovává uživatelské účty a jejich zůstatky. Blockchain uchovává transakce. (Franco, 2014)

Transakce jsou v jádru každého kryptoměnového ekosystému. Transakce mohou být tak jednoduché, jako pouhé zaslání kryptoměny z jedné adresy na druhou. Mohou ale být i velmi komplexní, záleží však na okolnostech. Každá transakce je složena z alespoň jednoho vstupu a jednoho výstupu. Za vstup jsou považovány utracené mince, které vznikly v předcházející transakci. Výstupem jsou „nově“ vznikající mince. Pokud se jedná o „coin creation“ transakci, neexistuje žádný vstup a tím pádem ani není potřeba transakci verifikovat. V případě, že se jedná o transakci jejímž účelem je přesunout kryptoměnu z jedné adresy na druhou, je za potřebí transakci podepsat za pomoci privátního klíče uživatele, který kryptoměnu přesouvá. Požadována je rovněž reference k předcházející transakci (vstup), aby byla zajištěna transparentnost a byl zřejmý původ mince. Samotné transakce jsou pak zaneseny do blockchainu a kdokoliv si je může zobrazit, například za pomoci online blockchain prohlížeče. (Bashir, 2018)

Aby byla transakce validní, součet vstupů musí být rovný, nebo větší než suma výstupů. Rozdíl mezi vstupy a výstupy, pokud nějaký existuje, představuje transakční poplatek. Transakční poplatek je připsán těžařům za zanesení transakce do blockchainu. (Franco, 2014)

Obrázek č. 1 reprezentuje příklad transakce. V tomto případě chce uživatel odeslat 6 jednotek kryptoměny příjemci. Nicméně odesílatel nemá na své adrese transakční výstup o hodnotě přesně 6 jednotek. Disponuje dvěma transakčními výstupy o hodnotě 5 jednotek. Přesto vytvoří transakci, kde se tyto dva výstupy sloučí a odešle tak 6 jednotek příjemci. Po zanesení transakce do systému zůstanou uživateli k dispozici 3 jednotky kryptoměny. Jedna jednotka kryptoměny je v tomto případě transakčním poplatkem a je tak postoupena těžařům. Předtím, než je transakce zanesena do sítě, musí uživatel transakci podepsat za pomoci privátního klíče, aby došlo k ověření, že daný uživatel má oprávněný přístup k dané adrese, ze které se kryptoměna přesouvá na jinou. (Franco, 2014)

Obrázek 4 Transakce



(zdroj: Franco, 2014)

4.4.1 Životní cyklus transakce

1. Uživatel odešle transakci prostřednictvím softwarové peněženky, nebo pomocí jiného rozhraní.
2. Softwarová peněženka podepíše transakci použitím privátního klíče odesílatele.
3. Transakce je zaslána do sítě pomocí zahlcovacího algoritmu (flooding algoritihm).
4. Těžaři transakci ověří a zanesou ji do dalšího bloku. Těsně před tím, než je transakce zanesena do bloku, je uložena ve speciální vyrovnávací paměti nazývané „transaction pool“.
5. Začne proces těžby. Proces těžby slouží k zabezpečení blockchainu a vytváření nových mincí, jakožto odměna pro těžaře za vynaložení značné míry výpočetní kapacity.
6. Jakmile těžař oznámí nalezení nového bloku, dojde k zanesení daného bloku do sítě.
7. Další těžaři následně ověří nově vzniklý blok a schválí ho.
8. Poté, co je nový blok schválen 3-6 dalšími těžaři, příjemce obdrží kryptoměnu ve své peněžence. Požadované schválení 3-6 těžaři je pouze doporučený rozsah. Transakce může být ovšem schválena i po jednom ověření. Nicméně pokud systém funguje na

principu mnohonásobného ověření, je v podstatě eliminováno riziko dvojí úhrady. (Bashir, 2018)

4.4.2 Transakční poplatek

Jak již bylo zmíněno, transakční poplatky jsou připisovány těžařům. Hodnota poplatku se odvíjí od množství kryptoměny, která je přesouvána a priority zpracování transakce. Transakční poplatek se vypočte jako rozdíl mezi sumou vstupů a sumou výstupů.

$$\text{poplatek} = \text{suma}(\text{vstupů}) - \text{suma}(\text{výstupů})$$

Poplatky jsou využívány jako motivace pro těžaře, aby zahrnuli transakce od uživatelů do bloku, který vytvářejí. Všechny transakce nejdříve skončí ve fondu paměti (memory pool), odkud jsou vybírány na základě priority těžaři a zahrnuty do kandidátského bloku. Transakce s vyšším poplatkem jsou zpracovány dříve než transakce s nižším poplatkem. (Bashir, 2018)

Transakční fond

Transakční fondy (memory pools) vznikají v operační paměti (RAM) jednotlivých těžařů za účelem uchování dočasného seznamu transakcí, které nebyly dosud zpracovány do bloku. Jak již bylo zmíněno, transakce jsou zapsány do bloku až po jejich verifikaci a rychlost zapsání závisí na jejich prioritě. (Bashir, 2018)

4.5 Těžba virtuálních měn

„Těžba je zásadním požadavkem k fungování blockchainu. Bylo by zavádějící, myslet si, že existuje reálná spojitost mezi těžním fyzického zlata a kryptoměnami. Ve skutečnosti těžaři zlata jsou odměňováni za produkci zlata, mezitím co těžaři kryptoměn nejsou odměňováni za produkci kryptoměn, ale za službu, která chrání celý systém.“ (Chowdhury, 2019)

4.5.1 Proces těžby

Těžba je proces, při němž dochází k zanesení nových bloků do blockchainu. Bloky obsahují transakce, které jsou validovány jednotlivými uzly v síti během procesu těžby. Jakmile je nový blok ověřen, dojde k jeho zanesení do blockchainu, čímž je zajištěna kontinuita a blockchain se tak neustále rozšiřuje. Tento proces je velmi náročný na zdroje kvůli

požadavkům algoritmu PoW, kde se těžaři snaží nalézt hash hodnotu, která je nižší, než obtížnost sítě – neboli „target“. Tato obtížnost nalezení správné hash hodnoty má zajistit, že těžaři vynaloží požadované množství zdrojů, než dojde k přijetí nového bloku. (Bashir, 2018)

Proces těžby by se rovněž dal charakterizovat, jako služba pro uchovávání záznamů prováděná prostřednictvím výpočetního výkonu počítačů účinkujících uzlů. Těžáři autorizují nové transakce a zapisují je do blockchainu. Pravidelně seskupují nové transakce do bloku, který je následně vysílán do sítě a ověřen dalšími uzly. Tímto mechanismem je docíleno, že blockchain je konzistentní, kompletní a nezměnitelný. (Chowdhury, 2019)

Těžáři, kteří disponují vysokým výpočetním výkonem mají vyšší pravděpodobnost vyřešení nového bloku. Nicméně náročnost těžby se postupně s počtem vytěžených bloků zvyšuje. V případě kryptoměny bitcoin, kterou se tato diplomová práce zabývá, došlo během první transakce k přenosu 50 bitcoinů mezi všechny tehdy účinkující uzly v síti. Odměna pro těžaře se přibližně každé čtyři roky snižuje na polovinu (exaktně se odměna půlí po vytěžení 210 000 bloků, což jsou zhruba zmiňované čtyři roky). Tento mechanismus se nazývá halving. Když byl Bitcoin představen, odměna za vytěžení bloku činila 50 Btc, poté v roce 2012 došlo k halvingu a odměna se tak snížila na 25 Btc. Další halving následoval v roce 2016 a odměna klesla na 12,5 Btc. Poslední halving byl v roce 2020, od kdy si těžaři za nově vytěžený blok připíší 6,25 Btc. (Lee, 2015) (Bashir, 2018)

Jeden blok je vytvořen a vytěžen zhruba každých 10 minut, aby byla zajištěna kontrola nad frekvencí generování nových bitcoinů. Tato frekvence musí být udržována Bitcoinovou sítí a je zakódována do samotného Bitcoin protokolu. Denně dojde k vytěžení 144 bloků, což v okamžiku psaní této diplomové práce představuje zhruba 900 nových bitcoinů. Počet nově vzniklých mincí se může drobně lišit, nicméně počet bloků zůstává stejný, a to 144. Nabídka bitcoinu je limitována a zhruba v roce 2140 dojde k vytěžení všech bitcoinů – konkrétně se jedná o 21 milionů. Těžáři budou ale i po tomto datu mít možnost stále profitovat z ekosystému v podobě transakčních poplatků. (Bashir, 2018)

Jednou z předností mechanismu těžby je, že odměňuje rané osvojitele (early adopters) za podporu sítě. Toto bylo velmi důležité v počátcích, kdy došlo k představení Bitcoinu. Bitcoin za sebou nemá velkou korporaci, která by investovala do marketingu a dostala ho tak do podvědomí lidí. Všechno muselo proběhnout přirozeně, kdy si prvotní uživatelé o novince povídali mezi sebou. (Pedro, 2014)

Úloha těžařů

Jakmile se do sítě připojí nový uzel, čeká na něj několik úkolů, které musí vykonat.

1. Synchronizace se sítí: Po připojení do sítě dojde ke stáhnutí blockchainu prostřednictvím vyžádání historických bloků od ostatních uzlů.
2. Validace transakce: Transakce vysílané do sítě jsou ověřovány plnými uzly za pomoci ověření podpisu a výstupu.
3. Validace bloku: Těžaři a plné uzly mohou začít validovat bloky, které obdrží. Validace probíhá podle určitých pravidel, které zahrnují ověření každé transakce v bloku spolu s ověřením kryptografické „nonce“ hodnoty. (nonce hodnota je číslo, u nějž je nízká pravděpodobnost, že se bude opakovat a slouží k zabezpečení blockchainu).
4. Vytvoření nového bloku: Těžaři navrhnou nový blok sloučením nově vyslaných transakcí do sítě po jejich validaci.
5. Vykonat Proof-of-Work: Tento úkol je v procesu těžby klíčový. V tomto bodě těžaři naleznou validní blok za použití výpočetního výkonu. Hlavička bloku obsahuje 32-bitové nonce pole a po těžařích je vyžadováno, aby opakovaně dosazovali nonce hodnotu dokud výsledný hash není menší než predeterminovaný target.
6. Připsání odměny: Jakmile uzel vyřeší PoW, dojde k okamžitému vyslání výsledku do sítě a ostatní uzly ověří a přijmou blok. Nicméně existuje malá šance, že nově vytěžený blok nebude okamžitě přijat ostatními těžaři z důvodu kolize s jiným nalezeným blokem ve stejný okamžik. Po přijetí bloku je těžař odměněn stanovenou sumou bitcoinu a příslušnými transakčními poplatky. (Bashir, 2018)

4.5.2 Technologie těžby

V průběhu času těžaři Bitcoinu využívali spoustu různých metod, jak kryptoměnu co nejefektivněji těžít. Hlavní princip těžby bitcoinu je založen na SHA-256 algoritmu a experti postupem času přicházeli se sofistikovanými systémy, jak hash vypočítat rychleji a rychleji. V následující kapitole budou zmíněny různé metody, které byly využívány k těžbě bitcoinu a jak se postupně vyvíjely. (Bashir, 2018)

CPU

CPU představuje zkratku pro Central Processing Unit – hlavní čip uvnitř počítačů a dalších zařízení. Je jedním z nezbytných hardwarových komponentů a jeho výpočetní kapacita může být využita na různé výpočetní úlohy včetně těžby kryptoměn. Při prvotním představení Bitcoinu byla těžba implementována právě na CPU. Během první fáze těžby, která probíhala od roku 2009 do léta roku 2020, byla těžba prováděna pouze za pomoci CPU. Během této fáze se náročnost těžby, spolu s nově vstupujícími nadšenci, zvyšovala a vznikla tak potřeba pro nalezení efektivnějšího řešení. (Franco, 2014)

GPU

Zkratka GPU znamená Graphics Processing Unit – specializovaný počítačový čip původně využívaný pro zrychlení grafických výpočtů. Právě kvůli narůstající obtížnosti těžby se těžaři snažili nalézt efektivnější alternativu, a tak začali využívat grafické karty, které podporují rychlejší a paralelní výpočty (= lze provádět více úloh najednou). Toto se ukázalo jako efektivnější řešení, než dosavadní CPU. Uživatelé rovněž využívali techniky jako přetaktování grafické jednotky, aby dosáhli maximálního možného výkonu. V případě GPU také existuje možnost mít více grafických jednotek najednou. Nicméně i grafické karty mají své limity, a to v podobě přehřívání a potřeby specializovaného hardwaru pro ukotvení více grafických karet najednou. K přechodu na jinou technologii také zapříčinil růst cen grafických jednotek z důvodu zvýšené poptávky, což ovlivnilo například i hráče PC her a uživatele grafických softwarů. (Bashir, 2018)

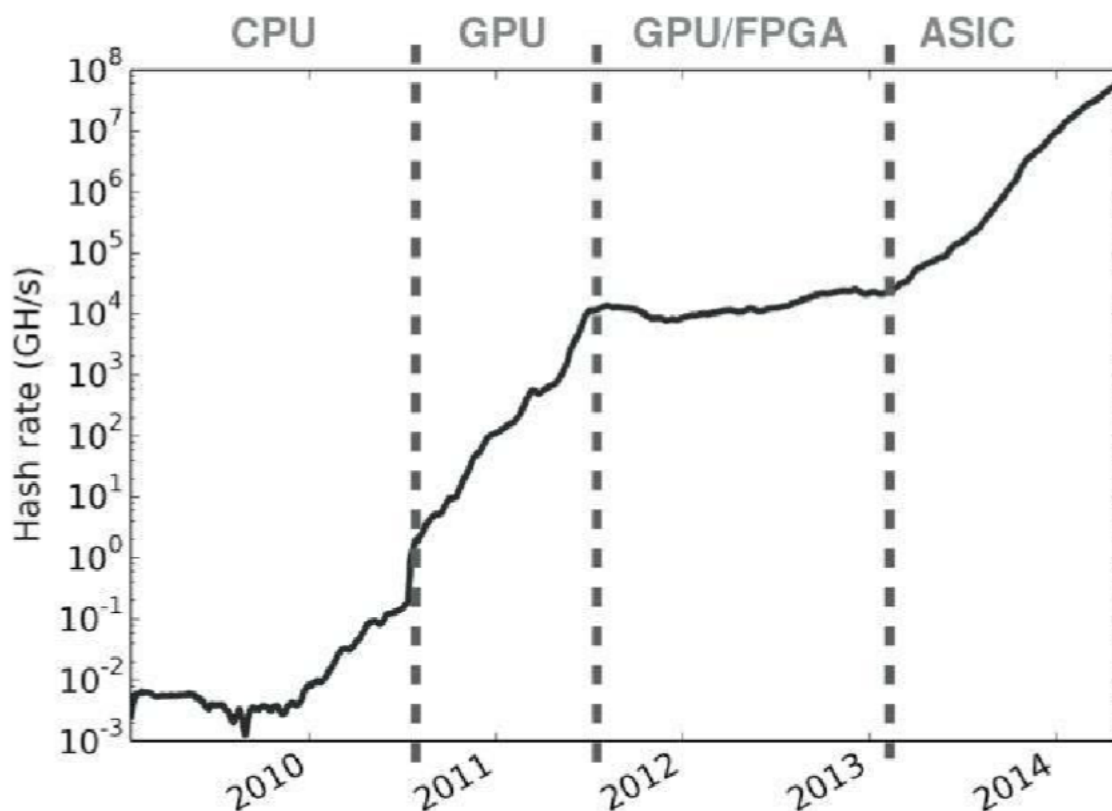
FPGA

FPGA neboli Field Programmable Gate Array. FPGA je integrovaný obvod čipů, který je sestaven s předem určeným účelem. Jak název napovídá, FPGA obvody jsou programovatelné a záleží tak na každém pro jaký účel čipy využije. Tato metoda byla představena v polovině roku 2011 a dlouhou dobu tak byla využívána simultánně s grafickými kartami. Oba způsoby měly svá pro a proti. Grafické jednotky měly lepší poměr cena/výkon a lépe si držely cenu. FPGA obvody zase byly efektivnější z hlediska spotřebované energie. Nicméně využití FPGA vyžadovalo hluboké znalosti k naprogramování a konfiguraci. To vedlo ke krátkodobému využití této technologie. (Franco, 2014)

ASIC

Application Specific Integrated Circuit byl přímo navržen k výpočtům SHA-256. Tyto specializované čipy byly vyráběny různými výrobci a nabízely velmi vysoký výpočetní výkon právě na šifru SHA-256. Toto řešení fungovalo ale pouze chvíli, neboť s rostoucí náročností těžby se těžba prostřednictvím jedné ASIC jednotky stala brzy neprofitabilní. V současné chvíli se těžba z pohledu jednotlivce v podstatě nevyplatí, jelikož je za potřebí. spousty energie a kapitálu k vytvoření profitabilní těžební jednotky. Existují však profesionální centra, která využívají tisíce ASIC jednotek současně a nabízejí těžební kontrakty uživatelům, kteří chtějí těžít svépomocí. (Bashir, 2018)

Graf 1 Hash rate Bitcoinové sítě na logaritmické křivce.



(zdroj: Franco, 2014, blockchain.info)

4.5.3 Možnosti těžby

Existují tři způsoby, jak těžít bitcoin a to solo mining, mining contracts a pool mining.

Solo mining

Solo mining neboli individuální těžba představuje způsob, kdy těžař vypočte celý hash individuálně a obdrží celou odměnu za vytěžení bloku. Šance, že tímto způsobem obdrží bitcoiny je velice nízká. Dobře technicky vybavený těžař by tímto způsobem potřeboval v průměru tři měsíce k tomu, aby obdržel nějakou odměnu. Proces těžby je náhodný a neukládá se do žádné paměti, takže když těžař nevyřeší blok v dané tříměsíční periodě, nebude nijak blíže k vyřešení bloku v periodě nadcházející. Navíc efektivita individuální těžby se se zvyšující se náročností postupně klesá. (Lee, 2015)

Průměrný potřebný čas na vytěžení nového bloku se dá přibližně spočítat pomocí následující rovnice:

$$\text{čas} = \frac{\text{náročnost} \times (2^{32})}{\text{hashrate}}$$

Mining contracts

Těžební kontrakty jsou pro ty, kteří by se chtěli podílet na těžbě bitcoinu, ale nechtějí se starat o potřebný hardware a investovat do něj. Tyto kontrakty poskytují těžební střediska, která zájemcům za poplatek poskytnou potřebný výkon po určitou dobu. Zájemce tak potřebuje pouze zařízení pro komunikaci a případně vlastní Bitcoinovou peněženku. Existují tři typy těžebních kontraktů:

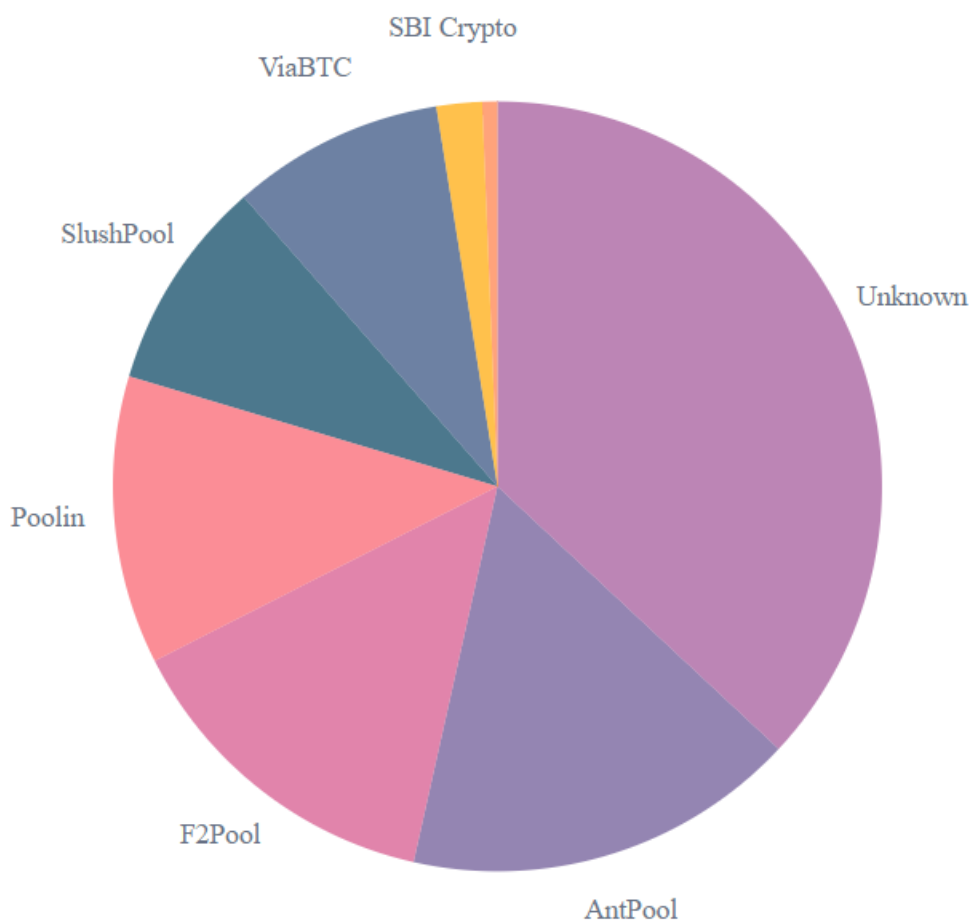
- Hosted mining – uživatel si od pronajímatele pronajme zařízení pro těžbu.
- Virtual hosted mining – v tomto případě si uživatel vytvoří vlastní soukromý server určený k těžbě bitcoinu na který si může případně nahrát svůj těžební software.
- Leased hashing power – uživatel si pronajme pouze výpočetní výkon, nebo jeho část. U tohoto kontraktu se tedy nejedná o pronájem fyzického/virtuálního zařízení. Poskytovatel služby si pak bere podíl na obdržovaných bitcoinech. (Lee, 2015)

Mining pools

Mining pool vzniká, když se skupina těžařů dohodne ke kooperaci při těžení bloků. Odměnu za vytěžený blok získá manažer poolu a ten ji následně rozdělí mezi participující těžaře, kteří investovali své zdroje. Tento způsob těžby je mnohem ziskovější než solo mining, neboť v případě poolu je odměněn každý těžař, který je jeho součástí nehledě na to, jestli blok vytěžil právě on. (Bashir, 2018)

Existuje vícero modelů, jak je odměna distribuována mezi těžaře. Jedním z nich je takzvaný Pay Per Share. V tomto modelu je každý těžař odměněn stejnou sumou. Dalším a častěji využívanějším modelem je model proporcionální. V případě proporcionálního modelu se odměna těžaře odvíjí od výpočetního výkonu, který pro těžbu alokoval. (Bashir, 2018)

Graf 2 Hashrate distribuce napříč největšími mining pooly k 23.9.2021



(zdroj: blockchain.info/charts/pools)

Na grafu č. 2 můžeme vidět nejvýznamnější mining pooly. Přidat se do poolu je velmi jednoduché a intuitivní. Správci poolů mají své webové stránky, kde potenciální zájemce navedou, jak se stát součástí poolu. Mezi nejvýznamnější pooly patří AntPool (<https://antpool.com>), F2Pool (<https://f2pool.com>) a Poolin (<https://poolin.com>). Významnou část pak představuje skupina Unknown, ke které web blockchain.info uvádí, že se jedná o pooly, u kterých nebylo možné zjistit jejich původ.

4.6 Bitcoin

„Čistá peer-to-peer¹ verze elektronických peněz by umožnila zadávat online platby přímo od jedné strany k druhé, aniž by daná platba musela projít skrze finanční instituci. Digitální podpisy poskytují částečné řešení, ale hlavní benefity jsou ztraceny, pokud k zamezení dvojité úhrady je za potřebí důvěrné třetí strany. Navrhujeme řešení problému dvojité úhrady za pomoci peer-to-peer sítě. Síť časově označuje transakce pomocí hashování a vytváří z nich kontinuálně se rozšiřující řetězec založený na mechanismu proof-of-work, formuje tak záznam, který nemůže být změněn, aniž by došlo k opakovanému provedení PoW. Dlouhý řetězec nejenže představuje důkaz dané sekvence událostí, ale také důkaz, že vznikl za vynaložení určitého množství výpočetního výkonu. Dokud bude majorita výpočetního výkonu ovládána nezávislými uzly, kteří se neuchýlí ke spolupráci za účelem napadení sítě, vytvoří společně nejdelší řetězec a zamezí tak případným útokům. Síť sama o sobě vyžaduje minimální strukturu. Uzly mohou kdykoliv síť opustit a následně se zase vrátit s tím, že akceptují PoW řetězec z období, kdy byly pryč.“ (Nakamoto, 2008)

4.6.1 Satoshi Nakamoto

Satoshi Nakamoto je tvůrcem/tvůrci² Bitcoinu. Není zřejmé, zda se jedná o skutečné jméno, či o pseudonym. V roce 2008 představil Bitcoin whitepaper, ve kterém přednesl samotnou myšlenku Bitcoinu. Začátkem roku 2009 Satoshi vypustil zdrojový kód Bitcoinu a 3. ledna začal těžit bitcoiny. V počátcích Bitcoinu se těžby zúčastnilo velmi málo lidí a obtížnost těžby byla nízká. Nicméně tato úzká skupina nadšenců měla tak příležitost získat významné množství bitcoinu. Analýza blockchainu indikuje, že sám Satoshi vytěžil přibližně 1 milion bitcoinů. Překvapivě žádný z těchto bitcoinů nebyl doposud utracen, nicméně až (a pokud) Satoshi začne tyto bitcoiny utrácet, mohlo by dojít k odhalení jeho identity. Transakce v blockchainu jsou transparentní a pokud by došlo k pohybům bitcoinů na Satoshiho adresách, mohlo by tak dojít ke spojení adresy s osobou ve fyzickém světě. (Franco, 2014)

¹ „peer-to-peer“ – označení typu počítačových sítí, kde všechny uzly jsou si rovnocenné a jednotliví klienti spolu komunikují přímo bez existence centrálního uzlu – serveru. Na rozdíl od asymetrického modelu klient-server, v P2P s rostoucím množstvím uživatelů roste i přenosová kapacita sítě. Nevýhodou symetrie P2P je naopak obtížnost počátečního navázání komunikace. (Stroukal, 2021)

² Pro přehlednost budeme dále o Satoshi Nakamoto uvažovat jako o jednotlivci.

Zakladatel na internetových fórech uvedl, že na Bitcoinu pracoval již od roku 2007. Poté, co byl Bitcoin rozšířen, předal Nakamoto doménu bitcoin.org fanouškovi projektu a později hlavnímu vývojáři Gavinu Andresenovi a následně se odmlčel. Zajímavostí však je, že sám Nakamoto o sobě tvrdil, že mu tehdy bylo 34 a je Japonec, nicméně perfektně ovládal anglický jazyk a jeho komunikace se obešla bez jakýchkoliv japonských slov, a to i v samotném Bitcoin protokolu. Spekuluje se tedy, že se jedná o osobu/osoby z anglicky mluvící země – nikoliv však z USA, neboť v publikovaných textech byl špatně použit americký dialekt, naopak britský dialekt ovládal perfektně. (Stroukal, 2021)

Vznik decentralizovaného systému nebyla náhoda. Ze Satoshiho slov je zřejmé, že projekt vytvořil s předem jasným úmyslem. Sám totiž řekl: *„Myslím si, že v 90. letech se o kryptoměny v jakékoliv podobě zajímalo více lidí, ale po více než deseti letech neúspěšných systémů založených na důvěryhodných třetích stranách to považují za ztracenou věc. Doufám, že dokážou rozlišit, že nyní se poprvé pokoušíme o systém nezaložený na důvěře v třetí stranu.“* Poté ještě dodal: *„Překvapilo by mě, kdybychom za 10 let nějakým způsobem nepoužívali virtuální měny, když už víme, jak to udělat, a aby to nebylo nevyhnutelné, pokud by se důvěryhodná třetí strana dostala do úzkých.“* (Franco, 2014)

4.6.2 Co je Bitcoin?

Nejabstraktnější pohled na Bitcoin je takový, že Bitcoin je zkrátka pouze počítačový program. (Franco, 2014)

Bitcoin je virtuální měna založená na kryptografických principech, blockchainu a proof-of-work mechanismu v rámci distribuovaného a decentralizovaného prostředí. Ačkoli se v literatuře objevily návrhy na vývoj podobné měny využívající kryptografické techniky, zůstává Bitcoin první realizovanou kryptoměnou na světě. Vyřešením problému dvojí úhrady za pomoci využití decentralizované databáze, přinesl Nakamoto způsob přesouvání peněz, jenž byl doposud nemožný. Díky této schopnosti se Bitcoin stal jedinečným a představil tak zcela nové odvětví technologií. (Chowdhury, 2019)

Bitcoin představuje digitální peer-to-peer měnu – kryptoměnu. Jak již z podstaty kryptoměn plyne, za Bitcoinem³ nestojí žádná centrální autorita, která by ho regulovala nebo měla možnost vytvářet nové bitcoiny³, jak je tomu u konvenčních peněz. Nicméně i přesto bitcoin splňuje základní charakteristiky dobrých peněz. (Stroukal, 2021)

Definicí bitcoinu je mnoho – například protokol, digitální měna nebo také platforma. Bitcoin je kombinací peer-to-peer sítě, protokolů a softwaru, který usnadňuje vznik a využití digitální měny nazývané bitcoin. Uzly v této peer-to-peer síti navzájem komunikují prostřednictvím Bitcoin protokolu. (Bashir, 2018)

Tato virtuální měna však v sobě skrývá více tajemství. Bitcoinu se říká virtuální měna, protože ve skutečnosti neexistuje. Nemůžeme se ho dotknout, ani ho cítit, a i přesto má skutečnou hodnotu. Ve skutečnosti je bitcoin ještě více virtuální než digitální soubor. Je tak virtuální, že nemá existenci ani v digitálním světě. V našem počítači ani na serveru neexistuje žádný takový soubor, který bychom mohli nazvat bitcoinem. (Chowdhury, 2019)

Srdcem Bitcoinové sítě je databáze, v níž jsou uloženy transakce, k nimž došlo v minulosti a aktuální držitelé prostředků. Tato databáze se někdy nazývá účetní kniha (ledger), protože obsahuje záznamy o vlastnících finančních prostředků. Požadavky na finanční databázi se však liší od požadavků jiných aplikací, jako je sdílení souborů nebo systémy pro zasílání zpráv. Finanční databáze musí být zejména odolná vůči uživatelům, kteří se snaží své prostředky uhradit dvakrát, což se v případě Bitcoinu povedlo vyřešit. (Franco, 2014)

Nakamoto si Bitcoin představoval ze zcela jiné perspektivy. Jeho protokol zkoumá transakce, aby zjistil, kolik bitcoinů kdo vlastní. Od vzniku každého bitcoinu se jeho životní cyklus odehrává na stránkách účetní knihy známé jako blockchain, která uchovává záznamy o každé transakci a na jejímž základě se pak ověřuje, zda daný uživatel skutečně disponuje reálnými prostředky. (Chowdhury, 2019)

³ Bitcoin s velkým B na začátku odkazuje na Bitcoinový protokol, mezitímco bitcoin s malým b na začátku symbolizuje měnu. (Bashir, 2018)

Bitcoin vzniká těžbou. Jakmile těžaři potvrdí transakce a vytvoří blok, jeden těžař/skupina těžařů dostane jako odměnu určité množství bitcoinů – a tak vznikají nové bitcoiny. Od tohoto okamžiku, kdy nově vzniklé bitcoiny změní majitele – dojde ke transakci, těžaři zapíší tuto transakci do blockchainu a cyklus se opakuje. (Chowdhury, 2019)

Co Bitcoin není

Někteří kritici tvrdí, že Bitcoin je Ponziho schéma. To ovšem není pravda. V Ponziho schématu existuje centrální provozovatel, který vyplácí výnosy stávajícím investorům z přílivu nového kapitálu. V Bitcoinu především neexistuje žádný centrální provozovatel, který by mohl profitovat z přesunu prostředků. Za druhé neexistuje žádný mechanismus, který by odváděl prostředky z nových investic do výplaty stávajícím investorům. Jediné prostředky uznávané v Bitcoinovém protokolu jsou bitcoiny: protokol sám o sobě nemůže samovolně přesouvat prostředky od jednoho uživatele k druhému. Za třetí – nové investice do bitcoinu vždy odpovídá odprodej. Investoři, kteří vkládají prostředky do bitcoinů, obvykle operují prostřednictvím burzy, kde kupují bitcoiny od jiného investora, který svou investici prodává. Do bitcoinů tak žádná nová investice neplyne – množství kapitálu, které do bitcoinu přiteklo přesně odpovídá množství kapitálu, které z bitcoinu odteklo. (Franco, 2014)

4.6.3 Regulace

Každá část světa a mnohdy i jednotlivé státy přistupují k regulaci kryptoměn odlišně a svým vlastním způsobem. Z tohoto důvodu se bude následující kapitola týkat pouze významných světových trhů.

Spojené státy

Navzdory velkému počtu investorů do kryptoměn ve Spojených státech zatím země nevytvořila jasný regulační rámec pro tuto třídu aktiv. Komise pro cenné papíry (SEC) obvykle považuje kryptoměnu za cenný papír, zatímco Komise pro obchodování s komoditními futures (CFTC) označuje Bitcoin za komoditu a Ministerstvo financí za měnu. Burzy kryptoměn ve Spojených státech spadají pod regulační působnost zákona o

bankovním tajemství (Bank Secrecy Act) a musí se registrovat u FinCENu (Financial Crimes Enforcement Network). Musí také plnit povinnosti v oblasti boje proti praní špinavých peněz (AML) a boje proti financování terorismu (CFT). Daňový úřad (IRS) klasifikuje kryptoměny jako majetek podléhající zdanění daní z příjmu. V současné chvíli probíhá významný soudní spor mezi společností Ripple a Komisí pro cenné papíry a burzy (SEC). SEC má rovněž v úmyslu zažalovat přední burzy kryptoměn Coinbase pro další vyjasnění regulačních záležitostí.

(zdroj:<https://www.investopedia.com/cryptocurrency-regulations-around-the-world-5202122>)

Evropská unie

Kryptoměny jsou legální na většině území Evropské unie (EU), ačkoli jejich správa závisí na jednotlivých členských státech. Mezitím se zdanění v jednotlivých zemích EU také liší a pohybuje se od 0 do 50 %. V posledních letech vstoupily v platnost pátá směrnice EU proti praní špinavých peněz (5AMLD) a šestá směrnice EU proti praní špinavých peněz (6AMLD), které zpřísňují povinnosti v oblasti KYC (Know your customer)/CFT (Combating the financing terrorism) a standardní požadavky na reporting. V září 2020 navrhla Evropská komise nařízení o trzích s kryptoaktivy (MiCA) - rámec, který zvyšuje ochranu spotřebitelů, stanoví jasné chování v kryptografickém průmyslu a zavádí nové požadavky na udělování licencí.

(zdroj:<https://www.investopedia.com/cryptocurrency-regulations-around-the-world-5202122>)

Čínská lidová republika

Čína v průběhu roku 2021 stále intenzivněji zasahovala proti kryptoměnám. Čínské úřady opakovaně varovaly své obyvatele, aby se trhu s digitálními aktivy vyhýbali, a tvrdě potlačily těžbu v zemi i směnárny v Číně i v zahraničí. Dne 27. srpna Yin Youping, zástupce ředitele Úřadu pro ochranu práv finančních spotřebitelů Čínské lidové banky (PBoC), označil kryptoměny za spekulativní aktiva a varoval lidi, aby si "chránili své kapsy". Snahy o podkopání bitcoinu – decentralizované měny mimo kontrolu vlád a institucí – jsou do

značné míry považovány za pokus čínských úřadů o uvedení vlastní elektronické měny na trh. PBoC se chce stát jednou z prvních velkých centrálních bank na světě, která by zavedla vlastní digitální měnu, a tím by mohla důkladněji sledovat transakce svých obyvatel. Dne 24. září šla PBoC ještě dál a přímo zakázala transakce s kryptoměnami v zemi.

(zdroj:<https://www.euronews.com/next/2021/09/24/bitcoin-ban-these-are-the-countries-where-crypto-is-restricted-or-illegal2>)

Ruská federace

Kryptoměny sice nejsou v Rusku zakázané, ale proti jejich používání se vede konflikt. Rusko přijalo první zákony o regulaci kryptoměn v červenci 2020, které poprvé označily kryptoměny za majetek podléhající zdanění. Zákon, který vstoupil v platnost letos v lednu, také zakazuje ruským státním zaměstnancům vlastnit jakákoli kryptoaktivita. Ruský prezident Vladimir Putin opakovaně spojil kryptoměny s trestnou činností a vyzval k větší pozornosti zejména přeshraničním kryptografickým transakcím. V červenci generální prokurátor oznámil nový návrh legislativy, který by policii umožnil zabavit kryptoměny považované za nelegálně získané s odkazem na jejich využití při úplatkářství.

(zdroj:<https://www.euronews.com/next/2021/09/24/bitcoin-ban-these-are-the-countries-where-crypto-is-restricted-or-illegal2>)

4.7 Determinanty

4.7.1 Makroekonomické a finanční ukazatele

Finanční literatura poskytuje smíšené náznaky toho, jaké ekonomické ukazatele by mohly nejlépe sloužit jako konvenční determinanty ceny bitcoinu. Při tvorbě ceny bitcoinu hrají zejména důležitou roli tradiční tržní síly nabídky a poptávky, stejně jako atraktivita pro investory. (Vo, Chapman, Lee, 2021)

Skupina autorů ve své studii „*Machine learning model for Bitcoin Exchange rate prediction using economic and technology determinants*“ pracovala s následujícími ukazateli, jakožto hlavními makroekonomickými determinanty: **FTSE100** (Financial Times Stock Exchange 100 představuje 100 společností s nejvyšší tržní kapitalizací ve Velké Británii), **DJ30** (Dow Jones industrial average – 30 amerických společností, které patří mezi největší a nejvíce

obchodované), index volatility **VIX**, index Šangajského akciového trhu **SSE**, **cena ropy**, **cena zlata**, akciový index **S&P500** (index 500 společností s největší tržní kapitalizací na americkém akciovém trhu) a index **NASDAQ** (National Association of Securities Dealers Automated Quotations představuje akciový index 3900 společností kotovaných na americké burze z 39 zemí světa). (Chen, Xu, Jia, Gao, 2020)

Negativní korelace byla zjištěna mezi cenou bitcoinu a sazbou fondů amerického FEDu. Je tomu tak, protože pokud je bitcoin používán jako finanční aktivum, rostoucí úrokové sazby FEDu umožní tok finančních prostředků zpět na americký trh, a tím se sníží investice do bitcoinu. (Chen, Chen, Du, 2020)

Bouri, Molnár, Azzi, Roubaud a Hagfors (2017) použili index **FTSE100**, **americký dolarový index**, **DAX** (německý burzovní index Frankfurtské burzy) a **Nikkei 225** (japonský akciový index) k vytvoření portfolia s bitcoinem s využitím denních a týdenních pozorování. Zjistili, že index amerického dolaru nemá žádnou významnou korelaci s cenou Bitcoinu, a to ani denní, ani týdenní. Pozitivní korelaci zjištěnou u indexů **FTSE100** a **DAX** vysvětlili tím, že přestože investoři nemohou Bitcoin přímo hedgovat, mohou jej využít ke zvýšení diverzifikace portfolia. A konečně byl zjištěn významný negativní vztah s indexem **Nikkei 225** při použití denních pozorování, což naznačuje, že investoři v Japonsku mají tendenci používat Bitcoin jako zajištění portfolia. Baur et al. (2018) rovněž zjistili negativní korelaci mezi dolarovým indexem a bitcoinem. (Chen, Chen, Du, 2020)

Přestože je bitcoin mezinárodní kryptoměna, výše zmíněné finanční ukazatele z USA jsou spolehlivými zástupnými ukazateli, protože USA v současné době představují největší světovou ekonomiku.

4.7.2 Technologické (blockchainové) ukazatele

Největší rozdíl mezi bitcoinem a tradičními měnami spočívá v tom, že trh s bitcoinem buduje důvěru prostřednictvím blockchainu. (Chen, Xu, Jia, Gao, 2020)

Napříč mnoha studiemi se jako významné determinanty jeví samotné informace o blockchainové síti Bitcoinu. Jedná se převážně o následující faktory:

- Block size (velikost bloku) – velikost dat v blockchainové síti obsahující trvale zaznamenaná data.
- Confirmation time (doba potvrzení) – medián doby potřebné k dokončení decentralizované transakce a jejímu přidání do blockchainu za účelem úspěšného potvrzení.
- Difficulty (obtížnost) – obtížnost úspěšného vytěžení nových bloků.
- Hash rate – měřítko schopnosti těžební sítě zpracovávat data.
- Mining profitability (ziskovost těžby) – celková hodnota odměn a transakčních poplatků vyplácených těžářům.
- Average transaction fee (průměrný transakční poplatek) – průměrný poplatek za zpracování všech transakcí, které proběhnou během jednoho dne.
- Average transaction value (průměrná hodnota transakce) – průměrná hodnota získaná všemi transakcemi, které se uskuteční během jednoho dne.
- Transaction volume (objem transakcí) – počet transakcí uzavřených pro kupující a prodávající.
- Market capitalization (tržní kapitalizace) – hodnota vypočtená vynásobením ceny a nabízených bitcoinů v oběhu. (Chen, Xu, Jia, Gao, 2020)

5 Vlastní práce

Vlastní práce diplomové práce se zabývá ekonometrickým modelováním vývoje hodnoty bitcoinu. Během této fáze bylo navrženo několik modelů, které byly následně během procesu specifikace upraveny do finální podoby, která bude využita v následujících kapitolách. Z počátku byla snaha přijít s modelem, který by měl lineární funkční formu a vycházel z denních pozorování v absolutních hodnotách. Tato varianta se i přes implikaci dalších proměnných a jejich zpoždění ukázala jako neefektivní, a tím pádem bylo potřeba model znovu specifikovat. Dalším krokem bylo využití jiné funkční formy. I v tomto případě se kvadratická a kubická funkce ukázala jako nedostatečná. Nakonec byla zvolena funkce mocninná, kterou je možné za pomoci logaritmizace linearizovat a model tak odhadnout pomocí BMNČ. Nicméně zvolením zmíněné funkční formy specifikace modelu nebyla kompletní, neboť model i tak nesplňoval potřebné předpoklady o náhodné složce a nebyl by tak vhodný k aplikaci. V poslední fázi specifikace modelu byl celý model převeden do prvních diferencí a po zahrnutí faktoru času ve formě zpožděných proměnných se výsledný model ukázal, alespoň z pohledu testování předpokladů o náhodné složce, jako validní. Ve výsledném modelu jsou použity determinanty z řad akciových indexů, obchodovaných komodit, blockchainových ukazatelů, veřejného zájmu, a nakonec dummy proměnných představující geopolitické vlivy. Vstupní data vycházejí z týdenních pozorování v intervalu od 3. 11. 2017 – 29. 10. 2021. Model byl odhadnut za pomoci SW Gretl, který bude i následně použit k prognóze vývoje hodnoty bitcoinu.

5.1 Deklarace proměnných a očekávané vztahy

Tabulka 1 Deklarace proměnných

Označení	Označení (Gretl)	Název proměnné	Typ proměnné	Jednotky
y	ld_BTC	bitcoin	endogenní	USD
x ₁	const	konstanta	exogenní	-
x ₂	ld_miners_revenue	Odměna těžářů	exogenní	USD
x ₃	ld_hash_rate	Hash rate	exogenní	TH/s
x _{4(t-1)}	ETHER_1	Ethereum	exogenní zpožděná	USD
x ₅	dummy_inc	Dummy – vzrůst	exogenní dummy	-
x ₆	dummy_dec	Dummy – pokles	exogenní dummy	-

X _{7(t-2)}	ld_SP500_2	S&P500	exogenní zpožděná	body
X _{8(t-1)}	ld_ZLATO_1	Zlato	exogenní zpožděná	USD/1oz
X _{9(t-4)}	ld_ROPA_4	Ropa Brent	exogenní zpožděná	USD/barel
X _{10(t-2)}	ld_public_interest_2	Veřejný zájem	exogenní zpožděná	%
X ₁₁	ld_median_conf_time	medián potřebného času pro potvrzení transakce	exogenní	minuty
X _{12(t-1)}	ld_unique_addresses	počet unikátních adres využívaných v blockchainu	exogenní zpožděná	jednotky
X ₁₃	ld_Avg_block_size	průměrná velikost bloku v posledních 24 hodinách	exogenní	Mb
X ₁₄	ld_NIKKEI225	akciový index NIKKEI 225	exogenní	body
X ₁₅	ld_DAX	akciový index DAX	exogenní	body
X ₁₆	ld_FTSE100_1	akciový index FTSE100	exogenní zpožděná	body
X ₁₇	ld_total_btc_1	počet vytěžených bitcoinů	exogenní zpožděná	jednotky

Očekávané vztahy:

Vzhledem k tomu, že kryptoměny jsou relativně novou oblastí, neexistuje v současné době jednoznačná ekonomická teorie, která by se na tuto třídu aktiv dala jednoduše aplikovat. S ohledem na strukturu zvolených determinant lze konstatovat, že v případě akciových indexů a obchodovaných komodit se může jednat jak o komplement, tak i substitut, tím pádem může na bitcoin jeden akciový index působit negativně, druhý zas pozitivně. Vše záleží na pohledu jednotlivých investorů, kteří buď tedy mohou bitcoin držet za účelem diverzifikace portfolia, jiní zas bitcoin po určité době prodají a nemají jej ve svém portfoliu vůbec, a další vsadí vše na bitcoin a prodají konvenční investiční instrumenty. Nicméně u některých determinant (zejména z oblasti blockchainových ukazatelů) lze za použití logické úvahy vztahy působící na hodnotu bitcoinu odvodit.

Odměna těžařů

Zvýší/sníží-li se odměna těžařů, zvýší/sníží se hodnota bitcoinu.

Veřejný zájem

Zvýší/sníží-li se veřejný zájem, zvýší/sníží se hodnota bitcoinu.

Medián doby potřebné k potvrzení transakce

Zvýší/sníží-li se medián doby potřebné k potvrzení transakce, zvýší/sníží se hodnota bitcoinu.

Počet použitých unikátních adres v blockchainové síti

Zvýší/sníží-li se počet použitých unikátních adres, zvýší/sníží se hodnota bitcoinu.

Průměrná velikost bloku

Zvýší/sníží-li se průměrná velikost bloku, zvýší/sníží se hodnota bitcoinu.

Počet vytěžených bitcoinů

Zvýší-li se počet bitcoinů v oběhu, zvýší se hodnota bitcoinu – počet bitcoinů v oběhu nemůže zákonitě poklesnout.

Deskriptivní statistiky:

Obrázek 5 Deskriptivní statistiky

	Střední hodnota	Medián	S.D.	Min	Max
ld_BTC	0,01039	0,01319	0,1113	-0,4838	0,4093
ld_SP500	0,003078	0,005074	0,02569	-0,1623	0,1142
ld_DAX	0,0003872	0,0009604	0,02766	-0,2233	0,1035
ld_FTSE100	-0,0002856	0,0009569	0,02385	-0,1859	0,07592
ld_NIKKEI225	0,0009389	0,001226	0,02826	-0,1743	0,1582
ld_Avg_block_size	0,001149	0,001403	0,1058	-0,4110	0,4852
ld_median_conf_t~	-0,002281	0,0003801	0,2718	-1,018	0,7013
ld_miners_revenue	0,007616	0,01110	0,1749	-0,7393	0,4728
ld_unique_addres~	0,0009551	0,004047	0,07528	-0,2552	0,2726
ld_total_btc	0,0005583	0,0006220	0,0002124	0,0001947	0,0009876
ld_ZLATO	0,001964	0,001874	0,02460	-0,08093	0,1172
ld_ROPA	0,001796	0,006346	0,1282	-0,6789	1,290
ld_ETHER	0,01185	0,01382	0,1335	-0,6073	0,5102
ld_public_intere~	-0,0003284	0,0000	0,1951	-0,5754	0,8267
ld_hash_rate	0,01262	0,004246	0,1167	-0,3701	0,3357

(zdroj: vlastní zpracování)

Na obrázku č. 5 můžeme vidět deskriptivní statistiky zvolených proměnných. Je vhodné podotknout, že zobrazené hodnoty jsou již v logaritmických diferencích. Mezi prezentované deskriptivní statistiky patří střední hodnota, tedy průměr, medián, směrodatná odchylka, minimum a maximum.

5.2 Formulace ekonomického a ekonometrického modelu

Ekonomický model:

$$y = fce(x_1; x_2; x_{3(t-1)}; x_4; x_5; x_6; x_{7(t-2)}; x_{8(t-1)}; x_{9(t-4)}; x_{10(t-2)}; x_{11}; x_{12(t-1)}; x_{13}; x_{14}; x_{15}; x_{16(t-1)}; x_{17}$$

Ekonometrický model:

$$\beta_1 y_{1t} = \gamma_1 x_2^{\gamma_2} x_3^{\gamma_3} x_{3(t-1)}^{\gamma_3} x_4^{\gamma_4} x_5^{\gamma_5} x_6^{\gamma_6} x_7^{\gamma_7} x_{7(t-1)}^{\gamma_7} x_{7(t-2)}^{\gamma_7} x_8^{\gamma_8} x_{8(t-1)}^{\gamma_8} x_9^{\gamma_9} x_{9(t-1)}^{\gamma_9} x_{9(t-2)}^{\gamma_9} x_{9(t-3)}^{\gamma_9} x_{9(t-4)}^{\gamma_9} \\ \cdot x_{10}^{\gamma_{10}} x_{10(t-1)}^{\gamma_{10}} x_{10(t-2)}^{\gamma_{10}} x_{11}^{\gamma_{11}} x_{12}^{\gamma_{12}} x_{12(t-1)}^{\gamma_{12}} x_{13}^{\gamma_{13}} x_{14}^{\gamma_{14}} x_{15}^{\gamma_{15}} x_{15}^{\gamma_{15}} x_{16(t-1)}^{\gamma_{16}} x_{17}^{\gamma_{17}}$$

Během fáze specifikace modelu bylo nezbytné zahrnout i faktor času. Pro vybrané proměnné (viz ekonometrický model výše) byly použity různé řady zpoždění. Kritériem pro výběr vhodného zpoždění byla asymptotická p-hodnota a to tak, že řád zpoždění s nejvyšší p-hodnotou byl zvolen jako nejvhodnější. Na ostatní zpožděné proměnné byly uvaleny nulové restriktce a získán následující ekonometrický model ve tvaru mocninné funkce:

$$\beta_1 y_{1t} = \gamma_1 x_2^{\gamma_2} x_{3(t-1)}^{\gamma_3} x_4^{\gamma_4} x_5^{\gamma_5} x_6^{\gamma_6} x_{7(t-2)}^{\gamma_7} x_{8(t-1)}^{\gamma_8} x_{9(t-4)}^{\gamma_9} x_{10(t-2)}^{\gamma_{10}} x_{11}^{\gamma_{11}} x_{12(t-1)}^{\gamma_{12}} x_{13}^{\gamma_{13}} x_{14}^{\gamma_{14}} x_{15}^{\gamma_{15}} x_{16(t-1)}^{\gamma_{16}} x_{17}^{\gamma_{17}}$$

Aby bylo možné odhadnout parametry BMNČ, musíme nejdříve ekonometrický model ve tvaru mocninné funkce linearizovat použitím přirozeného logaritmu. Po provedení linearizace získáme následující rovnici:

$$\ln y_{1t} = \ln \gamma_1 + \gamma_2 \ln x_2 + \gamma_3 \ln x_{3(t-1)} + \gamma_4 \ln x_4 + \gamma_5 \ln x_5 + \gamma_6 \ln x_6 + \gamma_7 \ln x_{7(t-2)} + \gamma_8 \ln x_{8(t-2)} \\ + \gamma_9 \ln x_{9(t-4)} + \gamma_{10} \ln x_{10(t-2)} + \gamma_{11} \ln x_{11} + \gamma_{12} \ln x_{12(t-1)} + \gamma_{13} \ln x_{13} + \gamma_{14} \ln x_{14} \\ + \gamma_{15} \ln x_{15} + \gamma_{16} \ln x_{16(t-1)} + \gamma_{17} \ln x_{17}$$

5.3 Odhad parametrů modelu

Před samotným odhadem parametrů modelu je nejprve potřeba prověřit, zda jsou vstupní časové řady stacionární. Stacionaritu lze otestovat pomocí Dickey-Fullerova testu, který je vyjádřen vztahy (3.4 – 3.7).

5.3.1 Stacionarita časových řad a multikolinearita

Předpoklad stacionarity bude otestován rozšířeným Dickey-Fuller testem, který probíhá dle vztahů (3.4 – 3.7). Testovací statistika a p-hodnota je pro přehlednost zaznamenána do následující tabulky č. 2. Tabulka rovněž obsahuje vyhodnocení testu. Pro vyhodnocení testu poslouží p-hodnota a samotné vyhodnocení je pak následující: je-li p-hodnota nižší než 0,05 – nulová hypotéza se zamítá, je-li naopak p-hodnota vyšší než 0,05 – přijímáme nulovou hypotézu.

Stanovení hypotéz:

H_0 – časová řada je nestacionární

H_1 – časová řada je stacionární

Tabulka 2 Stacionarita časových řad

Proměnná	t-statistika	p-hodnota	Vyhodnocení
ld_miners_revenue	-17,2118	1,787e-029	Stacionární
ld_ETHER	-14,3936	1,132e-025	Stacionární
ld_hash_rate	-16,7262	5,582e-052	Stacionární
ld_SP500	-17,0359	2,587e-029	Stacionární
ld_ZLATO	-15,1895	5,576e-044	Stacionární
ld_ROPA	-14,2731	2,47e-039	Stacionární
ld_public_interest	-12,6979	1,17e-031	Stacionární
ld_median_conf_time	-16,5916	2,853e-051	Stacionární
ld_unique_addresses	-19,1012	1,686e-030	Stacionární
ld_Avg_block_size	-15,4459	2,675e-045	Stacionární
ld_NIKKEI225	-16,2727	1,714e-028	Stacionární
ld_DAX	-14,244	2,104e-025	Stacionární
ld_FTSE100	-9,94661	1,394e-019	Stacionární
ld_total_btc	-4,19104	0,004549	Stacionární

Všechny proměnné splňují předpoklad o stacionaritě. Posledním krokem před odhadem parametrů je vyloučení možnosti výskytu vysoké / perfektní multikolinearity mezi zvolenými determinanty. Multikolinearitu lze detekovat pomocí korelační matice, kterou získáme ze SW Gretl. Samotný test multikolinearity se pak řídí dle vztahů (3.30 – 3.31).

Na následujícím obrázku č. 6 můžeme vidět korelační matici. Relativně vysoká multikolinearita se vyskytuje mezi proměnnými ld_DAX a ld_FTSE100 (0,8107). Hodnotu 0,8 lze považovat za vysokou multikolinearitu, nicméně názor na tuto hranici se napříč literaturou liší a někteří autoři považují vysokou multikolinearitu až od hranice 0,9. Pro účely této diplomové práce budeme považovat za vysokou multikolinearitu hodnotu 0,9 a více. Tím pádem tedy lze konstatovat, že mezi proměnnými se nevyskytuje těsná korelační závislost a můžeme tak přejít k samotnému odhadu parametrů.

Obrázek 6 Korelační matice

Korelační koeficienty, za použití pozorování 2017-11-10 - 2021-10-29
 5% kritická hodnota (oboustranná) = 0,1361 pro n = 208

ld_miners_reve~	ld_ETHER	ld_hash_rate	ld_SP500	
1,0000	0,5043	0,6758	0,2264	ld_miners_reve~
	1,0000	0,1419	0,2654	ld_ETHER
		1,0000	0,1963	ld_hash_rate
			1,0000	ld_SP500
ld_ZLATO	ld_ROPA	ld_public_inte~	ld_median_conf~	
-0,0051	0,1329	0,0650	-0,4167	ld_miners_reve~
0,1396	0,0368	0,2465	-0,0595	ld_ETHER
-0,0162	0,1737	-0,0300	-0,5619	ld_hash_rate
0,1315	0,2443	0,0593	-0,1437	ld_SP500
1,0000	-0,3680	-0,0975	-0,0268	ld_ZLATO
	1,0000	-0,0004	-0,1021	ld_ROPA
		1,0000	0,0078	ld_public_inte~
			1,0000	ld_median_conf~
ld_unique_addr~	ld_Avg_block_s~	ld_NIKKEI225	ld_DAX	
0,4034	-0,3587	0,2737	0,3036	ld_miners_reve~
0,2868	0,0008	0,2272	0,3817	ld_ETHER
0,1585	-0,4711	0,1827	0,1257	ld_hash_rate
0,1701	-0,1054	0,7152	0,7125	ld_SP500
0,0655	0,0541	0,0472	0,1299	ld_ZLATO
-0,0700	-0,1391	0,1836	0,1489	ld_ROPA
0,1402	0,0867	0,0056	-0,0338	ld_public_inte~
-0,0085	0,5532	-0,1845	-0,1048	ld_median_conf~
1,0000	0,0749	0,1709	0,2669	ld_unique_addr~
	1,0000	-0,1113	-0,1562	ld_Avg_block_s~
		1,0000	0,7619	ld_NIKKEI225
			1,0000	ld_DAX
ld_FTSE100	ld_total_btc			
0,2918	-0,0358	ld_miners_reve~		
0,3423	-0,0676	ld_ETHER		
0,1457	0,0789	ld_hash_rate		
0,7219	-0,0332	ld_SP500		
0,0489	0,0008	ld_ZLATO		
0,2151	0,0150	ld_ROPA		
-0,0073	0,0224	ld_public_inte~		
-0,1704	0,0068	ld_median_conf~		
0,1820	-0,0702	ld_unique_addr~		
-0,1574	0,0004	ld_Avg_block_s~		
0,7250	-0,0751	ld_NIKKEI225		
0,8107	-0,0725	ld_DAX		
1,0000	-0,0507	ld_FTSE100		
	1,0000	ld_total_btc		

(zdroj: vlastní zpracování)

5.3.2 Odhad parametrů

Parametry budou odhadnuty běžnou metodou nejmenších čtverců. Odhad probíhá dle vztahu (3.9).

Obrázek 7 Odhad parametrů modelu

Model 259: OLS, za použití pozorování 2017-12-08:2021-10-29 (T = 204)
 Závisle proměnná: ld_BTC

	koeficient	směr. chyba	t-podíl	p-hodnota	
const	-0,00691585	0,0150184	-0,4605	0,6457	
ld_miners_revenue	0,525984	0,0353259	14,89	1,40e-033	***
ld_ETHER_1	-0,0871421	0,0319469	-2,728	0,0070	***
ld_hash_rate	-0,409187	0,0534946	-7,649	1,04e-012	***
Dummy_inc	0,0220538	0,0105469	2,091	0,0379	**
Dummy_dec	-0,0390399	0,0109672	-3,560	0,0005	***
ld_SP500_2	0,222767	0,148082	1,504	0,1342	
ld_ZLATO_1	-0,265751	0,157153	-1,691	0,0925	*
ld_ROPA_4	-0,0489655	0,0307678	-1,591	0,1132	
ld_public_inte~_2	0,0405074	0,0195717	2,070	0,0399	**
ld_median_conf_t~	0,0212635	0,0190467	1,116	0,2657	
ld_unique_addr~_1	0,106289	0,0526241	2,020	0,0448	**
ld_Avg_block_size	0,111408	0,0444038	2,509	0,0130	**
ld_NIKKEI225	-0,422253	0,214653	-1,967	0,0506	*
ld_DAX	0,676114	0,225876	2,993	0,0031	***
ld_FTSE100_1	0,433750	0,170304	2,547	0,0117	**
ld_total_btc_1	36,6474	20,4188	1,795	0,0743	*
Střední hodnota závisle proměnné		0,008555			
Sm. odchylka závisle proměnné		0,110018			
Součet čtverců reziduí		0,598878			
Sm. chyba regrese		0,056591			
Koeficient determinace		0,756266			
Adjustovaný koeficient determinace		0,735411			
F(16, 187)		36,26429			
P-hodnota (F)		1,14e-48			
Logaritmus věrohodnosti		305,2799			
Akaikovo kritérium		-576,5599			
Schwarzovo kritérium		-520,1518			
Hannan-Quinnovo kritérium		-553,7418			
rho (koeficient autokorelace)		-0,106404			
Durbin-Watsonova statistika		2,207641			

(zdroj: vlastní zpracování)

Před samotným zápisem modelu do rovnice je zapotřebí odlogaritmovat konstantu a dummy proměnné. Odlogaritmování probíhá pomocí Eulerova čísla, které se umocní hodnotou odhadnutého parametru.

Konstanta:

$$\ln \gamma_1 = -0,00691585$$

$$\gamma_1 = e^{-0,00691585}$$

$$\gamma_1 = 0,993108$$

Dummy_inc:

$$\ln\gamma_5 = 0,0220538$$

$$\gamma_5 = e^{0,0220538}$$

$$\gamma_5 = 1,022299$$

Dummy_dec:

$$\ln\gamma_6 = -0,0390399$$

$$\gamma_6 = e^{-0,0390399}$$

$$\gamma_6 = 0,961712$$

Zápis modelu ve tvaru mocninné funkce:

y

$$= 0,99x_2^{0,525}x_{3(t-1)}^{-0,087}x_4^{-0,409}1,02x_50,96x_6x_7^{0,222}x_{8(t-1)}^{-0,266}x_{9(t-4)}^{-0,049}x_{10(t-2)}^{0,045}x_{11}^{0,021}x_{12(t-1)}^{0,106}x_{13}^{0,111}x_{14}^{-0,422}x_{15}^{0,676}x_{16(t-1)}^{0,434}x_{17}^{36,647}$$

5.3.3 Ekonomická verifikace a interpretace odhadnutých parametrů

Vzhledem k tomu, že získaný model pracuje s prvními diferencemi, je potřeba tento fakt zohlednit při interpretaci výsledných parametrů, a tedy interpretovat získané výsledky jako změnu ze změny. Při interpretaci je nutné rovněž vzít v potaz, že se jedná o mocninou funkci a parametry tak vyjadřují relativní působení na vysvětlovanou proměnnou. Exaktní interpretace by tedy zněla následovně: „jednoprocentní změna změny vysvětlující proměnné x_n vyvolá γ_n procentní změnu změny vysvětlované proměnné“. Nicméně pro přehlednost a lepší čtivost budou parametry (vyjma konstanty a dummy proměnných) interpretovány, jako by se jednalo o absolutní (napozorované) hodnoty.

$$\text{const} = 0,993108$$

Pokud budou všechny proměnné v modelu rovny nule, změna ze změny hodnoty bitcoinu bude 0,993108 USD, CP.

$$\text{ld_miners_revenue} = 0,525984$$

Vzroste-li odměna těžařům o jedno procento, vzroste hodnota bitcoinu o 0,525984 %, CP.

ld_ETHER_1 = -0,0871421

Vzroste-li hodnota Ethera v předcházejícím období o jedno procento, poklesne hodnota bitcoinu o 0,087142 %, CP.

ld_hash_rate = -0,409187

Vzroste-li objem hash ratu o jedno procento, poklesne hodnota bitcoinu o 0,409187 %, CP.

dummy_inc = 1,022299

Nastane-li geopolitická událost vedoucí ke zvýšení hodnoty bitcoinu, změna ze změny hodnoty bitcoinu tak bude 1,022299 USD, CP.

dummy_dec = 0,961712

Nastane-li geopolitická událost vedoucí ke snížení hodnoty bitcoinu, změna ze změny hodnoty bitcoinu tak bude 0,961712 USD, CP. Směr působení tohoto parametru je v kontradikci s očekáváním. Nicméně to je zapříčiněno matematickou úpravou – linearizací odhadnutého parametru, jehož hodnota je tak nízká, že po umocnění Eulerova čísla získaným parametrem vyjde kladná hodnota. Prognózu, která bude předmětem dalších kapitol, tato skutečnost neovlivní, neboť vstupní data pro prognózu budou zlogaritmována a dosazena do SW gretl.

ld_SP500_2 = 0,222767

Vzroste-li hodnota akciového indexu SP500 v t-2 o jedno procento, vzroste hodnota bitcoinu o 0,222767 %, CP.

ld_ZLATO_1 = -0,265751

Vzroste-li hodnota zlata v předcházejícím období o jedno procento, poklesne hodnota bitcoinu o 0,265751 %, CP.

ld_ROPA_4 = -0,0489655

Vzroste-li hodnota ropy v t-4 o jedno procento, poklesne hodnota bitcoinu o 0,0489655 %, CP.

ld_public_interest_2 = 0,0405074

Vzroste-li veřejný zájem v t-2 o jedno procento, vzroste hodnota bitcoinu o 0,0405074 %, CP.

ld_median_conf_time = 0,0212635

Vzroste-li doba potřebná pro potvrzení transakce o jedno procento, vzroste hodnota bitcoinu o 0,0212635 %, CP.

ld_unique_addresses_1 = 0,106289

Vzroste-li počet používaných unikátních adres v předcházejícím období o jedno procento, vzroste hodnota bitcoinu o 0,106289 %, CP.

ld_Avg_block_size = 0,111408

Vzroste-li průměrná hodnota velikosti jednoho bloku v blockchainové síti o jedno procento, vzroste hodnota bitcoinu o 0,111408 %, CP.

ld_NIKKEI225 = -0,422253

Vzroste-li hodnota akciového indexu NIKKEI225 o jedno procento, poklesne hodnota bitcoinu o 0,422253 %, CP.

ld_DAX = 0,676114

Vzroste-li hodnota akciového indexu DAX o jedno procento, vzroste hodnota bitcoinu o 0,676114 %, CP.

ld_FTSE100_1 = 0,433750

Vzroste-li hodnota akciového indexu FTSE100 v předcházejícím období o jedno procento, vzroste hodnota bitcoinu o 0,433750 %, CP.

ld_total_btc_1 = 36,6474

Vzroste-li celkový počet vytěžených bitcoinů v předcházejícím období o jedno procento, vzroste cena bitcoinu o 36,474 %, CP.

Ekonomická verifikace je více méně v souladu s očekáváním. Výjimkou je akorát dummy proměnná na pokles hodnoty bitcoinu, nicméně v tomto případě se jedná spíše o problém způsobený matematickou úpravou, v samotném modelu je směr působení této proměnné správný. Jak již bylo zmíněno dříve, tak vzhledem k nedostatečné ekonomické teorii k tomuto tématu je spíše vhodné se nad získanými výstupy zamyslet a posoudit tak směr a intenzitu působení jednotlivých parametrů. Co se týče akciových indexů, tak některé působí na bitcoin pozitivně, jiné negativně – to je dáno přístupem jednotlivých investorů na daných trzích, ze kterých jsou akciové indexy kalkulovány. V případě tradičních obchodovaných komodit (zlato a ropa) můžeme vidět, že obě zmíněné komodity jsou ve vztahu k bitcoinu jasnými substituty. Lze tedy konstatovat, že pro určitou skupiny investorů nahradil bitcoin tradiční komodity a lze jej tak, alespoň z tohoto pohledu, považovat za tzv. „digitální zlato“. V případě blockchainových ukazatelů a proměnné veřejného zájmu jsou odhadnuté parametry v souladu s původními očekáváním uvedenými v kapitole č. 4.1.

5.3.4 Statistická verifikace

Statistická verifikace odhadnutých parametrů probíhá dle vztahu (3.20). Použitý SW Gretl poskytne výstup, z něhož lze na první pohled určit, zda je daný parametr významný či nikoliv. Hodnoty z obrázku č. 7 budou převedeny do následující tabulky, která bude rovněž obsahovat i vyhodnocení testu. Zda je parametr významný lze určit podle počtu hvězdiček (*) za každým odhadnutým parametrem. Jedna hvězdička symbolizuje, že parametr je významný na hladině významnosti $\alpha = 0,1$, v případě dvou hvězdiček je parametr významný na hladině významnosti $\alpha = 0,05$, jsou-li za parametrem tři hvězdičky, parametr je významný na hladině významnosti $\alpha = 0,01$. Není-li za parametrem hvězdička žádná, parametr je statisticky nevýznamný. Statistická významnost parametrů se dá rovněž vyhodnotit podle p-hodnoty a to tak, že se vypočtená p-hodnota porovná s hladinou významnosti α . Je-li p-hodnota menší než zvolená hladina významnosti α , pak je parametr statisticky významný na zvolené hladině významnosti.

Tabulka 3 Statistická verifikace odhadnutých parametrů

Proměnná	p-hodnota	***	vyhodnocení
const	0,6457	-	statisticky nevýznamná
ld_miners_revenue	1,40e-033	***	statisticky významný na $\alpha = 0,01$
ld_ETHER_1	0,0070	***	statisticky významný na $\alpha = 0,01$
ld_hash_rate	1,04e-012	***	statisticky významný na $\alpha = 0,01$
dummy_inc	0,0379	**	statisticky významný na $\alpha = 0,05$
dummy_dec	0,0005	***	statisticky významný na $\alpha = 0,01$
ld_SP500_2	0,1342	-	statisticky nevýznamný
ld_ZLATO_1	0,0925	*	statisticky významný na $\alpha = 0,1$
ld_ROPA_4	0,1132	-	statisticky nevýznamný
ld_public_interest_2	0,0399	**	statisticky významný na $\alpha = 0,05$
ld_median_conf_time	0,2657	-	statisticky nevýznamný
ld_unique_addresses_1	0,0448	**	statisticky významný na $\alpha = 0,05$
ld_Avg_block_size	0,0130	**	statisticky významný na $\alpha = 0,05$
ld_NIKKEI225	0,0506	*	statisticky významný na $\alpha = 0,1$
ld_DAX	0,0031	***	statisticky významný na $\alpha = 0,01$
ld_FTSE100_1	0,0117	**	statisticky významný na $\alpha = 0,05$
ld_total_btc_1	0,0743	*	statisticky významný na $\alpha = 0,1$

Z výše uvedené tabulky můžeme vidět, že statisticky nevýznamné jsou parametry pro akciový index SP500, ropu, medián doby potřebné pro potvrzení transakce a konstanta. O statistické významnosti na hladině významnosti $\alpha = 0,01$ můžeme uvažovat v případě parametrů pro proměnné odměna těžařů, Ethereum, hash rate, dummy proměnná na pokles hodnoty a akciový index DAX. Na hladině významnosti $\alpha = 0,05$ jsou pak významné parametry proměnných veřejného zájmu, celkového počtu unikátních adres, průměrné velikosti jednoho bloku v blockchainové síti, akciového indexu FTSE100 a dummy proměnné symbolizující geopolitické vlivy zapříčiňující vzrůst hodnoty bitcoinu. Co se týče

nejnižší hranice $\alpha = 0,1$, tak na této hladině významnosti ještě můžeme přijmout parametry proměnných Zlato, akciového indexu NIKKEI225 a celkového počtu vytěžených bitcoinů.

Součástí statistické verifikace je i ověření, na kolik % jsou změny ve vysvětlované proměnné vysvětlovány zvolenými determinanty. K tomu poslouží adjustovaný koeficient determinace, jehož hodnotu lze získat dle vztahu (3.15). Z obrázku č. 7 můžeme vidět, že adjustovaný koeficient determinace nabývá hodnoty 0,735411, což udává, že změny ve vysvětlované proměnné jsou ze 73,5411 % vysvětlovány právě změnami zvolených vysvětlujících proměnných.

5.3.5 Ekonometrická verifikace

Heteroskedasticita:

Pro otestování, zda se v modelu nevyskytuje heteroskedasticita použijeme Whiteův test, který je dán vztahy (3.21 – 3.22). K vyhodnocení testu poslouží asymptotická p-hodnota, která představuje nejnižší přípustnou hladinu k přijetí nulové hypotézy.

H_0 – není zde heteroskedasticita

H_1 – je zde heteroskedasticita

Obrázek 8 Test heteroskedasticity

```
Whiteův test heteroskedasticity -  
  Nulová hypotéza: není zde heteroskedasticita  
  Testovací statistika: LM = 172,847  
  s p-hodnotou = P(Chí-kvadrát(150) > 172,847) = 0,0975672
```

(zdroj: vlastní zpracování)

$0,0975672 > 0,05$

$p > \alpha$

Z provedeného testu vyplývá, že nelze zamítnout nulovou hypotézu – v modelu se nevyskytuje heterosekdasticita, a tím pádem odhadnuté parametry jsou nestranné, nejlepší a konzistentní.

Autokorelace reziduí:

Testování předpokladu o (ne)autokorelovatelnosti reziduí se provádí za pomoci Breusch-Godfreyho testu, který je vyjádřen vztahy (3.26 – 3.28). Vyhodnocení testu probíhá, jako tomu bylo v případě testu heteroskedasticity, opět tedy pomocí p-hodnoty.

H_0 – žádná autokorelace

H_1 – autokorelace je přítomna

Obrázek 9 Test autokorelace reziduí

```
LM test pro autokorelaci až do řádu 1 -  
  Nulová hypotéza: žádná autokorelace  
  Testovací statistika: LMF = 2,51546  
  s p-hodnotou = P(F(1, 186) > 2,51546) = 0,114433  
LM test pro autokorelaci až do řádu 2 -  
  Nulová hypotéza: žádná autokorelace  
  Testovací statistika: LMF = 1,32667  
  s p-hodnotou = P(F(2, 185) > 1,32667) = 0,267871  
LM test pro autokorelaci až do řádu 3 -  
  Nulová hypotéza: žádná autokorelace  
  Testovací statistika: LMF = 0,949414  
  s p-hodnotou = P(F(3, 184) > 0,949414) = 0,417921  
LM test pro autokorelaci až do řádu 4 -  
  Nulová hypotéza: žádná autokorelace  
  Testovací statistika: LMF = 2,02043  
  s p-hodnotou = P(F(4, 183) > 2,02043) = 0,0933786  
LM test pro autokorelaci až do řádu 5 -  
  Nulová hypotéza: žádná autokorelace  
  Testovací statistika: LMF = 1,61486  
  s p-hodnotou = P(F(5, 182) > 1,61486) = 0,158176  
LM test pro autokorelaci až do řádu 6 -  
  Nulová hypotéza: žádná autokorelace  
  Testovací statistika: LMF = 1,60581  
  s p-hodnotou = P(F(6, 181) > 1,60581) = 0,147835  
LM test pro autokorelaci až do řádu 7 -  
  Nulová hypotéza: žádná autokorelace  
  Testovací statistika: LMF = 1,38375  
  s p-hodnotou = P(F(7, 180) > 1,38375) = 0,214621  
LM test pro autokorelaci až do řádu 8 -  
  Nulová hypotéza: žádná autokorelace  
  Testovací statistika: LMF = 1,27884  
  s p-hodnotou = P(F(8, 179) > 1,27884) = 0,257097  
LM test pro autokorelaci až do řádu 9 -  
  Nulová hypotéza: žádná autokorelace  
  Testovací statistika: LMF = 1,21087  
  s p-hodnotou = P(F(9, 178) > 1,21087) = 0,290865  
LM test pro autokorelaci až do řádu 10 -  
  Nulová hypotéza: žádná autokorelace  
  Testovací statistika: LMF = 1,14178  
  s p-hodnotou = P(F(10, 177) > 1,14178) = 0,333732
```

(zdroj: vlastní zpracování)

Autokorelace byla testována až do řádu 10 a ve všech případech p-hodnota převyšuje hladinu významnosti $\alpha = 0,05$. V modelu se tedy nevyskytuje autokorelace reziduí a náhodná složka tak není závislá na svých zpožděných hodnotách.

Normalita reziduí:

Posledním předpokladem, který budeme testovat, je, zda náhodná složka splňuje normální rozdělení. K otestování normality náhodné složky využijeme Jacque-Bera test, který je dán vztahy (3.33 – 3.34). Stejně jako tomu bylo v předcházejících dvou případech, i zde k vyhodnocení testu použijeme p-hodnotu.

H_0 – náhodná složka je normálně rozdělena

H_1 – náhodná složka není normálně rozdělena

Obrázek 10 Test normality reziduí

```
Test normality reziduí -  
  Nulová hypotéza: chyby jsou normálně rozdělené  
  Testovací statistika: Chí-kvadrát (2) = 5,46367  
  s p-hodnotou = 0,0650998
```

(zdroj: vlastní zpracování)

$0,0650998 > 0,05$

$p > \alpha$

P-hodnota převyšuje hladinu významnosti α – nulovou hypotézu nelze zamítnout. Náhodná složka tedy splňuje předpoklad o normálním rozdělení.

5.3.6 Aplikace modelu

Po úspěšné fázi verifikace modelu přichází na řadu jeho aplikace. Výsledný model bude v následujících kapitolách aplikován prostřednictvím simulace scénářů s využitím koeficientů pružnosti a na závěr bude provedena i prognóza ex-post a ex-ante.

Simulace definovaných scénářů s využitím koeficientů pružnosti:

V případě mocninné funkce vyjadřují odhadnuté parametry koeficient pružnosti. To lze jednoduše ověřit dle vztahu (3.35). Simulace scénářů bude vycházet z posledního známého období při odhadu modelu, tedy 29.10.2021. Při simulaci scénářů je nutné brát v potaz, že se celý model nachází ve stavu prvních diferencí. I v tomto případě se tedy bude jednat o změnu ze změny, nikoliv o absolutní hodnoty. Pro přehlednost a lepší čtivost budeme však uvažovat o absolutních změnách hodnoty, jako tomu bylo v případě interpretace odhadnutých parametrů. Exaktní zadání simulace by znělo následovně: „*jak se změní změna hodnoty bitcoinu v případě, že se změna změny proměnné x_n změní o y %?*“. Odpověď pak na tuto otázku by zněla následovně: „*Změní-li se změna změny o y %, změní se změna změny hodnoty bitcoinu o z %*“. Poslední známá změna hodnoty bitcoinu tj. 29.10.2021 činila 1570,4 USD. Všechny definované scénáře budou tvořeny za podmínek ceteris paribus.

Jak se změní hodnota bitcoinu v případě, že proměnná odměna těžařům vzroste o 10 %, CP?

$$0,526 * 10 = 5,26 \%$$

Vzroste-li proměnná x_2 o 10 %, vzroste hodnota bitcoinu o 5,26 %, CP. Poslední známá hodnota proměnné x_2 činí 5 189 664 USD (jedná se o změnu oproti hodnotě z 22.10.2021). Nová hodnota této proměnné pak představuje 5 708 631 USD. V takovém případě by pak hodnota bitcoinu (změna hodnoty bitcoinu oproti 22.10.2021) činila 1 653 USD.

Jak se změní hodnota bitcoinu v případě, že se hodnota Ethera v předcházejícím období zvýší o 10 %, CP?

$$-0,087 * 10 = -0,87 \%$$

Zvýší-li se hodnota Ethera v předcházejícím období o 10 %, poklesne hodnota bitcoinu o 0,87 %. Ethereum v předcházejícím období dosáhlo hodnoty 103,86 USD. Po 10% nárůstu pak představuje hodnota Ethera 114,25 USD, hodnota bitcoinu poklesne na 1 556,74 USD.

Jak se změní hodnota bitcoinu, zvýší-li se hodnota proměnné hash rate o 10 %, CP?

$$-0,409 * 10 = -4,09 \%$$

Vzroste-li hodnota hash rate o 10 %, tj. na 14 275 754,46 TH/s, poklesne hodnota bitcoinu o 4,09 %, tj. na 1 506,17 USD.

Jak se změní hodnota bitcoinu, vzroste-li hodnota akciového indexu S&P500 v t-2 o 10 %, CP?

$$0,223 * 10 = 2,23 \%$$

Vzroste-li hodnota akciového indexu S&P500 v t-2 o 10 %, tj. na 88,033, zvýší-se hodnota bitcoinu o 2,23 % na 1 605,42 USD.

Jak se změní hodnota bitcoinu, dojde-li k nárůstu hodnoty zlata v předcházejícím období o 10 %, CP?

$$-0,266 * 10 = -2,66 \%$$

Dojde-li k nárůstu hodnoty zlata o 10 % v předcházejícím období, tj. na 30,8 USD, hodnota bitcoinu poklesne o 2,66 % na 1 528,63 USD.

Jak se změní hodnota bitcoinu, vzroste-li hodnota ropy v t-4 o 10 %, CP?

$$-0,049 * 10 = -0,49 \%$$

Zvýšila-by se hodnota ropy v t-4 o 10 % tj. na 0,341, poklesla by hodnota bitcoinu o 0,49 % na 1 562,7 USD.

Jak se změní hodnota bitcoinu, zvýší-li se počet unikátních adres v předcházejícím období o 10 %, CP?

$$0,106 * 10 = 1,06 \%$$

Byl by počet unikátních adres v předcházejícím období vyšší o 10 % tj. 11 380, hodnota bitcoinu by vzrostla o 1,06 % na 1587,05 USD.

Jak se změní hodnota bitcoinu, vzroste-li hodnota akciového indexu DAX o 10 %, CP?

$$0,676 * 10 = 6,76 \%$$

Zvýší-li se hodnota akciového indexu DAX o 10 % tj. 201,179, hodnota bitcoinu vzroste o 6,76 % na 1 676,56 USD.

Prognóza ex-post:

Před samotnou prognózou ex-ante je vhodné nejprve provést prognózu ex-post, jejímž cílem je otestovat prognostické předpoklady získaného modelu. V případě, že model poskytuje přesné „předpovědi“ minulosti, lze očekávat, že bude poskytovat i dobré předpovědi budoucnosti. Prognóza ex-post funguje na bázi dosazení skutečných hodnot do výsledné rovnice modelu a jejich porovnání se skutečností. Na obrázku č. 11 můžeme vidět prognózu ex-post. Vzhledem k délce časové řady bude na obrázku č. 11 zobrazen pouze začátek a konec sledovaného období. Celá prognóza ex-post bude uvedena v příloze diplomové práce.

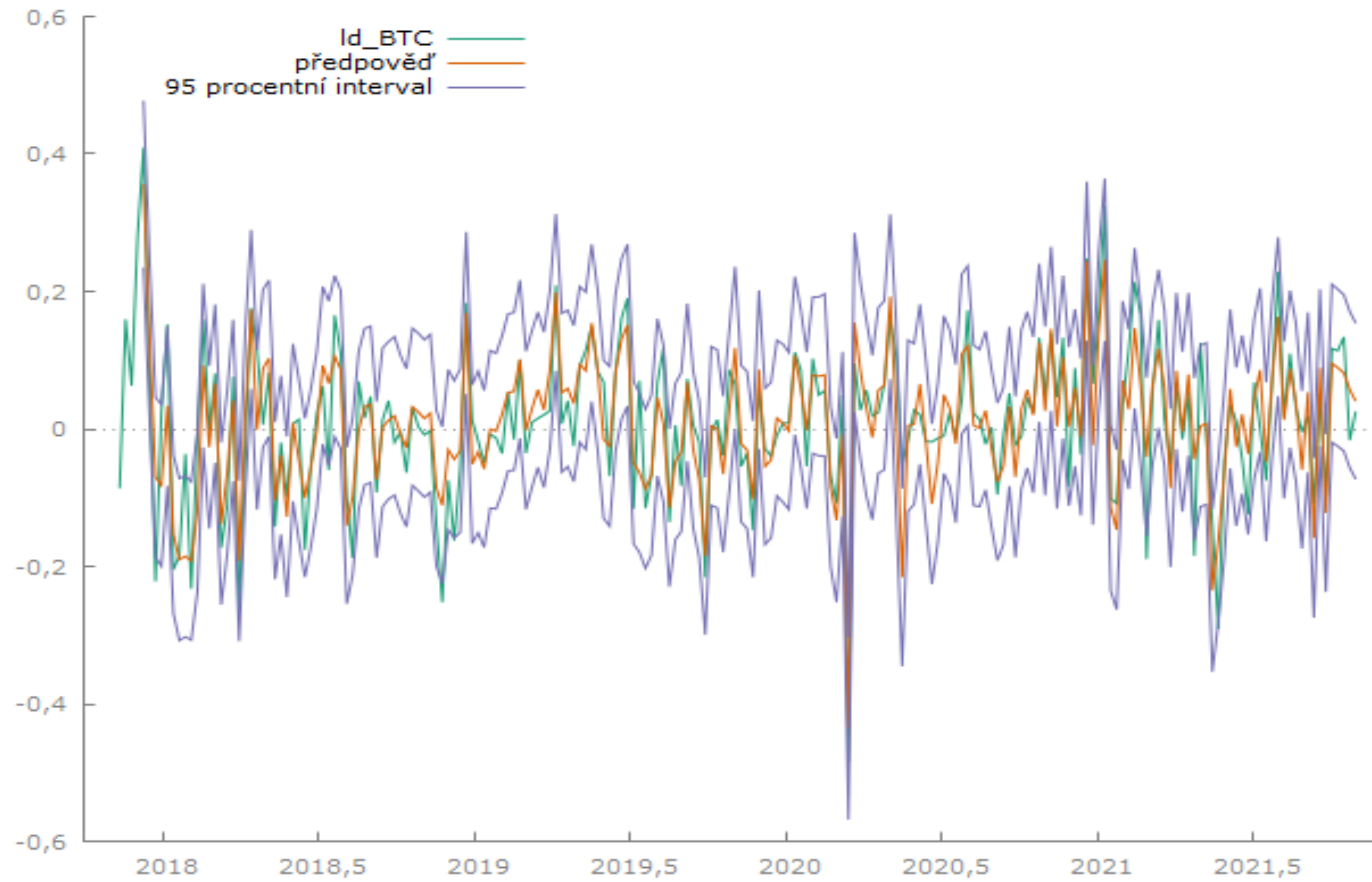
Obrázek 11 Prognóza ex-post

	ld_BTC	předpověď	směr. chyba	95% konfidenční interval
2017-11-03				
2017-11-10	-0,086234			
2017-11-17	0,159456			
2017-11-24	0,062834			
2017-12-01	0,280029			
2017-12-08	0,409277	0,356130	0,061471	0,234864 - 0,477397
2017-12-15	0,080478	0,134536	0,058380	0,019367 - 0,249704
2017-12-22	-0,221761	-0,069983	0,058828	-0,186035 - 0,046069
2017-12-29	0,024639	-0,082023	0,059545	-0,199489 - 0,035443
2018-01-05	0,152233	0,033439	0,058861	-0,082677 - 0,149556
2018-01-12	-0,204741	-0,153451	0,058384	-0,268627 - -0,038274
2018-01-19	-0,183858	-0,189914	0,059719	-0,307724 - -0,072104
2018-01-26	-0,036496	-0,185097	0,059386	-0,302250 - -0,067943
2018-02-02	-0,232431	-0,191919	0,058358	-0,307043 - -0,076795
2018-02-09	-0,013347	-0,121367	0,059001	-0,237760 - -0,004975
2018-02-16	0,159210	0,092148	0,060272	-0,026752 - 0,211048
2018-02-23	-0,002215	-0,026562	0,059934	-0,144796 - 0,091672
2018-03-02	0,080915	0,065850	0,058428	-0,049412 - 0,181112
2018-03-09	-0,172731	-0,137725	0,059749	-0,255593 - -0,019856
2018-03-16	-0,111925	-0,063358	0,060129	-0,181976 - 0,055261
2018-03-23	0,075853	0,041462	0,059506	-0,075927 - 0,158852
2018-03-30	-0,265133	-0,192015	0,059143	-0,308687 - -0,075342
2021-07-02	0,067559	0,043913	0,058909	-0,072298 - 0,160125
2021-07-09	0,000568	0,085522	0,060438	-0,033706 - 0,204750
2021-07-16	-0,074971	-0,047909	0,058599	-0,163508 - 0,067690
2021-07-23	0,065978	0,071779	0,057630	-0,041910 - 0,185467
2021-07-30	0,228752	0,163214	0,058541	0,047727 - 0,278700
2021-08-06	0,017225	0,013006	0,057810	-0,101037 - 0,127049
2021-08-13	0,109647	0,087158	0,057948	-0,027158 - 0,201474
2021-08-20	0,030043	0,038834	0,058101	-0,075783 - 0,153451
2021-08-27	-0,004450	-0,059255	0,058131	-0,173931 - 0,055420
2021-09-03	0,019122	0,053260	0,058984	-0,063100 - 0,169620
2021-09-10	-0,109168	-0,158626	0,058869	-0,274759 - -0,042494
2021-09-17	0,051780	0,088912	0,057851	-0,025212 - 0,203037
2021-09-24	-0,097647	-0,122453	0,058145	-0,237157 - -0,007749
2021-10-01	0,117030	0,095384	0,058314	-0,019654 - 0,210422
2021-10-08	0,113795	0,089094	0,057852	-0,025032 - 0,203220
2021-10-15	0,133828	0,081534	0,057598	-0,032092 - 0,195159
2021-10-22	-0,016402	0,057316	0,057624	-0,056361 - 0,170993
2021-10-29	0,025548	0,040456	0,057506	-0,072989 - 0,153900

(zdroj: vlastní zpracování)

Prognózu ex-post lze znázornit i graficky:

Graf 3 Prognóza ex-post



(zdroj: vlastní zpracování)

Ze získaného výstupu lze usoudit, že skutečné a předpovídané hodnoty se nikterak významně neliší. Předpovídané hodnoty se rovněž drží v rámci 95 % intervalu spolehlivosti. Posledním indikátorem prognostické kvality modelu je statistický ukazatel Theilovo U, jehož hodnota v tomto případě dosahuje 0,37872. V případě, že hodnota Theilova U nepřesahuje 1, lze model považovat za vhodný k predikci.

Prognóza ex-ante

Před samotnou prognózou ex-ante je nejprve zapotřebí získat hodnoty vysvětlujících proměnných. Pro účely této diplomové práce byly hodnoty odhadnuty v aplikaci MS Excel. Jednou z užívaných metod je odhad pomocí trendové funkce. V tomto případě byla využita jak trendová funkce lineární, tak i složitější vícestupňové polynomy. Jako indikátor vhodné trendové funkce posloužil koeficient determinace R^2 , který MS Excel poskytuje. Nicméně v některých případech byla sice hodnota R^2 vyšší pro vícestupňové polynomy, avšak po provedení grafické analýzy trendu se ukázala lineární trendová funkce jako vhodnější alternativou. V případě dummy proměnných se odhad pomocí trendové funkce ukázal jako nepoužitelný. K odhadu tedy byla využita funkce FORECAST.EST, která funguje na principu předpovědi budoucí hodnoty na základě stávajících historických hodnot pomocí algoritmu exponenciálního vyhlazování. Proměnnou total_btc neboli celkový počet vytěžených bitcoinů není třeba odhadovat, neboť se dá snadno spočítat. Každý den se vytěží přibližně 900 bitcoinů a jelikož vstupní data jsou v týdenních intervalech, stačí tuto hodnotu vynásobit 7.

V následující tabulce č. 4 můžeme vidět trendovou funkci, R^2 , odhadnuté hodnoty, jejich přirozený logaritmus a difference pro proměnné – odměna těžařům, Ethereum a hash rate. Pro všechny zbylé proměnné jsou hodnoty uvedeny v příloze diplomové práce.

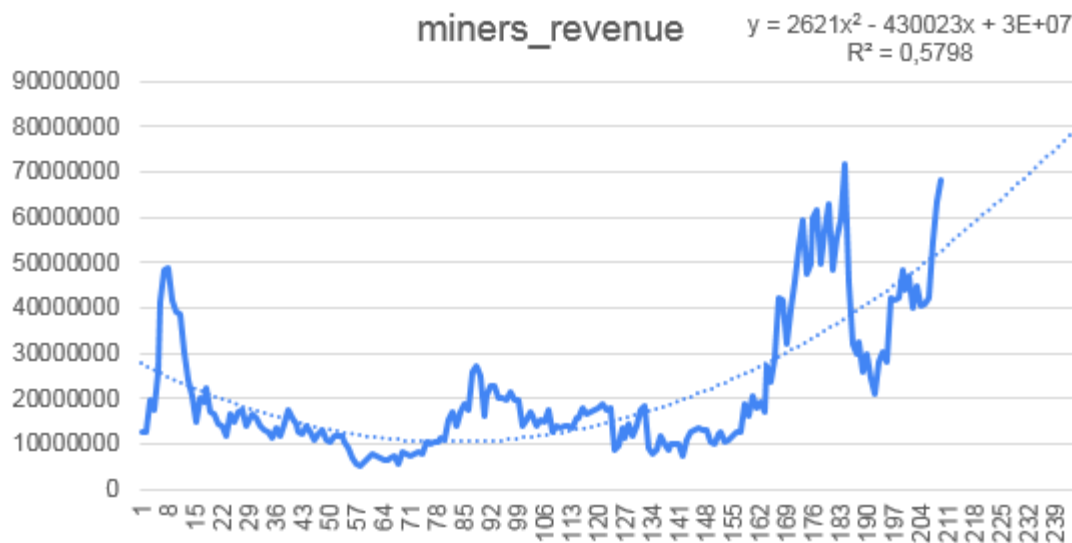
Tabulka 4 Odhadnuté hodnoty pro prognózu ex-ante

	miners_revenue			ETHER			hash_rate		
	$y = 2621x^2 - 430023x + 3E+07$			$y = 0,2101x^2 - 34,27x + 1298,4$			$y = 714689x + 1E+07$		
	$R^2 = 0,5798$			$R^2 = 0,8456$			$R^2 = 0,8605$		
	odhad	ln	diff	odhad	ln	diff	odhad	ln	diff
5.11.2021	55281270,00	17,82794471	-0,2128665963	3367,11	8,12181	-0,2709620844	160084690	18,8912135	-0,0642636378
12.11.2021	55954688,00	17,84005278	0,0121080672	3421,292	8,137774	0,0159634771	160799379	18,8956681	0,0044545071
19.11.2021	56633348,00	17,85210856	0,0120557786	3475,894	8,153607	0,0158335405	161514068	18,9001028	0,0044347524
26.11.2021	57317250,00	17,86411218	0,0120036265	3530,917	8,169313	0,0157057551	162228757	18,904518	0,0044151722
3.12.2021	58006394,00	17,8760638	0,0119516203	3586,36	8,184893	0,0155800668	162943446	18,9089137	0,0043957641
10.12.2021	58700780,00	17,88796357	0,0118997688	3642,223	8,200349	0,0154564232	163658135	18,9132903	0,0043765259
17.12.2021	59400408,00	17,89981165	0,0118480804	3698,506	8,215684	0,0153347739	164372824	18,9176477	0,0043574554
24.12.2021	60105278,00	17,91160822	0,0117965630	3755,209	8,230899	0,0152150700	165087513	18,9219863	0,0043385503
31.12.2021	60815390,00	17,92335344	0,0117452240	3812,332	8,245996	0,0150972642	165802202	18,9263061	0,0043198086
7.1.2022	61530744,00	17,93504751	0,0116940704	3869,876	8,260978	0,0149813107	166516891	18,9306073	0,0043012280
14.1.2022	62251340,00	17,94669062	0,0116431089	3927,84	8,275845	0,0148671654	167231580	18,9348903	0,0042828067
21.1.2022	62977178,00	17,95828296	0,0115923456	3986,224	8,2906	0,0147547855	167946269	18,9391547	0,0042645425
28.1.2022	63708258,00	17,96982475	0,0115417863	4045,028	8,305244	0,0146441295	168660958	18,9434011	0,0042464333
4.2.2022	64444580,00	17,98131619	0,0114914365	4104,253	8,319779	0,0145351573	169375647	18,9476296	0,0042284774
11.2.2022	65186144,00	17,99275749	0,0114413014	4163,898	8,334207	0,0144278299	170090336	18,9518402	0,0042106726
18.2.2022	65932950,00	18,00414887	0,0113913855	4223,963	8,348529	0,0143221098	170805025	18,9560333	0,0041930171
25.2.2022	66684998,00	18,01549057	0,0113416935	4284,448	8,362747	0,0142179604	171519714	18,9602088	0,0041755091
4.3.2022	67442288,00	18,0267828	0,0112922295	4345,353	8,376862	0,0141153463	172234403	18,9643669	0,0041581467
11.3.2022	68204820,00	18,03802579	0,0112429973	4406,678	8,390876	0,0140142332	172949092	18,9685078	0,0041409281
18.3.2022	68972594,00	18,0492198	0,0111940005	4468,424	8,404791	0,0139145877	173663781	18,9726317	0,0041238515
25.3.2022	69745610,00	18,06036504	0,0111452424	4530,59	8,418607	0,0138163777	174378470	18,9767386	0,0041069152
1.4.2022	70523868,00	18,07146176	0,0110967261	4593,176	8,432327	0,0137195717	175093159	18,9808287	0,0040901174
8.4.2022	71307368,00	18,08251022	0,0110484544	4656,182	8,445951	0,0136241394	175807848	18,9849022	0,0040734565
15.4.2022	72096110,00	18,09351065	0,0110004299	4719,609	8,459481	0,0135300511	176522537	18,9889591	0,0040569307
22.4.2022	72890094,00	18,1044633	0,0109526550	4783,456	8,472918	0,0134372782	177237226	18,9929997	0,0040405385
29.4.2022	73689320,00	18,11536843	0,0109051319	4847,723	8,486264	0,0133457928	177951915	18,9970239	0,0040242782
6.5.2022	74493788,00	18,1262263	0,0108578625	4912,41	8,49952	0,0132555680	178666604	19,0010321	0,0040081483
13.5.2022	75303498,00	18,13703715	0,0108108486	4977,517	8,512686	0,0131665772	179381293	19,0050242	0,0039921472
20.5.2022	76118450,00	18,14780124	0,0107640917	5043,044	8,525765	0,0130787951	180095982	19,0090005	0,0039762733
27.5.2022	76938644,00	18,15851883	0,0107175934	5108,992	8,538757	0,0129921967	180810671	19,0129611	0,0039605251
3.6.2022	77764080,00	18,16919019	0,0106713549	5175,36	8,551664	0,0129067579	181525360	19,0169059	0,0039449012
10.6.2022	78594758,00	18,17981556	0,0106253772	5242,148	8,564487	0,0128224551	182240049	19,0208353	0,0039294001
17.6.2022	79430678,00	18,19039522	0,0105796613	5309,356	8,577226	0,0127392656	182954738	19,0247493	0,0039140203
24.6.2022	80271840,00	18,20092943	0,0105342081	5376,985	8,589883	0,0126571669	183669427	19,0286481	0,0038987605
1.7.2022	81118244,00	18,21141845	0,0104890181	5445,034	8,602459	0,0125761376	184384116	19,0325317	0,0038836192

(zdroj: vlastní zpracování)

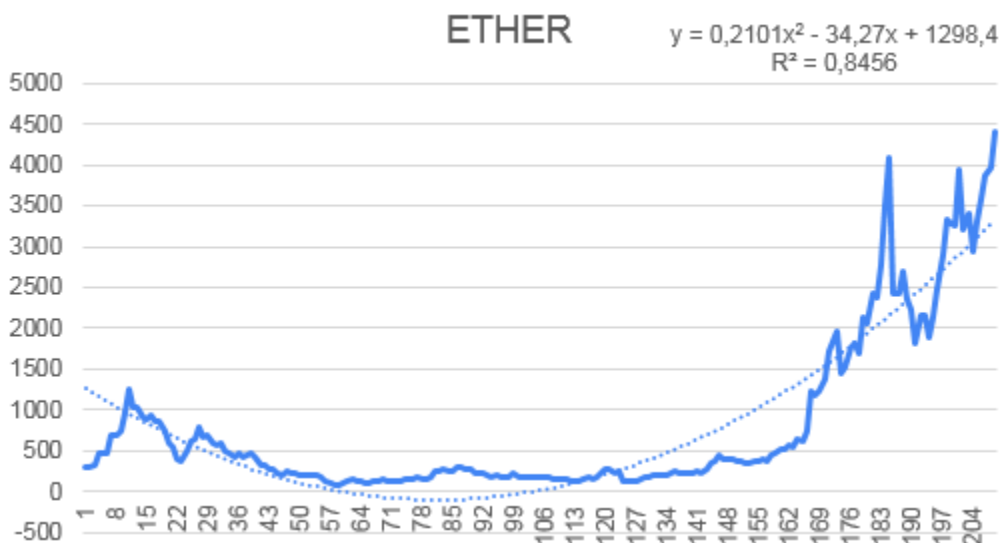
Nyní ještě grafy vývoje zmíněných třech proměnných se zobrazenou trendovou funkcí. Obdobně jako v případě tabulky i zbylé grafy jsou uvedeny v příloze diplomové práce.

Graf 4 Vývoj a trend – miners_revenue



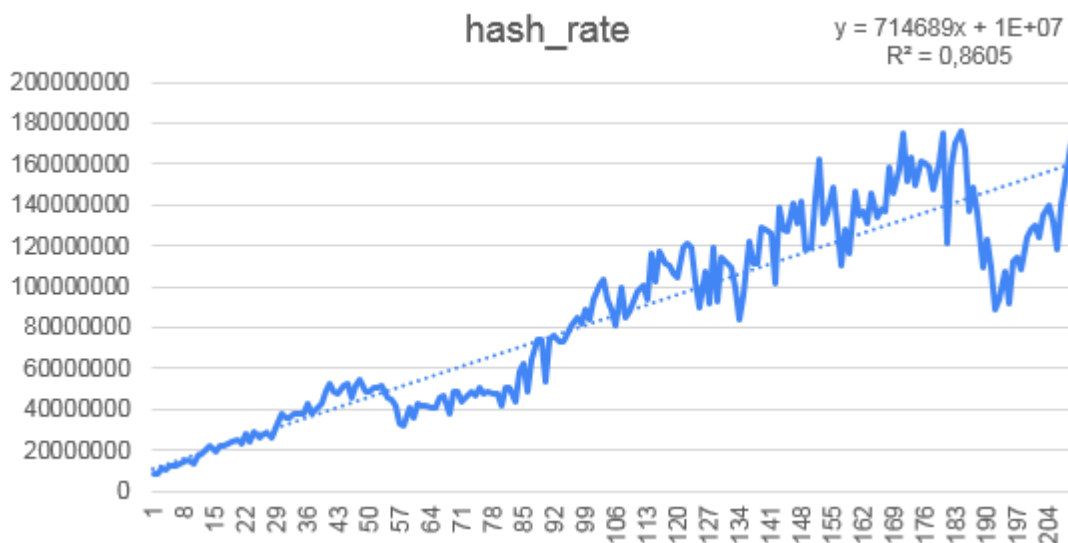
(zdroj: vlastní zpracování)

Graf 5 Vývoj a trend – Ether



(zdroj: vlastní zpracování)

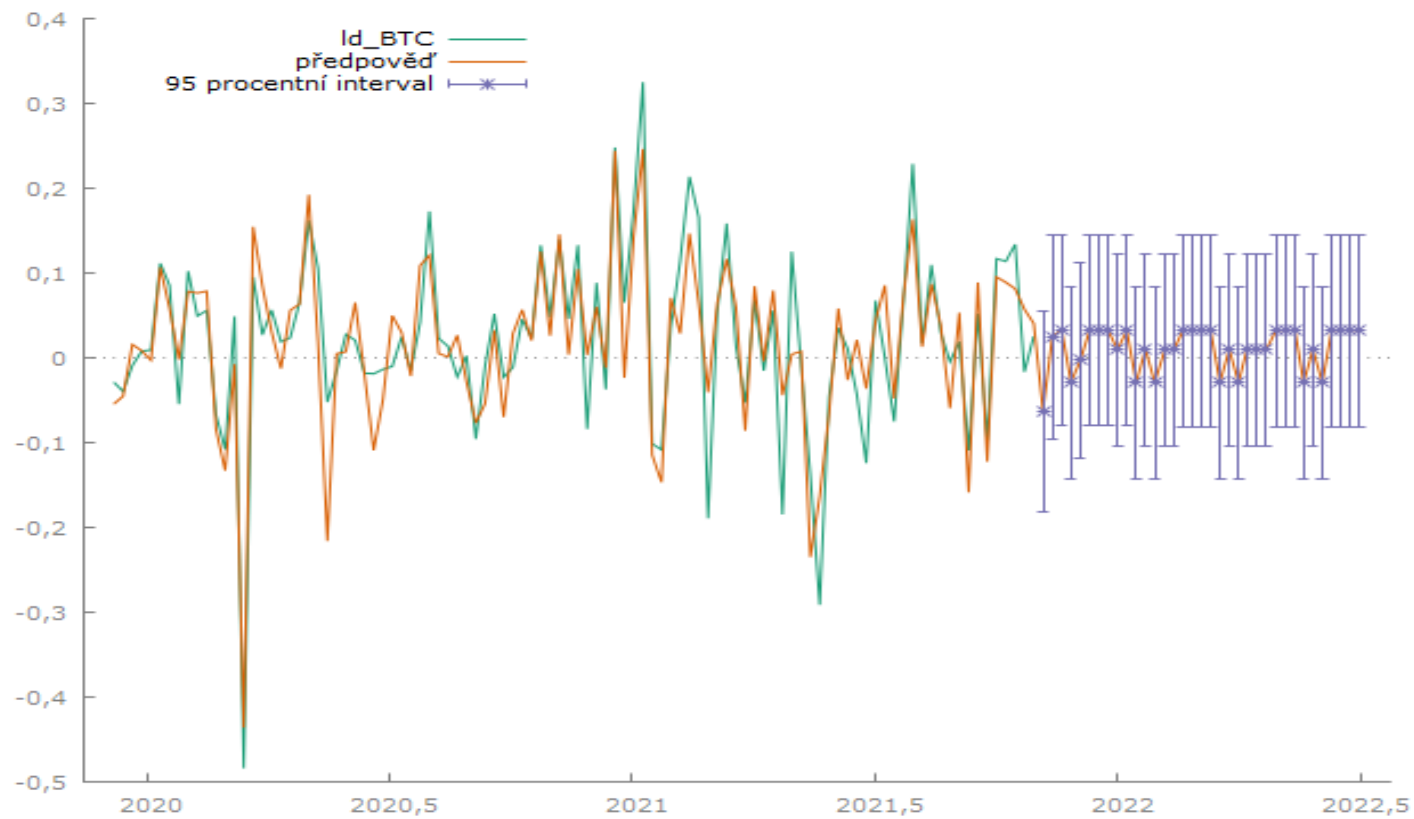
Graf 6 Vývoj a trend – hash rate



(zdroj: vlastní zpracování)

Po odhadu hodnot všech proměnných následuje jejich dosazení do gretlu. Výstupem gretlu je pak následující graf č.7:

Graf 7 Prognóza ex-ante



(zdroj: vlastní zpracování)

Gretl poskytuje i konkrétní hodnoty včetně směrodatné chyby a konfidenčních intervalů. Ty můžeme vidět na následujícím obrázku.

Obrázek 12 Prognóza ex-ante

Pro 95% konfidenční intervaly, $t(187, 0,025) = 1,973$

	ld_BTC	předpověď	směr. chyba	95% konfidenční interval
2021-09-24	-0,097647	-0,122453		
2021-10-01	0,117030	0,095384		
2021-10-08	0,113795	0,089094		
2021-10-15	0,133828	0,081534		
2021-10-22	-0,016402	0,057316		
2021-10-29	0,025548	0,040456		
2021-11-05		-0,062574	0,060169	-0,181271 - 0,056123
2021-11-12		0,024980	0,061346	-0,096039 - 0,145998
2021-11-19		0,033217	0,057083	-0,079393 - 0,145827
2021-11-26		-0,028653	0,057497	-0,142079 - 0,084773
2021-12-03		-0,002973	0,058020	-0,117432 - 0,111486
2021-12-10		0,032111	0,057084	-0,080501 - 0,144722
2021-12-17		0,032158	0,057084	-0,080454 - 0,144770
2021-12-24		0,032100	0,057085	-0,080513 - 0,144712
2021-12-31		0,010040	0,057470	-0,103332 - 0,123412
2022-01-07		0,032088	0,057085	-0,080526 - 0,144702
2022-01-14		-0,029012	0,057496	-0,142436 - 0,084413
2022-01-21		0,010022	0,057470	-0,103351 - 0,123395
2022-01-28		-0,029024	0,057497	-0,142450 - 0,084401
2022-02-04		0,010009	0,057471	-0,103365 - 0,123383
2022-02-11		0,010002	0,057471	-0,103372 - 0,123377
2022-02-18		0,032049	0,057087	-0,080567 - 0,144666
2022-02-25		0,032042	0,057087	-0,080575 - 0,144659
2022-03-04		0,032035	0,057087	-0,080583 - 0,144653
2022-03-11		0,032028	0,057087	-0,080590 - 0,144646
2022-03-18		-0,029073	0,057498	-0,142500 - 0,084354
2022-03-25		0,009959	0,057472	-0,103418 - 0,123337
2022-04-01		-0,029088	0,057498	-0,142516 - 0,084340
2022-04-08		0,009944	0,057473	-0,103434 - 0,123322
2022-04-15		0,009937	0,057473	-0,103442 - 0,123315
2022-04-22		0,009929	0,057473	-0,103450 - 0,123308
2022-04-29		0,031975	0,057089	-0,080647 - 0,144596
2022-05-06		0,031967	0,057089	-0,080655 - 0,144589
2022-05-13		0,031959	0,057090	-0,080664 - 0,144581
2022-05-20		-0,029143	0,057499	-0,142573 - 0,084287
2022-05-27		0,009889	0,057474	-0,103492 - 0,123270
2022-06-03		-0,029160	0,057499	-0,142590 - 0,084271
2022-06-10		0,031926	0,057091	-0,080699 - 0,144551
2022-06-17		0,031993	0,057091	-0,080632 - 0,144618
2022-06-24		0,032032	0,057091	-0,080594 - 0,144658
2022-07-01		0,031901	0,057091	-0,080725 - 0,144527

(zdroj: vlastní zpracování)

Získaná prognóza je však ve stavu logaritmických diferencí. Aby bylo možné prognózu interpretovat, bude nutné hodnoty převést do absolutních čísel. Tyto hodnoty jsou zobrazeny v následující tabulce.

Tabulka 5 Prognóza ex-ante – absolutní hodnoty v USD

	ln_diff	ln	abs
5.11.2021	-0,062574	10,976468	58 481,65
12.11.2021	0,024980	11,001448	59 960,92
19.11.2021	0,033217	11,034665	61 986,09
26.11.2021	-0,028653	11,006012	60 235,21
3.12.2021	-0,002973	11,003039	60 056,40
10.12.2021	0,032111	11,035150	62 016,16
17.12.2021	0,032158	11,067308	64 042,89
24.12.2021	0,032100	11,099408	66 132,02
31.12.2021	0,010040	11,109448	66 799,33
7.1.2022	0,032088	11,141536	68 977,55
14.1.2022	-0,029012	11,112524	67 005,12
21.1.2022	0,010022	11,122546	67 680,02
28.1.2022	-0,029024	11,093522	65 743,91
4.2.2022	0,010009	11,103531	66 405,24
11.2.2022	0,010002	11,113533	67 072,76
18.2.2022	0,032049	11,145582	69 257,20
25.2.2022	0,032042	11,177624	71 512,27
4.3.2022	0,032035	11,209659	73 840,25
11.3.2022	0,032028	11,241687	76 243,49
18.3.2022	-0,290730	10,950957	57 008,59
25.3.2022	0,009959	10,960916	57 579,18
1.4.2022	-0,029088	10,931828	55 928,44
8.4.2022	0,009944	10,941772	56 487,37
15.4.2022	0,009937	10,951709	57 051,48
22.4.2022	0,009929	10,961638	57 620,77
29.4.2022	0,031975	10,993613	59 492,96
6.5.2022	0,031967	11,025580	61 425,50
13.5.2022	0,031959	11,057539	63 420,30
20.5.2022	-0,029143	11,028396	61 598,72
27.5.2022	0,009889	11,038285	62 210,89
3.6.2022	-0,029160	11,009125	60 423,01
10.6.2022	0,031926	11,041051	62 383,20
17.6.2022	0,031993	11,073044	64 411,30
24.6.2022	0,032032	11,105076	66 507,92
1.7.2022	0,031901	11,136977	68 663,79

(zdroj: vlastní zpracování)

Algoritmus výpočtu absolutních hodnot byl následující: sloupeček ln_diff představuje hodnoty získané z gretlu, sloupeček ln představuje samostatné přirozené logaritmy prognózovaných hodnot bitcoinu – v tomto sloupečku byly hodnoty zjištěny jako přirozený logaritmus hodnoty bitcoinu v posledním známém (neprognozovaném) období + diference.

Ve sloupci abs pak můžeme vidět předpovídanou hodnotu bitcoinu, která byla vypočtena jako odlogaritmování hodnot ve sloupci ln pomocí Eulerova čísla (v excelu také jako funkce EXP

6 Zhodnocení výsledků

Vzhledem k tomu, že datová základna použitá pro odhad modelu končí 29.10.2021, byla v čase psaní této kapitoly k dispozici část skutečných hodnot. Porovnání můžeme vidět v následující tabulce:

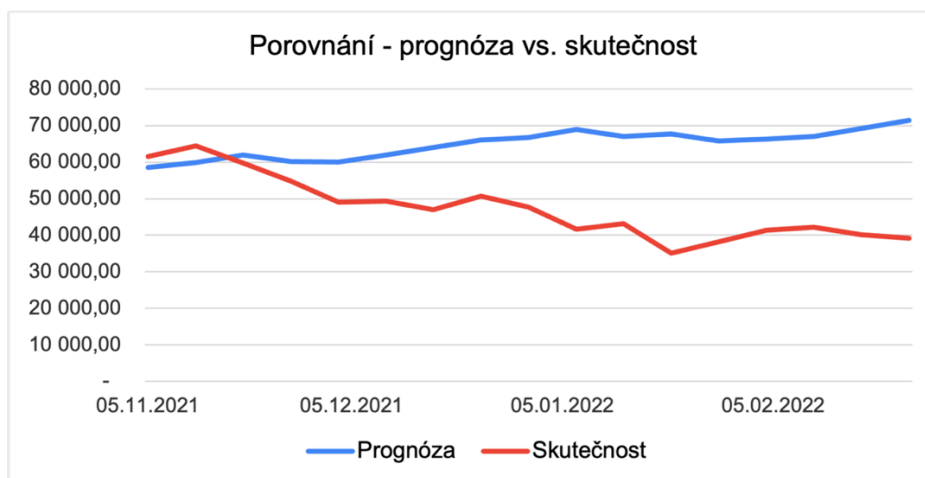
Tabulka 6 Porovnání – prognóza vs. skutečnost v USD

Datum	Prognóza	Skutečnost
05.11.2021	58 482	61 539
12.11.2021	59 961	64 400
19.11.2021	61 986	59 761
26.11.2021	60 235	54 760
03.12.2021	60 056	49 106
10.12.2021	62 016	49 343
17.12.2021	64 043	46 928
24.12.2021	66 132	50 653
31.12.2021	66 799	47 733
07.01.2022	68 978	41 685
14.01.2022	67 005	43 160
21.01.2022	67 680	35 070
28.01.2022	65 744	38 191
04.02.2022	66 405	41 434
11.02.2022	67 073	42 178
18.02.2022	69 257	40 148
25.02.2022	71 512	39 138

(zdroj: vlastní zpracování)

Pro lepší znázornění můžeme vyjádřit prognózované a skutečné hodnoty na následujícím grafu č. 8:

Graf 8 Porovnání – prognóza vs. skutečnost



(zdroj: vlastní zpracování)

Na výše uvedeném grafu můžeme vidět, že v případě krátkodobé a střednědobé prognózy se predikované hodnoty od skutečných lišily pouze minimálně a model tak předpovídal hodnoty relativně přesně. Nicméně čím byl prognostický horizont delší, začaly se predikované a skutečné hodnoty celkem významně rozcházet. To je zapříčiněno hned několika faktory. Tím prvním může být nedostatečná specifikace ve formě počtu zvolených proměnných, protože na čím delší dobu chceme prognózovat, tím více proměnných musíme do modelu zahrnout. Požadavek na zahrnutí dalších proměnných však roste s délkou prognostického horizontu exponenciálně. Dalším faktorem může být jednoznačně zvolená aproximovaná metoda odhadu vstupních dat – tedy hodnot regresorů. Pro účely diplomové práce byla využita metoda trendových funkcí. Problém trendových funkcí v tomto konkrétním případě spočívá v tom, že z pohledu historického vývoje zvolených regresorů, na základě nějž je trendová funkce odhadnuta, se můžeme setkat s jednoznačným růstem zvolených determinant. Ačkoliv byly použity i jiné než lineární funkční formy trendových funkcí, nedokázaly patřičně zohlednit situaci na trzích, která v prognózovaném období proběhla. Geopolitická situace a situace na trzích je pravděpodobně tím nejzásadnějším faktorem, proč se prognóza tak vychyluje od skutečnosti. V prognózovaném období se svět potýkal hned s několika problémy, které jednoznačně ovlivňují situaci na světových trzích, ať už se jedná o akcie, kryptoměny či konvenční obchodované instrumenty v podobě nerostných surovin. Právě ona nejistota na trzích způsobená každou další vlnou viru COVID-19, různými návrhy či úplnými regulacemi kryptoměn, napjatými vztahy mezi světovými velmocemi a vyvrcholením války na Ukrajině, se negativně promítne jednak na samotné hodnotě bitcoinu, tak i na hodnotě vysvětlujících proměnných. Výsledkem pak tedy je, že klesá hodnota kryptoměn, akcií a dalších investičních instrumentů, což je přímo v rozporu se zvolenou metodou odhadu regresorů, tedy trendovými funkcemi, které z dlouhodobého hlediska předpovídají růst.

7 Závěr

Hlavním cílem práce byla konstrukce modelu zaměřeného na simulaci hodnoty kryptoměny bitcoin a následná prognóza vývoje s využitím metod ekonometrické analýzy. K dosažení hlavního cíle byly stanoveny cíle dílčí, a to v podobě identifikace vhodných determinant, specifikace ekonometrického modelu, kvantifikace, verifikace a aplikace modelu a ex-ante prognóza hodnoty bitcoinu.

V první řadě bylo zapotřebí identifikovat vhodné determinanty. Determinanty byly zvoleny na základě dvou faktorů. Prvním faktorem bylo studium vědeckých článků dostupných v online databázích Web of science a Scopus, které se do jisté míry modelováním, ať už v jakékoli podobě, hodnoty kryptoměn zabývaly. Druhým faktorem pak byly poznatky a znalosti autora zkoumané problematiky. Jako vhodné determinanty se ukázaly proměnné z řad klasických investičních instrumentů v podobě akcií, které jsou běžně agregovány do takzvaných akciových indexů. V diplomové práci byly využity následující akciové indexy: S&P500, jenž představuje 500 nejhodnotnějších firem obchodovaných na americké burze, japonský index NIKKEI225, který se skládá z 225 nejvýznamnějších akciových titulů obchodovaných na japonské burze, německý index frankfurtské burzy DAX čítající 40 nejvýznamnějších německých společností a britský index 100 firem s nejvyšší tržní kapitalizací FTSE100. Další významné determinanty pak vzešly přímo z blockchainové sítě bitcoinu. Z řad blockchainových ukazatelů byly zvoleny následující indikátory: odměna těžařů, hash-rate, medián doby potřebné pro potvrzení transakce, počet unikátních adres, průměrná velikost bloku a celkový počet vytěžených bitcoinů. Akciové indexy a blockchainové ukazatele lze považovat za hlavní determinanty. Jako vedlejší determinanty byly zvoleny ještě instrumenty v podobě nerostných surovin – zlato a ropa, veřejný zájem v podobě podílu na vyhledávaných pojmech na google.com a druhá nejznámější kryptoměna Ethereum.

Během fáze specifikace modelu bylo zapotřebí do modelu zahrnout pouze relevantní proměnné a vypustit ty irelevantní, zvolit správnou funkční formu a zahrnout faktor času. K dosažení výsledného modelu vedla dlouhá cesta a během fáze specifikace model prošel několika úpravami. V předešlém odstavci jsou zmíněny pouze relevantní proměnné, které se nacházejí ve výsledném modelu. Na počátku specifikace byly využity i například následující

determinanty – úroková míra amerického FEDu, index volatility VIX, počet transakcí v blockchainové síti, náročnost těžby a další. Nicméně tyto proměnné se ukázaly jako irelevantní a byly během specifikace z modelu odstraněny. Na počátku byla snaha přijít s lineárním regresním modelem. Nicméně tato funkční forma se ukázala jako nedostatečná a bylo tedy potřeba pokračovat ve specifikaci modelu a využít i jiné funkční formy. Funkce kvadratická i kubická taktéž nesplňovaly specifikační předpoklady modelu. Jako nejvhodnější funkční forma se ukázala funkce mocninná, která byla prostřednictvím logaritmicke linearizována a model tak bylo možné odhadnout běžnou metodou nejmenších čtverců. Zvolením mocninné funkce však fáze specifikace nekončila, neboť model stále nesplňoval předpoklady o náhodné složce. Dalšími kroky bylo převedení vstupních dat do prvních diferencí a zahrnutí faktoru času v podobě zpožděných a dummy proměnných. Nicméně tato změna vedla k tomu, že model již nepracoval s absolutními hodnotami, avšak pracoval s diferencemi – tedy změnami, což bylo potřeba zohlednit při interpretaci odhadnutých parametrů a změnit tak celkový pohled na získaný model. Zohlednit bylo potřeba taktéž zvolení mocninné funkční formy, neboť v jejím případě odhadnuté parametry vyjadřují relativní působení na vysvětlovanou proměnnou v podobě koeficientů pružnosti.

Po úspěšné specifikaci modelu přišla na řadu jeho kvantifikace, verifikace a aplikace. Před samotným odhadem modelu byla nejprve ověřena neexistence perfektní multikolinerity a stacionárnost časových řad. K otestování, zda se v modelu nevyskytuje perfektní multikolinerita byla využita korelační matice. Stacionárnost časových řad pak byla ověřena prostřednictvím rozšířeného Dickey-Fullerova testu. Model byl kvantifikován a verifikován s využitím volně dostupného ekonometricko-statistického softwaru gretl. Pro modelování byly použity časové řady v týdenních intervalech za období 30. 10. 2017 – 29. 10. 2021. Data byla získána především z googlefinance, blockchain.info, googletrends a macrotrends.net. Během fáze verifikace byla prvně testována shoda odhadnutého modelu s daty prostřednictvím korigovaného koeficientu determinace. Korigovaný koeficient determinace nabyl hodnoty 0,735411 což implikuje, že model vysvětluje změny v hodnotě bitcoinu ze 73,54 %. Dalším krokem bylo ověření statistické významnosti parametrů s využitím t-testu. Na hladině významnosti $\alpha = 0,01$ byly významné parametry odměna těžařů, Ethereum, hash rate, dummy proměnná znázorňující pokles hodnoty bitcoinu a akciový index DAX. Další testovanou hladinou významnosti je pak $\alpha = 0,05$, na které byly

významné parametry: dummy proměnná symbolizující růst hodnoty bitcoinu, veřejný zájem, počet unikátních adres, průměrná velikost bloku a akciový index FTSE100. Na poslední přípustné hladině významnosti $\alpha = 0,1$ pak byly významné ještě parametry proměnných zlato, celkový počet vytěžených bitcoinů a akciový index NIKKEI225. Jako statisticky nevýznamné se ukázaly proměnné a jejich parametry: konstanta, ropa, akciový index S&P500 a medián doby potřebné pro potvrzení jedné transakce. V rámci ekonometrické verifikaci se testovaly standardní předpoklady o náhodné složce – tedy heteroskedasticita, normalita rozdělení a autokorelace reziduí. Všechny zmíněné předpoklady model splnil a byl tak vhodný k aplikaci. Model byl aplikován v podobě simulování scénářů a odvození prognózy ex-ante. Všechny scénáře byly simulovány za podmínek ceteris paribus a jejich předmětem bylo zkoumání vlivu na vysvětlovanou proměnou v případě 10% růstu hodnot vysvětlujících proměnných.

Posledním dílčím cílem bylo odvození prognózy ex-ante. Před samotným provedením ex-ante prognózy bylo nejprve potřeba otestovat prognostickou kvalitu modelu. K tomu byla využita prognóza ex-post, tedy prognóza do minulosti. Výsledek ex-post prognózy se ukázal jako příznivý, neboť prognózované hodnoty se od skutečných nikterak významně nelišily. Všechny předpovídané hodnoty se rovněž držely v rámci 95% konfidenčního intervalu. Před samotným provedením prognózy ex-ante bylo nejprve potřeba odhadnout budoucí hodnoty všech regresorů, k čemuž byl využit software Microsoft Excel. Hodnoty pro většinu proměnných byly odhadnuty prostřednictvím trendových funkcí, ať už lineárních, tak i vícestupňových polynomů. V případě dummy proměnných nebylo možné využít trendové funkce a k odhadu jejich očekávaného vývoje byla využita funkce FORECAST.EST. Pro proměnnou total_btc šlo jednoduše určit budoucí hodnoty, neboť každý den přibude téměř stejný počet nových bitcoinů. Po odhadu hodnot pro všechny proměnné (vyjma dummy proměnných) bylo potřeba tyto hodnoty zlogaritmovat a převést do postupných diferencí. Následně byly odhadnuté a upravené hodnoty zaneseny do SW gretl a provedena ex-ante prognóza na 35 období, tedy týdnů. Dle klasifikace se jednalo o dlouhodobou prognózu, avšak v mezi jedné třetiny délky časové řady podkladových údajů. Aby bylo možné prognózu interpretovat, bylo nezbytné získané hodnoty odlogaritmovat a „oddiferencovat“ – tedy převést zpět na absolutní hodnoty. Vzhledem k tomu, že v době psaní této diplomové práce byly dostupné skutečné hodnoty z prognózovaných období, byla v rámci poslední

kapitoly provedena komparace. V případě krátkodobé a střednědobé prognózy se předpovídané hodnoty od skutečných významně nelišily. Z počátku byly lehce podhodnocené, poté lehce nadhodnocené. Nicméně čím byl předpovídaný časový úsek delší, tím se prognóza více a více rozcházela se skutečností, což mohlo být zapříčiněno hned několika faktory. Prvním faktorem mohla být aproximovaná metoda odhadu budoucích hodnot regresorů. Dalším faktorem mohla být skutečnost, že v případě provádění dlouhodobých prognóz roste požadavek na zahrnutí dalších vysvětlujících proměnných, a to exponenciálně. V neposlední řadě mohla být prognóza negativně ovlivněna nejistotou na trzích způsobenou různými geopolitickými vlivy, které v době psaní této diplomové práce probíhaly. Ať už se jedná o vlivy ovlivňující přímo bitcoin, tedy různé regulace či úplné restrikce v jistých jurisdikcích, tak i vlivy které negativně působily na zvolené regresory – zejména pak akciové indexy. S každou další vlnou viru Covid-19, napjatými vztahy mezi světovými mocnostmi, či vyvrcholením války na Ukrajině nejistota na trzích rapidně stoupala a hodnota akcií klesala, čímž došlo k nepřesnému odhadu vstupních dat vysvětlujících proměnných pro prognózu, neboť vzhledem k historickému vývoji zvolených determinant trendové funkce předpokládaly růst, ačkoliv v praxi došlo k opaku.

8 Seznam použitých zdrojů

Knížní publikace:

1. ABBATEMARCO, Nico, et al. *The Blockchain Journey: A Guide to Practical Business Applications*, Bocconi University Press, 2018. ISBN 978-88-854-8666-9
2. ALMAN, Susan, and Sandra HIRSCH. *Blockchain*, American Library Association, 2019. ISBN 978-08-389-4681-7
3. ARLT, Josef a Markéta ARLTOVÁ. *Ekonomické časové řady*. Praha: Professional Publishing, 2009. ISBN 978-80-86946-85-6.
4. ARLT, Josef a Markéta ARLTOVÁ. *Finanční časové řady: [vlastnosti, metody modelování, příklady a aplikace]*. Praha: Grada, 2003. ISBN 80-247-0330-0.
5. BALTAGI, Badi. *A Companion to Theoretical Econometrics*. John Wiley & Sons, Incorporated, 2001. ISBN 978-04-709-9830-4
6. BASHIR, Imran. *Mastering Blockchain: Distributed Ledger Technology, Decentralization, and Smart Contracts Explained, 2nd Edition*, Packt Publishing, Limited, 2018. ISBN 978-17-888-3867-2
7. CIPRA, Tomáš. *Finanční ekonometrie. 2., upr. vyd.* Praha: Ekopress, 2013. ISBN 978-80-86929-93-4.
8. ČERNOHORSKÝ, Jan a Petr TEPLÝ. *Základy financí*. Praha: Grada, 2011. ISBN 978-80-247-3669-3.
9. FRANCO, Pedro. *Understanding Bitcoin: Cryptography, Engineering and Economics*, John Wiley & Sons, Incorporated, 2014. ISBN 978-11-190-1915-2
10. GOLDBERGER, John. *Econometric Theory*. New York: John Wiley & Sons, 1964. ISBN 978-04-713-1101-0.
11. GRABOWSKI, Mark. *Cryptocurrencies: A Primer on Digital Money*, Taylor & Francis Group, 2019. ISBN 978-04-295-1014-4
12. GUJARATI, Damodar. *Basic econometrics*. Singapore: McGraw-Hill, 2003. ISBN 978-00-724-7852-5.
13. HAAVELMO, Trygve. *The probability Approach in Econometrics*. Supplement to *Econometrica*, 1944, vol 12. ISSN 1468-0262.
14. HANČLOVÁ, Jana. *Ekonomické modelování: klasické přístupy s aplikacemi*. Praha: Professional Publishing, 2012. ISBN 978-80-7431-088-1.

15. HUŠEK, Roman. *Ekonometrická analýza*. Praha: Oeconomica, 2007. ISBN 978-80-245-1300-3.
16. CHOWDHURY, Niaz. *Inside Blockchain, Bitcoin, and Cryptocurrencies*, Auerbach Publishers, Incorporated, 2019. ISBN 978-10-005-0770-6
17. CHUEN, Kuo, LEE, David. *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data*. Elsevier Science & Technology, 2015. ISBN 978-01-280-2351-8
18. JÍLEK, Josef. *Finance v globální ekonomice*. Praha: Grada, 2013. Finanční trhy a instituce. ISBN 978-80-247-3893-2.
19. LANSKY, Jan. *Possible State Approaches to Cryptocurrencies*. Journal of Systems Integration, 2018. ISSN 1804-2724.
20. NAGHSHPOU, Shahdad. *The Fundamentals of Money and Financial Systems*, Business Expert Press, 2013. ISBN 978-16-064-9485-1
21. NARAYANAN, Arvind. *Bitcoin and cryptocurrency technologies: a comprehensive introduction*. Princeton: Princeton University Press, 2016. ISBN 978-069-1171-692.
22. SAMUELSON, P., A., KOOMPANS, T. C., STONE J. R. N., *Report of the Evaluative Committee of Econometrica*. Econometrica, 1954. ISSN – 1468-0262.
23. STROUKAL, Dominik a Jan SKALICKÝ. *Bitcoin a jiné kryptopeníze budoucnosti: historie, ekonomie a technologie kryptoměn, stručná příručka pro úplné začátečníky*. Třetí rozšířené vydání. Praha: Grada Publishing, 2021. Finance pro každého. ISBN 978-80-271-1043-8.
24. WWSTHOFF, Frank. *An Introduction to Econometrics: A Self-Contained Approach*, MIT Press, 2013. ISBN 978-02-623-1715-3
25. WILSON, J. Holton, et al. *Regression Analysis: Understanding and Building Business and Economic Models Using Excel, Second Edition*, Business Expert Press, 2016. ISBN 978-16-315-7386-6
26. WOLLRIDGE, Jeffrey. *Introductory econometrics: a modern approach*. Mason, Ohio: South-Western Cengage Learning, 2008. ISBN 978-0-324-66054-8.

Elektronické články:

27. Au Vo, Thomas A. Chapman & Yen-Sheng Lee (2021) Examining Bitcoin and Economic Determinants: An Evolutionary Perspective, *Journal of Computer Information Systems*, DOI: [10.1080/08874417.2020.1865851](https://doi.org/10.1080/08874417.2020.1865851)
28. Chen, TH., Chen, MY. & Du, GT. The Determinants of Bitcoin's Price: Utilization of GARCH and Machine Learning Approaches. *Comput Econ* 57, 267–280 (2021). <https://doi-org.infozdroje.czu.cz/10.1007/s10614-020-10057-7>
29. NAKAMOTO, Satoshi. Bitcoin: A peer-to-peer electronic cash system, 2008. Dostupné z: <https://bitcoin.org>
30. ROSENFELD, Meni. Analysis of hashrate-based double-spending, 2012. Dostupné z: <https://bitcoil.co.il/Doublespend.pdf>
31. Wei Chen, Huilin Xu, Lifen Jia, Ying Gao. Machine learning model for Bitcoin Exchange rate prediction using economic and technology determinants: *International Journal of Forecasting* 37, 28-43 (2021) <https://doi.org/10.1016/j.ijforecast.2020.02.008>.

Ostatní zdroje:

32. Bitcoin ban these are the countries where crypto is restricted or illegal. Euronews [online]. [cit.17.03.2022]. Dostupné z: <https://www.euronews.com/next/2021/09/24/bitcoin-ban-these-are-the-countries-where-crypto-is-restricted-or-illegal2>
33. Blockchain Explorer - Search the Blockchain | BTC | ETH | BCH. Blockchain.com | The Most Trusted Crypto Wallet & Exchange[online]. [cit. 17.03.2022]. Dostupné z: <https://www.blockchain.com/charts>
34. Crude Oil Prices - 70 Year Historical Chart | MacroTrends. Macrotrends | The Long Term Perspective on Markets [online]. Copyright © 2010 [cit. 17.03.2022]. Dostupné z: <https://www.macrotrends.net/1369/crude-oil-price-history-chart>
35. Gold Prices - 100 Year Historical Chart | MacroTrends. Macrotrends | The Long Term Perspective on Markets [online]. Copyright © 2010 [cit. 17.03.2022]. Dostupné z: <https://www.macrotrends.net/1333/historical-gold-prices-100-year-chart>

36. Google Finance – ceny na akciovém trhu, odhady cen v reálném čase a novinky ze světa obchodu. Google [online]. [cit.17.03.2022]. Dostupné z:
<https://www.google.com/finance/?hl=cs>
37. Google Trends. [online]. [cit.17.03.2022]. Dostupné z: <https://trends.google.com/trends/?geo=CZ>
38. Investopedia. Investopedia: Sharper insight, better investing. [online]. [cit.17.03.2022]. Dostupné z: <https://www.investopedia.com/cryptocurrency-regulations-around-the-world-5202122>)
39. Least Squares Regression Line: Ordinary and Partial - Statistics How To. Statistics How To: Elementary Statistics for the rest of us![online]. Copyright © 2022 [cit. 17.03.2022]. Dostupné z: <https://www.statisticshowto.com/probability-and-statistics/statistics-definitions/least-squares-regression-line/>
40. The Durbin-Watson Test - Basic Statistics and Data Analysis. Basic Statistics and Data Analysis - Statistics Lecture Notes, Online MCQs [online]. Copyright © 2022. All Rights Reserved. [cit. 17.03.2022]. Dostupné z: <https://itfeature.com/time-series-analysis-and-forecasting/autocorrelation/durbin-watson-test>

Přílohy

Příloha 1 Datová základna	106
Příloha 2 Whiteův test heteroskedasticity.....	108
Příloha 3 Breusch-Paganův test normálního rozdělení.....	111
Příloha 4 Breusch-Godfreův test autokorelace	112
Příloha 5 Prognóza ex-post	113
Příloha 6 Data pro prognózu ex-ante 1. část.....	117
Příloha 7 Data pro prognózu ex-ante 2. část.....	117
Příloha 8 Data pro prognózu ex-ante 3. část.....	118
Příloha 9 Graf vývoje a trendu S&P500	118
Příloha 10 Graf vývoje a trendu ZLATO.....	119
Příloha 11 Graf vývoje a trendu ROPA.....	119
Příloha 12 Graf vývoje a trendu public_interest.....	120
Příloha 13 Graf vývoje a trendu median_confirmation_time	120
Příloha 14 Graf vývoje a trendu unique_addresses	121
Příloha 15 Graf vývoje a trendu Avg_block_size.....	121
Příloha 16 Graf vývoje a trendu NIKKEI225.....	122
Příloha 17 Graf vývoje a trendu DAX.....	122
Příloha 18 Graf vývoje a trendu FTSE100	123
Příloha 19 Nepoužitý model I.....	124
Příloha 20 Nepoužitý model II.....	125
Příloha 21 Nepoužitý model III	126

Příloha 2 Whiteův test heteroskedasticity

Whiteův test heteroskedasticity

OLS, za použití pozorování 2017-12-08:2021-10-29 (T = 204)

Závisle proměnná: uhat²

	koeficient	směr. chyba	t-podíl	p-hodnota	
const	0,00139969	0,00643401	0,2175	0,8286	
ld_miners_revenue	-0,0360333	0,0268460	-1,342	0,1852	
ld_ETHER_1	0,00706569	0,0160955	0,4390	0,6625	
ld_hash_rate	0,0835836	0,0319573	2,615	0,0116	**
Dummy_inc	-0,000204863	0,00589006	-0,03478	0,9724	
Dummy_dec	-0,00228970	0,00589124	-0,3887	0,6991	
ld_SP500_2	0,198969	0,151227	1,316	0,1939	
ld_ZLATO_1	-0,128162	0,105834	-1,211	0,2313	
ld_ROPA_4	0,0299588	0,0400313	0,7484	0,4575	
ld_public_inte~_2	0,000798209	0,0131426	0,06073	0,9518	
ld_median_conf_t~	0,000919193	0,0116574	0,07885	0,9374	
ld_unique_addr~_1	-0,0134356	0,0346518	-0,3877	0,6998	
ld_Avg_block_size	0,00722686	0,0238491	0,3030	0,7631	
ld_NIKKEI225	-0,160791	0,135761	-1,184	0,2416	
ld_DAX	0,199890	0,148951	1,342	0,1853	
ld_FTSE100_1	0,108756	0,114469	0,9501	0,3464	
ld_total_btc_1	-2,41726	21,4805	-0,1125	0,9108	
sq_ld_miners_rev~	0,0694811	0,0436166	1,593	0,1171	
X2_X3	0,161486	0,0596309	2,708	0,0091	***
X2_X4	0,0524315	0,100007	0,5243	0,6023	
X2_X5	-0,0226715	0,0172526	-1,314	0,1945	
X2_X6	-0,000710470	0,0218127	-0,03257	0,9741	
X2_X7	0,265080	0,324988	0,8157	0,4183	
X2_X8	0,270221	0,353652	0,7641	0,4482	
X2_X9	-0,00859756	0,0598340	-0,1437	0,8863	
X2_X10	-0,0379558	0,0289600	-1,311	0,1956	
X2_X11	0,0502996	0,0241752	2,081	0,0423	**
X2_X12	0,108629	0,0598898	1,814	0,0754	*
X2_X13	-0,0270271	0,0841090	-0,3213	0,7492	
X2_X14	0,777140	0,290252	2,677	0,0099	***
X2_X15	-1,00094	0,372228	-2,689	0,0096	***
X2_X16	-0,168094	0,439428	-0,3825	0,7036	
X2_X17	57,8966	35,9501	1,610	0,1132	
sq_ld_ETHER_1	0,0234601	0,0275340	0,8520	0,3980	
X3_X4	-0,0253910	0,0734560	-0,3457	0,7310	
X3_X5	0,00443760	0,0121829	0,3642	0,7171	
X3_X6	0,0198555	0,0154700	1,283	0,2049	
X3_X7	-0,490623	0,240374	-2,041	0,0462	**
X3_X8	0,229998	0,240786	0,9552	0,3438	
X3_X9	0,00284526	0,0976824	0,02913	0,9769	
X3_X10	-0,0406155	0,0242708	-1,673	0,1001	
X3_X11	0,0212797	0,0241472	0,8812	0,3822	
X3_X12	-0,0308517	0,0747727	-0,4126	0,6816	
X3_X13	-0,0182727	0,0754635	-0,2421	0,8096	
X3_X14	0,0557754	0,284653	0,1959	0,8454	
X3_X15	-0,114713	0,369004	-0,3109	0,7571	
X3_X16	-0,493288	0,294411	-1,676	0,0997	*
X3_X17	-8,37697	21,9522	-0,3816	0,7043	
sq_ld_hash_rate	-0,00601667	0,0798595	-0,07534	0,9402	
X4_X5	-0,0267634	0,0258710	-1,034	0,3056	
X4_X6	0,00124699	0,0273287	0,04563	0,9638	
X4_X7	0,605540	0,389343	1,555	0,1258	
X4_X8	-0,873248	0,453156	-1,927	0,0593	*
X4_X9	-0,257467	0,137188	-1,877	0,0661	*

X4_X10	0,0345594	0,0474387	0,7285	0,4695	
X4_X11	0,0233451	0,0398079	0,5864	0,5601	
X4_X12	-0,0526259	0,0900831	-0,5842	0,5616	
X4_X13	0,0679134	0,0974041	0,6972	0,4887	
X4_X14	-0,216824	0,552468	-0,3925	0,6963	
X4_X15	0,820617	0,526772	1,558	0,1252	
X4_X16	0,161041	0,556191	0,2895	0,7733	
X4_X17	-117,412	41,3213	-2,841	0,0064	***
X5_X6	0,000730723	0,00534672	0,1367	0,8918	
X5_X7	-0,00123608	0,0814179	-0,01518	0,9879	
X5_X8	0,0374625	0,0611353	0,6128	0,5426	
X5_X9	-0,0258648	0,0310514	-0,8330	0,4086	
X5_X10	0,00104039	0,0107487	0,09679	0,9233	
X5_X11	-0,0112826	0,00820775	-1,375	0,1750	
X5_X12	-0,0156121	0,0212202	-0,7357	0,4651	
X5_X13	-0,0120535	0,0188019	-0,6411	0,5242	
X5_X14	0,0544707	0,0879251	0,6195	0,5382	
X5_X15	0,000440432	0,108016	0,004077	0,9968	
X5_X16	-0,0840656	0,0875647	-0,9600	0,3414	
X5_X17	1,68004	8,06418	0,2083	0,8358	
X6_X7	-0,0734627	0,0779934	-0,9419	0,3505	
X6_X8	0,0711298	0,0849999	0,8368	0,4064	
X6_X9	-0,0472249	0,0297257	-1,589	0,1181	
X6_X10	-0,00365226	0,0101756	-0,3589	0,7211	
X6_X11	0,00546366	0,00814071	0,6712	0,5050	
X6_X12	-0,0245332	0,0247677	-0,9905	0,3264	
X6_X13	-0,0139712	0,0165379	-0,8448	0,4020	
X6_X14	0,0704430	0,0901975	0,7810	0,4383	
X6_X15	-0,148121	0,108283	-1,368	0,1771	
X6_X16	-0,0632270	0,0999427	-0,6326	0,5297	
X6_X17	5,84852	8,01099	0,7301	0,4686	
sq_ld_SP500_2	-1,04434	0,795753	-1,312	0,1950	
X7_X8	0,769995	1,20881	0,6370	0,5269	
X7_X9	0,0172445	0,429275	0,04017	0,9681	
X7_X10	0,268392	0,180642	1,486	0,1433	
X7_X11	0,343530	0,188462	1,823	0,0740	*
X7_X12	0,909366	0,471471	1,929	0,0591	*
X7_X13	-0,0897363	0,423382	-0,2120	0,8330	
X7_X14	0,296639	1,23574	0,2401	0,8112	
X7_X15	1,80196	1,70455	1,057	0,2952	
X7_X16	-2,17692	1,23644	-1,761	0,0841	*
X7_X17	-251,302	198,028	-1,269	0,2100	
sq_ld_ZLATO_1	-0,756692	0,687974	-1,100	0,2764	
X8_X9	-0,135362	0,416257	-0,3252	0,7463	
X8_X10	-0,226814	0,143873	-1,576	0,1209	
X8_X11	-0,0804974	0,176502	-0,4561	0,6502	
X8_X12	0,122033	0,450612	0,2708	0,7876	
X8_X13	0,201567	0,342653	0,5883	0,5589	
X8_X14	0,429561	1,85209	0,2319	0,8175	
X8_X15	-2,37668	2,01156	-1,182	0,2427	
X8_X16	1,18236	1,23327	0,9587	0,3421	
X8_X17	109,074	151,119	0,7218	0,4736	
sq_ld_ROPA_4	-0,00715707	0,0171214	-0,4180	0,6776	
X9_X10	-0,0142807	0,0404263	-0,3533	0,7253	
X9_X11	0,00172426	0,0457886	0,03766	0,9701	
X9_X12	-0,0498362	0,150579	-0,3310	0,7420	
X9_X13	-0,141694	0,137581	-1,030	0,3077	
X9_X14	0,364563	0,692336	0,5266	0,6007	
X9_X15	-0,862562	0,730884	-1,180	0,2432	
X9_X16	-0,368096	0,361113	-1,019	0,3127	

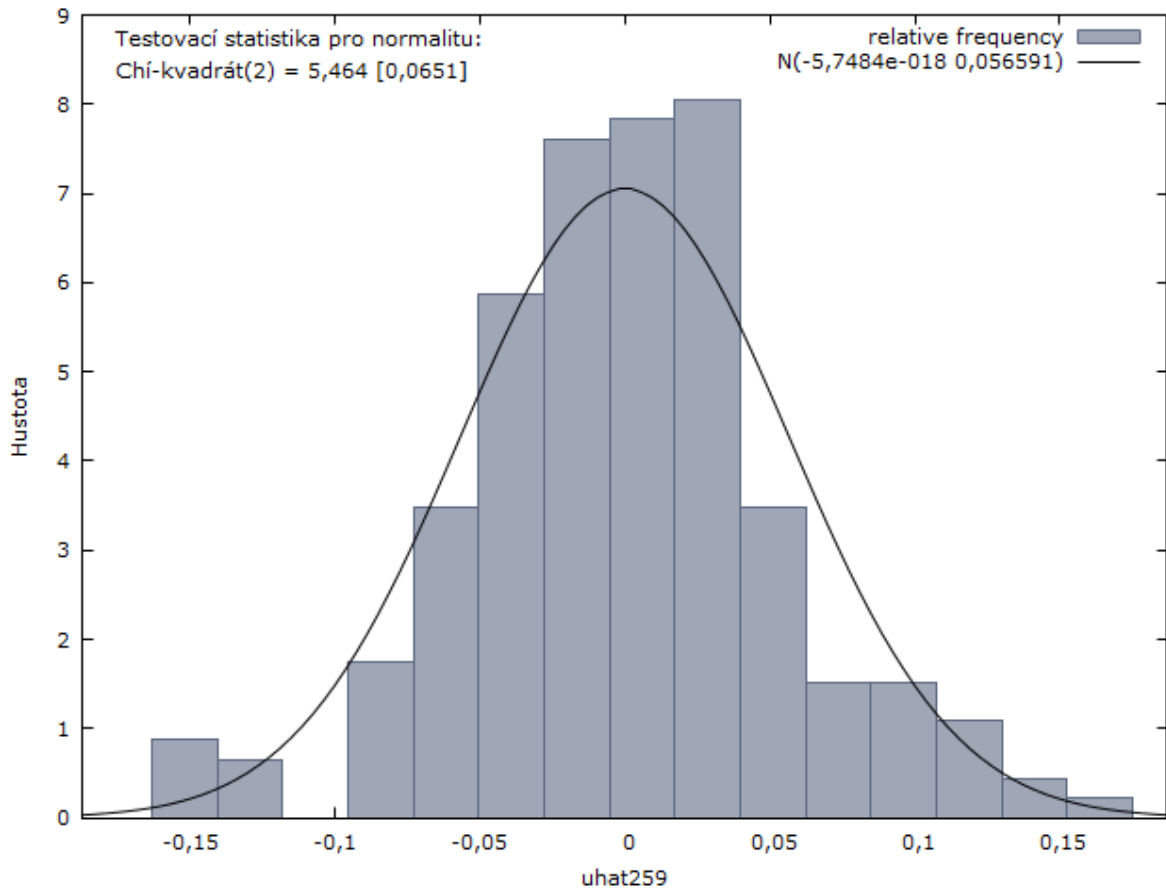
X9_X17	18,3941	46,1526	0,3985	0,6918	
sq_ld_public_i~_2	0,0116338	0,0100715	1,155	0,2532	
X10_X11	0,0167938	0,0158233	1,061	0,2934	
X10_X12	-0,0103290	0,0406018	-0,2544	0,8002	
X10_X13	-0,0810051	0,0479082	-1,691	0,0967	*
X10_X14	-0,0678131	0,215843	-0,3142	0,7546	
X10_X15	-0,114779	0,234837	-0,4888	0,6270	
X10_X16	0,0713133	0,182520	0,3907	0,6976	
X10_X17	-2,45814	12,1802	-0,2018	0,8408	
sq_ld_median_con~	-0,00551857	0,00827213	-0,6671	0,5076	
X11_X12	-0,0320933	0,0476722	-0,6732	0,5037	
X11_X13	0,100267	0,0347624	2,884	0,0057	***
X11_X14	0,123152	0,197605	0,6232	0,5358	
X11_X15	-0,109240	0,170005	-0,6426	0,5233	
X11_X16	0,138717	0,189264	0,7329	0,4668	
X11_X17	-5,25983	15,4557	-0,3403	0,7350	
sq_ld_unique_a~_1	-0,00692851	0,0899090	-0,07706	0,9389	
X12_X13	0,188451	0,0910923	2,069	0,0435	**
X12_X14	0,660237	0,479788	1,376	0,1746	
X12_X15	-0,137905	0,541648	-0,2546	0,8000	
X12_X16	0,462516	0,471218	0,9815	0,3308	
X12_X17	14,9656	42,8302	0,3494	0,7282	
sq_ld_Avg_block~	-0,0423084	0,0485990	-0,8706	0,3879	
X13_X14	-0,00103359	0,466335	-0,002216	0,9982	
X13_X15	0,258200	0,513968	0,5024	0,6175	
X13_X16	0,329116	0,332617	0,9895	0,3269	
X13_X17	-1,93808	29,3639	-0,06600	0,9476	
sq_ld_NIKKEI225	1,28599	1,18464	1,086	0,2826	
X14_X15	-2,83178	2,57485	-1,100	0,2764	
X14_X16	0,0279665	1,77775	0,01573	0,9875	
X14_X17	200,693	204,148	0,9831	0,3300	
sq_ld_DAX	0,506442	1,55238	0,3262	0,7455	
X15_X16	1,04848	1,95296	0,5369	0,5936	
X15_X17	-282,307	197,332	-1,431	0,1584	
sq_ld_FTSE100_1	1,10185	0,798124	1,381	0,1732	
X16_X17	-121,853	160,143	-0,7609	0,4501	
sq_ld_total_btc_1	3648,06	19665,3	0,1855	0,8535	

Neadjustovaný koeficient determinace = 0,847291

Testovací statistika: $TR^2 = 172,847313$,

s p-hodnotou = $P(\text{Chi-kvadrát}(150) > 172,847313) = 0,097567$

Příloha 3 Breusch-Paganův test normálního rozdělení



Frekvenční rozdělení pro uhat259, poz. 6-209
 počet tříd = 15, střední hodnota = -5,7484e-018, so = 0,0565911

interval	střed	frequence	rel.	kum.
< -0,14051	-0,15178	4	1,96%	1,96%
-0,14051 - -0,11797	-0,12924	3	1,47%	3,43%
-0,11797 - -0,095431	-0,10670	0	0,00%	3,43%
-0,095431 - -0,072893	-0,084162	8	3,92%	7,35% *
-0,072893 - -0,050354	-0,061623	16	7,84%	15,20% **
-0,050354 - -0,027815	-0,039084	27	13,24%	28,43% ****
-0,027815 - -0,0052764	-0,016546	35	17,16%	45,59% *****
-0,0052764 - 0,017262	0,0059930	36	17,65%	63,24% *****
0,017262 - 0,039801	0,028532	37	18,14%	81,37% *****
0,039801 - 0,062340	0,051070	16	7,84%	89,22% **
0,062340 - 0,084879	0,073609	7	3,43%	92,65% *
0,084879 - 0,10742	0,096148	7	3,43%	96,08% *
0,10742 - 0,12996	0,11869	5	2,45%	98,53%
0,12996 - 0,15249	0,14123	2	0,98%	99,51%
>= 0,15249	0,16376	1	0,49%	100,00%

Test nulové hypotézy normálního rozdělení:
 Chi-kvadrát(2) = 5,464 s p-hodnotou 0,06510

Příloha 4 Breusch-Godfreyův test autokorelace

Breusch-Godfreyův test pro autokorelaci až do řádu 10
 OLS, za použití pozorování 2017-12-08:2021-10-29 (T = 204)
 Závisle proměnná: uhat

	koeficient	směr. chyba	t-podíl	p-hodnota	
const	-0,00167388	0,0152514	-0,1098	0,9127	
ld_miners_revenue	0,000779497	0,0365396	0,02133	0,9830	
ld_ETHER_1	0,0417032	0,0355755	1,172	0,2427	
ld_hash_rate	-0,0175806	0,0563361	-0,3121	0,7554	
Dummy_inc	-0,00346950	0,0106139	-0,3269	0,7441	
Dummy_dec	-0,00257374	0,0109928	-0,2341	0,8152	
ld_SP500_2	0,00950523	0,150005	0,06337	0,9495	
ld_ZLATO_1	-0,0412131	0,163280	-0,2524	0,8010	
ld_ROPA_4	-0,000953965	0,0311515	-0,03062	0,9756	
ld_public_inte~_2	0,00617410	0,0203567	0,3033	0,7620	
ld_median_conf_t~	-0,00165433	0,0195081	-0,08480	0,9325	
ld_unique_addr~_1	-0,00266276	0,0535722	-0,04970	0,9604	
ld_Avg_block_size	-0,0130710	0,0454296	-0,2877	0,7739	
ld_NIKKEI225	-0,0722017	0,218610	-0,3303	0,7416	
ld_DAX	0,0405638	0,226716	0,1789	0,8582	
ld_FTSE100_1	-0,0345725	0,172219	-0,2007	0,8411	
ld_total_btc_1	6,61172	20,9809	0,3151	0,7530	
uhat_1	-0,135776	0,0816885	-1,662	0,0983	*
uhat_2	0,0168872	0,0808845	0,2088	0,8349	
uhat_3	-0,0106532	0,0776609	-0,1372	0,8910	
uhat_4	0,190132	0,0797052	2,385	0,0181	**
uhat_5	0,00206256	0,0787193	0,02620	0,9791	
uhat_6	0,102631	0,0778684	1,318	0,1892	
uhat_7	0,0229476	0,0799494	0,2870	0,7744	
uhat_8	-0,0609970	0,0774497	-0,7876	0,4320	
uhat_9	-0,0702327	0,0787698	-0,8916	0,3738	
uhat_10	-0,0571172	0,0771824	-0,7400	0,4603	

Neadjustovaný koeficient determinace = 0,060598

Testovací statistika: LMF = 1,141780,
 s p-hodnotou = $P(F(10,177) > 1,14178) = 0,334$

Alternativní statistika: $TR^2 = 12,362054$,
 s p-hodnotou = $P(\text{Chí-kvadrát}(10) > 12,3621) = 0,262$

Ljung-Box $Q' = 11,3707$,
 s p-hodnotou = $P(\text{Chí-kvadrát}(10) > 11,3707) = 0,329$

Příloha 5 Prognóza ex-post

Pro 95% konfidenční intervaly, $t(187, 0,025) = 1,973$

	ld_BTC	předpověď	směr. chyba	95% konfidenční interval
2017-11-03				
2017-11-10	-0,086234			
2017-11-17	0,159456			
2017-11-24	0,062834			
2017-12-01	0,280029			
2017-12-08	0,409277	0,356130	0,061471	0,234864 - 0,477397
2017-12-15	0,080478	0,134536	0,058380	0,019367 - 0,249704
2017-12-22	-0,221761	-0,069983	0,058828	-0,186035 - 0,046069
2017-12-29	0,024639	-0,082023	0,059545	-0,199489 - 0,035443
2018-01-05	0,152233	0,033439	0,058861	-0,082677 - 0,149556
2018-01-12	-0,204741	-0,153451	0,058384	-0,268627 - -0,038274
2018-01-19	-0,183858	-0,189914	0,059719	-0,307724 - -0,072104
2018-01-26	-0,036496	-0,185097	0,059386	-0,302250 - -0,067943
2018-02-02	-0,232431	-0,191919	0,058358	-0,307043 - -0,076795
2018-02-09	-0,013347	-0,121367	0,059001	-0,237760 - -0,004975
2018-02-16	0,159210	0,092148	0,060272	-0,026752 - 0,211048
2018-02-23	-0,002215	-0,026562	0,059934	-0,144796 - 0,091672
2018-03-02	0,080915	0,065850	0,058428	-0,049412 - 0,181112
2018-03-09	-0,172731	-0,137725	0,059749	-0,255593 - -0,019856
2018-03-16	-0,111925	-0,063358	0,060129	-0,181976 - 0,055261
2018-03-23	0,075853	0,041462	0,059506	-0,075927 - 0,158852
2018-03-30	-0,265133	-0,192015	0,059143	-0,308687 - -0,075342
2018-04-06	-0,034012	0,018390	0,059953	-0,099880 - 0,136660
2018-04-13	0,176055	0,173846	0,058573	0,058297 - 0,289395
2018-04-20	0,116254	-0,001269	0,058869	-0,117402 - 0,114865
2018-04-27	0,006328	0,088040	0,058076	-0,026528 - 0,202607
2018-05-04	0,081997	0,102764	0,057585	-0,010835 - 0,216363
2018-05-11	-0,141950	-0,104268	0,057869	-0,218429 - 0,009893
2018-05-18	-0,019809	-0,038054	0,058507	-0,153472 - 0,077364
2018-05-25	-0,099383	-0,127826	0,059130	-0,244473 - -0,011179
2018-06-01	0,007374	0,009174	0,058005	-0,105253 - 0,123602
2018-06-08	0,013808	-0,045196	0,059241	-0,162063 - 0,071671
2018-06-15	-0,175694	-0,100180	0,058532	-0,215647 - 0,015287
2018-06-22	-0,053245	-0,057328	0,058192	-0,172125 - 0,057468
2018-06-29	0,023250	-0,001139	0,057973	-0,115503 - 0,113226
2018-07-06	0,062140	0,092510	0,058069	-0,022046 - 0,207065
2018-07-13	-0,059896	0,066309	0,060703	-0,053442 - 0,186059
2018-07-20	0,165411	0,105885	0,059375	-0,011247 - 0,223016
2018-07-27	0,109623	0,086530	0,058371	-0,028621 - 0,201681
2018-08-03	-0,098826	-0,140620	0,057667	-0,254382 - -0,026858
2018-08-10	-0,187578	-0,097977	0,057742	-0,211887 - 0,015933
2018-08-17	0,069066	-0,001973	0,058166	-0,116719 - 0,112773
2018-08-24	0,015877	0,032454	0,057653	-0,081280 - 0,146188
2018-08-31	0,047307	0,035836	0,057635	-0,077863 - 0,149535
2018-09-07	-0,092534	-0,073836	0,057573	-0,187413 - 0,039741
2018-09-14	0,012900	0,002225	0,058526	-0,113232 - 0,117682
2018-09-21	0,041125	0,012508	0,058082	-0,102071 - 0,127088
2018-09-28	-0,019446	0,019098	0,058408	-0,096125 - 0,134322
2018-10-05	-0,003946	-0,007562	0,058159	-0,122295 - 0,107170
2018-10-12	-0,063537	-0,027324	0,058293	-0,142321 - 0,087673
2018-10-19	0,031023	0,032162	0,057942	-0,082142 - 0,146466
2018-10-26	0,003422	0,024442	0,058128	-0,090229 - 0,139113
2018-11-02	-0,008635	0,015243	0,058016	-0,099207 - 0,129693
2018-11-09	-0,002351	0,022873	0,058183	-0,091906 - 0,137651
2018-11-16	-0,139101	-0,086170	0,057393	-0,199392 - 0,027051
2018-11-23	-0,252131	-0,110889	0,057766	-0,224846 - 0,003069

2018-11-30	-0,074564	-0,030208	0,059095	-0,146786	-0,086370
2018-12-07	-0,162398	-0,044083	0,057934	-0,158372	-0,070206
2018-12-14	-0,056069	-0,031580	0,060175	-0,150288	-0,087129
2018-12-21	0,183418	0,168751	0,059668	0,051041	-0,286460
2018-12-28	0,012683	-0,051062	0,058525	-0,166516	-0,064391
2019-01-04	-0,017594	-0,033333	0,059568	-0,150846	-0,084179
2019-01-11	-0,049517	-0,058184	0,057886	-0,172377	-0,056010
2019-01-18	-0,007687	-0,000476	0,058087	-0,115065	-0,114114
2019-01-25	-0,012742	-0,003114	0,057370	-0,116289	-0,110061
2019-02-01	-0,035625	0,021277	0,057790	-0,092728	-0,135281
2019-02-08	0,052279	0,053103	0,057899	-0,061116	-0,167323
2019-02-15	-0,015414	0,054627	0,058158	-0,060103	-0,169358
2019-02-22	0,100083	0,101366	0,058241	-0,013528	-0,216261
2019-03-01	-0,035070	-0,001875	0,058344	-0,116973	-0,113222
2019-03-08	0,009661	0,029500	0,057741	-0,084408	-0,143409
2019-03-15	0,015410	0,056940	0,057226	-0,055952	-0,169832
2019-03-22	0,020537	0,027808	0,057276	-0,085183	-0,140800
2019-03-29	0,026561	0,085290	0,058312	-0,029743	-0,200324
2019-04-05	0,208745	0,198602	0,057769	0,084640	-0,312563
2019-04-12	0,007416	0,052798	0,058558	-0,062721	-0,168318
2019-04-19	0,040933	0,059075	0,057628	-0,054610	-0,172760
2019-04-26	-0,025045	0,036970	0,057474	-0,076411	-0,150351
2019-05-03	0,092123	0,093919	0,057406	-0,019328	-0,207166
2019-05-10	0,114409	0,084693	0,058040	-0,029804	-0,199189
2019-05-17	0,148835	0,154182	0,057923	0,039915	-0,268449
2019-05-24	0,083508	0,085011	0,058869	-0,031122	-0,201145
2019-05-31	0,068088	-0,015127	0,058166	-0,129872	-0,099619
2019-06-07	-0,068598	-0,025215	0,058881	-0,141371	-0,090941
2019-06-14	0,083822	0,082655	0,057923	-0,031611	-0,196921
2019-06-21	0,161317	0,131095	0,059106	0,014496	-0,247694
2019-06-28	0,190151	0,151028	0,059644	0,033366	-0,268690
2019-07-05	-0,116194	-0,048589	0,060035	-0,167021	-0,069844
2019-07-12	0,069965	-0,063756	0,058706	-0,179567	-0,052054
2019-07-19	-0,115133	-0,086949	0,058619	-0,202588	-0,028690
2019-07-26	-0,066375	-0,066708	0,059101	-0,183298	-0,049881
2019-08-02	0,067753	0,046042	0,057931	-0,068240	-0,160324
2019-08-09	0,118329	0,007808	0,057794	-0,106203	-0,121820
2019-08-16	-0,135595	-0,114744	0,058191	-0,229539	-0,000050
2019-08-23	0,005596	-0,047097	0,057527	-0,160581	-0,066388
2019-08-30	-0,082914	-0,033715	0,058555	-0,149228	-0,081799
2019-09-06	0,072883	0,067800	0,058127	-0,046869	-0,182470
2019-09-13	0,005853	-0,030139	0,057747	-0,144060	-0,083781
2019-09-20	-0,019342	-0,073655	0,057575	-0,187235	-0,039924
2019-09-27	-0,215923	-0,184992	0,058041	-0,299491	-0,070493
2019-10-04	-0,004565	0,004310	0,058490	-0,111075	-0,119695
2019-10-11	0,013476	0,000364	0,058318	-0,114683	-0,115410
2019-10-18	-0,038617	-0,065698	0,057528	-0,179186	-0,047789
2019-10-25	0,085943	0,025142	0,059335	-0,091909	-0,142193
2019-11-01	0,065323	0,117887	0,059894	-0,000268	-0,236042
2019-11-08	-0,054421	-0,021310	0,057644	-0,135026	-0,092406
2019-11-15	-0,035488	-0,030525	0,057924	-0,144794	-0,083745
2019-11-22	-0,147426	-0,102065	0,057618	-0,215731	-0,011600
2019-11-29	0,061357	0,086222	0,058490	-0,029162	-0,201607
2019-12-06	-0,028645	-0,054483	0,057633	-0,168178	-0,059212
2019-12-13	-0,039580	-0,045120	0,057369	-0,158294	-0,068055
2019-12-20	-0,009072	0,015771	0,057339	-0,097344	-0,128885
2019-12-27	0,007991	0,008476	0,058276	-0,106486	-0,123437
2020-01-03	0,009306	-0,002749	0,057874	-0,116920	-0,111422
2020-01-10	0,111520	0,106656	0,058246	-0,008247	-0,221560
2020-01-17	0,085484	0,058785	0,057974	-0,055582	-0,173152

2020-01-24	-0,054514	-0,001916	0,057712	-0,115765	- 0,111934
2020-01-31	0,102297	0,078329	0,057687	-0,035472	- 0,192130
2020-02-07	0,049434	0,076534	0,058522	-0,038914	- 0,191982
2020-02-14	0,055840	0,078641	0,059774	-0,039276	- 0,196559
2020-02-21	-0,066880	-0,083968	0,058923	-0,200207	- 0,032272
2020-02-28	-0,107818	-0,132731	0,060346	-0,251777	- -0,013684
2020-03-06	0,048947	-0,007451	0,060565	-0,126929	- 0,112027
2020-03-13	-0,483833	-0,435989	0,067057	-0,568275	- -0,303704
2020-03-20	0,095350	0,154598	0,066162	0,024078	- 0,285119
2020-03-27	0,027161	0,085340	0,064927	-0,042743	- 0,213424
2020-04-03	0,056385	0,030932	0,064917	-0,097132	- 0,158996
2020-04-10	0,019087	-0,012565	0,060615	-0,132142	- 0,107011
2020-04-17	0,023633	0,056121	0,061073	-0,064360	- 0,176602
2020-04-24	0,064983	0,063453	0,062247	-0,059344	- 0,186250
2020-05-01	0,162031	0,192284	0,060696	0,072548	- 0,312021
2020-05-08	0,105313	0,017990	0,069577	-0,119266	- 0,155246
2020-05-15	-0,052088	-0,215852	0,065591	-0,345245	- -0,086458
2020-05-22	-0,015504	0,004755	0,063000	-0,119527	- 0,129036
2020-05-29	0,027768	0,007265	0,059196	-0,109513	- 0,124043
2020-06-05	0,020784	0,065095	0,058926	-0,051150	- 0,181339
2020-06-12	-0,017925	-0,018691	0,059908	-0,136872	- 0,099491
2020-06-19	-0,018641	-0,109012	0,059044	-0,225490	- 0,007466
2020-06-26	-0,013497	-0,048795	0,058538	-0,164275	- 0,066686
2020-07-03	-0,010004	0,049834	0,058129	-0,064839	- 0,164507
2020-07-10	0,024622	0,029945	0,057575	-0,083635	- 0,143525
2020-07-17	-0,014876	-0,021446	0,058391	-0,136635	- 0,093743
2020-07-24	0,041848	0,108837	0,058889	-0,007334	- 0,225009
2020-07-31	0,172666	0,120991	0,058946	0,004706	- 0,237276
2020-08-07	0,023009	0,005155	0,058999	-0,111234	- 0,121545
2020-08-14	0,013776	0,001334	0,057840	-0,112769	- 0,115437
2020-08-21	-0,022369	0,026751	0,058532	-0,088717	- 0,142220
2020-08-28	0,002413	-0,027989	0,058020	-0,142448	- 0,086469
2020-09-04	-0,095583	-0,076749	0,058055	-0,191275	- 0,037777
2020-09-11	-0,009546	-0,053745	0,057861	-0,167890	- 0,060400
2020-09-18	0,051941	0,032514	0,058774	-0,083432	- 0,148460
2020-09-25	-0,022842	-0,069805	0,059355	-0,186896	- 0,047286
2020-10-02	-0,011042	0,028642	0,058564	-0,086889	- 0,144172
2020-10-09	0,045655	0,056710	0,057589	-0,056897	- 0,170318
2020-10-16	0,023389	0,020430	0,057410	-0,092826	- 0,133685
2020-10-23	0,132734	0,125382	0,058352	0,010268	- 0,240495
2020-10-30	0,047858	0,026243	0,062199	-0,096458	- 0,148945
2020-11-06	0,139315	0,145552	0,060505	0,026191	- 0,264913
2020-11-13	0,045972	0,003841	0,060637	-0,115780	- 0,123462
2020-11-20	0,132931	0,104599	0,060079	-0,013920	- 0,223119
2020-11-27	-0,083942	0,003524	0,058526	-0,111932	- 0,118981
2020-12-04	0,088408	0,060134	0,057817	-0,053923	- 0,174191
2020-12-11	-0,037117	-0,011758	0,057887	-0,125954	- 0,102437
2020-12-18	0,248059	0,244135	0,058546	0,128639	- 0,359630
2020-12-25	0,065361	-0,023603	0,058734	-0,139470	- 0,092263
2021-01-01	0,173660	0,142416	0,058177	0,027648	- 0,257183
2021-01-08	0,325037	0,246209	0,059881	0,128081	- 0,364338
2021-01-15	-0,101223	-0,114462	0,061175	-0,235144	- 0,006219
2021-01-22	-0,108403	-0,146598	0,058927	-0,262845	- -0,030351
2021-01-29	0,035940	0,070747	0,058477	-0,044613	- 0,186108
2021-02-05	0,113800	0,028615	0,058908	-0,087593	- 0,144824
2021-02-12	0,213533	0,146637	0,059094	0,030060	- 0,263213
2021-02-19	0,165562	0,064440	0,058736	-0,051431	- 0,180311
2021-02-26	-0,189254	-0,040635	0,058374	-0,155791	- 0,074520
2021-03-05	0,053763	0,064916	0,058479	-0,050447	- 0,180279
2021-03-12	0,158446	0,116451	0,058356	0,001330	- 0,231571

2021-03-19	0,013517	0,059665	0,057255	-0,053284	- 0,172613
2021-03-26	-0,052666	-0,085817	0,058243	-0,200714	- 0,029080
2021-04-02	0,068524	0,084602	0,057543	-0,028914	- 0,198118
2021-04-09	-0,015135	-0,003993	0,058934	-0,120254	- 0,112267
2021-04-16	0,055814	0,079484	0,060022	-0,038923	- 0,197891
2021-04-23	-0,184538	-0,043964	0,059862	-0,162055	- 0,074127
2021-04-30	0,125147	0,004299	0,059494	-0,113067	- 0,121665
2021-05-07	-0,008550	0,007698	0,059568	-0,109814	- 0,125209
2021-05-14	-0,138657	-0,234878	0,059938	-0,353119	- -0,116636
2021-05-21	-0,291171	-0,163396	0,059548	-0,280868	- -0,045924
2021-05-28	-0,045760	-0,065679	0,061311	-0,186629	- 0,055271
2021-06-04	0,035317	0,058286	0,058646	-0,057407	- 0,173978
2021-06-11	0,010689	-0,025903	0,058365	-0,141041	- 0,089235
2021-06-18	-0,043285	0,021175	0,058348	-0,093929	- 0,136280
2021-06-25	-0,123996	-0,036217	0,059389	-0,153376	- 0,080941
2021-07-02	0,067559	0,043913	0,058909	-0,072298	- 0,160125
2021-07-09	0,000568	0,085522	0,060438	-0,033706	- 0,204750
2021-07-16	-0,074971	-0,047909	0,058599	-0,163508	- 0,067690
2021-07-23	0,065978	0,071779	0,057630	-0,041910	- 0,185467
2021-07-30	0,228752	0,163214	0,058541	0,047727	- 0,278700
2021-08-06	0,017225	0,013006	0,057810	-0,101037	- 0,127049
2021-08-13	0,109647	0,087158	0,057948	-0,027158	- 0,201474
2021-08-20	0,030043	0,038834	0,058101	-0,075783	- 0,153451
2021-08-27	-0,004450	-0,059255	0,058131	-0,173931	- 0,055420
2021-09-03	0,019122	0,053260	0,058984	-0,063100	- 0,169620
2021-09-10	-0,109168	-0,158626	0,058869	-0,274759	- -0,042494
2021-09-17	0,051780	0,088912	0,057851	-0,025212	- 0,203037
2021-09-24	-0,097647	-0,122453	0,058145	-0,237157	- -0,007749
2021-10-01	0,117030	0,095384	0,058314	-0,019654	- 0,210422
2021-10-08	0,113795	0,089094	0,057852	-0,025032	- 0,203220
2021-10-15	0,133828	0,081534	0,057598	-0,032092	- 0,195159
2021-10-22	-0,016402	0,057316	0,057624	-0,056361	- 0,170993
2021-10-29	0,025548	0,040456	0,057506	-0,072989	- 0,153900

Statistiky vyhodnocující předpověď using 204 observations

Střední chyba	-5,7484e-018
Odmocnina střední kvadratické chyby	0,054182
Střední absolutní chyba	0,041292
Střední procentuální chyba	-58,98
Střední absolutní procentuální chyba	206,23
Theilovo U	0,37872
Zastoupení vychýlení, UM	0
Zastoupení regrese, UR	0
Zastoupení disturbancí, UD	1

Příloha 6 Data pro prognózu ex-ante 1. část

	SP500			ZLATO			ROPA			public interest		
	$y = 0,0695x^2 - 6,1419x + 2828,5$			$y = 3,6856x + 1146,5$			$y = 0,0021x^2 + 0,4687x + 75,477$			$y = 0,0451x + 15,771$		
	odhad	ln	diff	odhad	ln	diff	odhad	ln	diff	odhad	ln	diff
	R ² = 0,9185			R ² = 0,8001			R ² = 0,31			R ² = 0,0266		
05.11.2021	4603,851	8,434605	-0,000375501	1920,476	7,560328	0,0737710932	69,66	4,24362626	0,2721297855	25,242	3,228509	0,0504554435
12.11.2021	4626,769	8,439614	0,005009014	1924,162	7,562246	0,0019172684	70,0754	4,24957181	0,0059455403	25,2871	3,230294	0,0017851104
19.11.2021	4650,025	8,444628	0,005013941	1927,847	7,564159	0,0019135995	70,495	4,25554179	0,0059699801	25,3322	3,232076	0,0017819295
26.11.2021	4673,421	8,449647	0,00501867	1931,533	7,566069	0,0019099447	70,9188	4,26153556	0,0059937753	25,3773	3,233855	0,0017787599
03.12.2021	4696,955	8,45467	0,005023203	1935,218	7,567975	0,0019063037	71,3468	4,26755249	0,0060169330	25,4224	3,235631	0,0017756015
10.12.2021	4720,629	8,459697	0,005027542	1938,904	7,569878	0,0019026766	71,779	4,27359195	0,0060394606	25,4675	3,237403	0,0017724543
17.12.2021	4744,442	8,464729	0,00503169	1942,59	7,571777	0,0018990633	72,2154	4,27965332	0,0060613654	25,5126	3,239172	0,0017693183
24.12.2021	4768,393	8,469765	0,005035649	1946,275	7,573673	0,0018954637	72,656	4,28573597	0,0060826548	25,5577	3,240939	0,0017661933
31.12.2021	4792,484	8,474804	0,005039423	1949,961	7,575565	0,0018918778	73,1008	4,29183931	0,0061033363	25,6028	3,242702	0,0017630794
07.01.2022	4816,713	8,479847	0,005043013	1953,646	7,577453	0,0018883053	73,5498	4,29796273	0,0061234172	25,6479	3,244462	0,0017599764
14.01.2022	4841,082	8,484894	0,005046421	1957,332	7,579338	0,0018847463	74,003	4,30410563	0,0061429051	25,693	3,246219	0,0017568843
21.01.2022	4865,59	8,489943	0,005049651	1961,018	7,581219	0,0018812007	74,4604	4,31026744	0,0061618075	25,7381	3,247972	0,0017538031
28.01.2022	4890,236	8,494996	0,005052704	1964,703	7,583096	0,0018776685	74,922	4,31644757	0,0061801319	25,7832	3,249723	0,0017507327
04.02.2022	4915,022	8,500051	0,005055584	1968,389	7,584971	0,0018741494	75,3878	4,32264546	0,0061978858	25,8283	3,251471	0,0017476730
11.02.2022	4939,946	8,50511	0,005058292	1972,074	7,586841	0,0018706436	75,8578	4,32886054	0,0062150768	25,8734	3,253215	0,0017446239
18.02.2022	4965,01	8,510171	0,005060831	1975,76	7,588708	0,0018671508	76,332	4,33509225	0,0062317124	25,9185	3,254957	0,0017415855
25.02.2022	4990,213	8,515234	0,005063202	1979,446	7,590572	0,0018636710	76,8104	4,34134005	0,0062478002	25,9636	3,256696	0,0017385577
04.03.2022	5015,554	8,520299	0,005065641	1983,131	7,592432	0,0018602042	77,293	4,3476034	0,0062633476	26,0087	3,258431	0,0017355403
11.03.2022	5041,035	8,525367	0,005067455	1986,817	7,594289	0,0018567503	77,7798	4,35388176	0,0062793222	26,0538	3,260164	0,0017325334
18.03.2022	5066,654	8,530436	0,00506934	1990,502	7,596142	0,0018533092	78,2708	4,36017461	0,0062928514	26,0989	3,261893	0,0017295730
25.03.2022	5092,413	8,535507	0,005071067	1994,188	7,597992	0,0018498808	78,766	4,36648143	0,0063068229	26,144	3,26362	0,0017265508
01.04.2022	5118,311	8,54058	0,005072639	1997,874	7,599839	0,0018464650	79,2654	4,37280172	0,0063202840	26,1891	3,265343	0,0017235750
08.04.2022	5144,347	8,545664	0,005074057	2001,559	7,601682	0,0018430619	79,769	4,37913496	0,0063332422	26,2342	3,267064	0,0017206094
15.04.2022	5170,523	8,550729	0,005075324	2005,245	7,603521	0,0018396712	80,2768	4,38548066	0,0063457048	26,2793	3,268782	0,0017176540
22.04.2022	5196,837	8,555806	0,005076443	2008,93	7,605358	0,0018362931	80,7888	4,39183834	0,0063576794	26,3244	3,270496	0,0017147087
29.04.2022	5223,291	8,560883	0,005077415	2012,616	7,607191	0,0018329273	81,305	4,39820752	0,0063691732	26,3695	3,272208	0,0017117735
06.05.2022	5249,884	8,565961	0,005078242	2016,302	7,60902	0,0018295738	81,8254	4,40458771	0,0063801936	26,4146	3,273917	0,0017088483
13.05.2022	5276,815	8,57104	0,005078927	2019,987	7,610846	0,0018262326	82,35	4,41097846	0,0063907478	26,4597	3,275623	0,0017059332
20.05.2022	5303,486	8,57612	0,005079471	2023,673	7,612669	0,0018229035	82,8788	4,4173793	0,0064008430	26,5048	3,277326	0,0017030279
27.05.2022	5330,495	8,581199	0,005079877	2027,358	7,614489	0,0018195866	83,4118	4,42378979	0,0064104865	26,5499	3,279026	0,0017001325
03.06.2022	5357,444	8,586228	0,005080147	2031,044	7,616305	0,0018162817	83,949	4,43020947	0,0064196854	26,595	3,280723	0,0016972470
10.06.2022	5384,932	8,59136	0,005080282	2034,73	7,618118	0,0018129888	84,4904	4,43663792	0,0064284468	26,6401	3,282418	0,0016943712
17.06.2022	5412,358	8,59644	0,005080286	2038,415	7,619928	0,0018097078	85,036	4,4430747	0,0064367778	26,6852	3,284109	0,0016915052
24.06.2022	5439,924	8,60152	0,005080159	2042,101	7,621734	0,0018064387	85,5858	4,44951938	0,0064446853	26,7303	3,285798	0,0016886488
01.07.2022	5467,628	8,6066	0,005079904	2045,786	7,623538	0,0018031814	86,1398	4,45597156	0,0064521763	26,7754	3,287484	0,0016858021

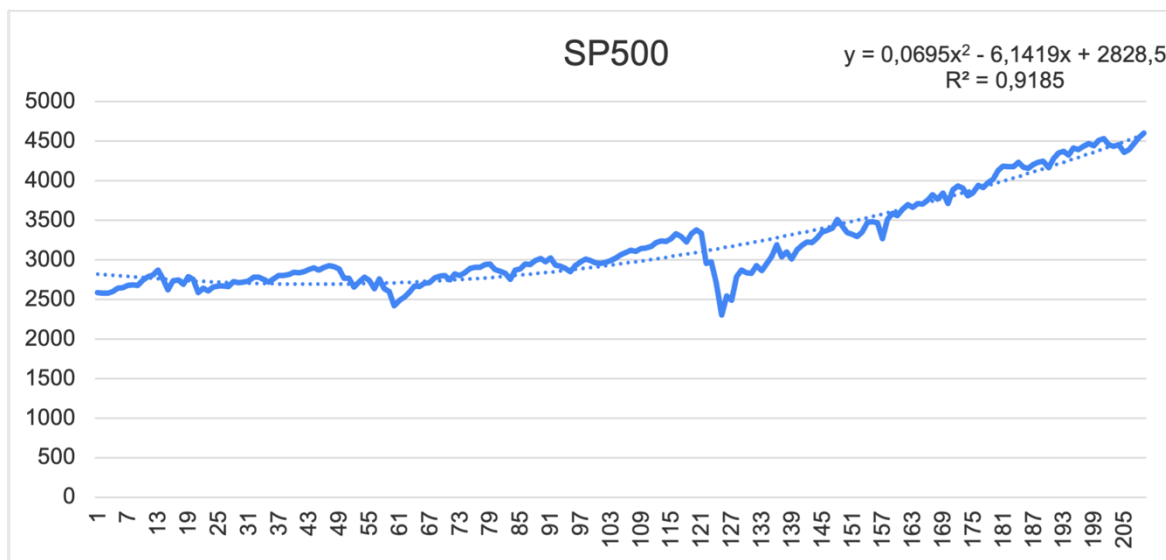
Příloha 7 Data pro prognózu ex-ante 2. část

	median conf time			unique addresses			avg block size			NIKKEI 225		
	$y = 0,0041x + 9,8418$			$y = 10,439x^2 - 1550,1x + 602972$			$y = 0,0019x + 0,92$			$y = 33,899x + 20044$		
	odhad	ln	diff	odhad	ln	diff	odhad	ln	diff	odhad	ln	diff
	R ² = 0,0059			R ² = 0,5206			R ² = 0,4557			R ² = 0,4529		
05.11.2021	10,7028	2,370505	0,5622166183	737810,9	13,511443	-0,0272728334	1,319	0,276874	0,2117379488	27162,79	10,2096	-0,0617405999
12.11.2021	10,7069	2,370888	0,0003830040	740655,62	13,515291	0,0038482069	1,3209	0,278313	0,0014394487	27196,69	10,21085	0,0012472159
19.11.2021	10,7111	2,371271	0,0003828573	743521,22	13,519153	0,0038615352	1,3228	0,279751	0,0014373797	27230,59	10,2121	0,0012456623
26.11.2021	10,7151	2,371654	0,0003827108	746407,69	13,523027	0,0038746528	1,3247	0,281186	0,0014353166	27264,49	10,21334	0,0012441126
03.12.2021	10,7192	2,372037	0,0003825644	749315,04	13,526915	0,0038875610	1,3266	0,282619	0,0014332594	27298,39	10,21458	0,0012425667
10.12.2021	10,7233	2,372419	0,0003824181	752243,28	13,530815	0,0039002610	1,3285	0,28405	0,0014312081	27332,29	10,21582	0,0012410325
17.12.2021	10,7274	2,372801	0,0003822719	755192,38	13,534728	0,0039127544	1,3304	0,28548	0,0014291627	27366,18	10,21706	0,0012394864
24.12.2021	10,7315	2,373183	0,0003821258	758162,37	13,538653	0,0039250424	1,3323	0,286907	0,0014271231	27400,08	10,2183	0,0012379520
31.12.2021	10,7356	2,373565	0,0003819799	761153,24	13,542459	0,0039371265	1,3342	0,288332	0,0014250893	27433,98	10,21954	0,0012364213
07.01.2022	10,7397	2,373947	0,0003818340	764164,98	13,546339	0,003949080	1,3361	0,289755	0,0014230613	27467,88	10,22077	0,0012348945
14.01.2022	10,7438	2,374329	0,0003816883	767197,6	13,5505	0,0039606884	1,338	0,291176	0,0014210391	27501,78	10,22201	0,0012333714
21.01.2022	10,7479	2,374711	0,0003815426	770251,11	13,554472	0,0039721690	1,3399	0,292595	0,0014190226	27535,68	10,22324	0,0012318521
28.01.2022	10,752	2,375092	0,0003813971	773325,48	13,558455	0,0039834513	1,3418	0,294012	0,0014170118	27569,58	10,22447	0,0012303365
04.02.2022	10,7561	2,375473	0,0003812517	776420,73	13,56245	0,0039945368	1,3437	0,295427	0,0014150068	27603,48	10,2257	0,0012288246
11.02.2022	10,7602	2,375854	0,0003811064	779536,86	13,566455	0,0040054269	1,3456	0,29684	0,0014130073	27637,38	10,22692	0,0012273165
18.02.2022	10,7643	2,376235	0,0003809612	782673,88	13,570471	0,0040161230	1,3475	0,298251	0,0014110136	27671,28	10,22815	0,0012258120
25.02.2022	10,7684	2,376616	0,0003808162	785831,76	13,574498	0,0040266266	1,3494	0,29966	0,0014090254	27705,17	10,22937	0,0012243112
04.03.2022	10,7725	2,376997	0,0003806712	789010,53	13,578535	0,0040369392	1,3513	0,301067	0,0014070429	27739,07	10,2306	0,0012228141
11.03.2022	10,7766	2,377377	0,0003805263	792210,18	13,582582	0,0040470623	1,3532	0,302472	0,0014050659	27772,97	10,23182	0,0012213207
18.03.2022	10,7807	2,377757	0,0003803816	795430,7	13,586639	0,0040569974	1,3551	0,303875	0,0014030944	27806,87	10,23304	0,0012198309
25.03.2022	10,7848	2,378138	0,0003802370	798672,1								

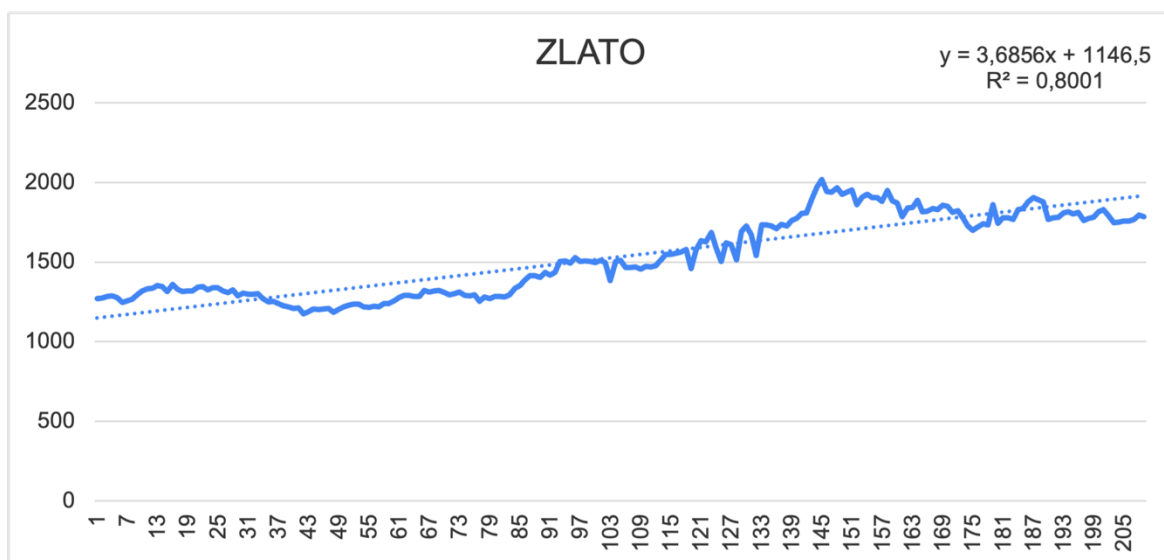
Příloha 8 Data pro prognózu ex-ante 3. část

	DAX			FTSE100			total_btc			dummy_inc	dummy_dec
	$y = 13,872 + 11413$			$y = 0,047x^2 - 14,669x + 7831,3$							
	$R^2 = 0,3436$			$R^2 = 0,3184$							
odhad	ln	diff	odhad	ln	diff	odhad	ln	diff	odhad	odhad	
05.11.2021	14326,12	9,569884	-0,0919462631	6823,51	8,828129	-0,0589115125	18863856	16,75276	0,000339330720	1	0
12.11.2021	14339,99	9,570808	0,0009678328	6828,628	8,828879	0,0007497727	18870256	16,7531	0,000339215614	1	0
19.11.2021	14353,86	9,571774	0,0009668970	6833,84	8,829642	0,0007629661	18876656	16,75344	0,000339100585	1	0
26.11.2021	14367,74	9,57274	0,0009659630	6839,146	8,830418	0,0007761290	18883056	16,75378	0,000338985635	0	1
03.12.2021	14381,61	9,573705	0,0009650308	6844,546	8,831207	0,0007892607	18889456	16,75411	0,000338870763	0	0
10.12.2021	14395,48	9,57467	0,0009641004	6850,04	8,83201	0,0008023609	18895856	16,75445	0,000338755968	1	0
17.12.2021	14409,35	9,575633	0,0009631718	6855,628	8,832825	0,0008154291	18902256	16,75479	0,000338641252	1	0
24.12.2021	14423,22	9,576595	0,0009622450	6861,31	8,833654	0,0008284648	18908656	16,75513	0,000338526612	1	0
31.12.2021	14437,1	9,577556	0,0009613200	6867,086	8,834495	0,0008414676	18915056	16,75547	0,000338412051	0	0
07.01.2022	14450,97	9,578517	0,0009603967	6872,956	8,83535	0,0008544370	18921456	16,75581	0,000338297567	1	0
14.01.2022	14464,84	9,579476	0,0009594753	6878,92	8,836217	0,0008673726	18927856	16,75615	0,000338183160	0	1
21.01.2022	14478,71	9,580435	0,0009585555	6884,978	8,837097	0,0008802739	18934256	16,75648	0,000338068831	0	0
28.01.2022	14492,58	9,581392	0,0009576376	6891,13	8,83799	0,0008931406	18940656	16,75682	0,000337954579	0	1
04.02.2022	14506,46	9,582349	0,0009567214	6897,376	8,838896	0,0009059720	18947056	16,75716	0,000337840405	0	0
11.02.2022	14520,33	9,583305	0,0009558070	6903,716	8,839815	0,0009187679	18953456	16,7575	0,000337726307	1	0
18.02.2022	14534,2	9,58426	0,0009548943	6910,15	8,840747	0,0009315279	18959856	16,75783	0,000337612286	0	0
25.02.2022	14548,07	9,585214	0,0009539833	6916,678	8,841691	0,0009442513	18966256	16,75817	0,000337498343	1	0
04.03.2022	14561,94	9,586167	0,0009530741	6923,3	8,842648	0,0009569380	18972656	16,75851	0,000337384476	1	0
11.03.2022	14575,82	9,587119	0,0009521666	6930,016	8,843617	0,0009695874	18979056	16,75885	0,000337270686	1	0
18.03.2022	14589,69	9,58807	0,0009512608	6936,826	8,8446	0,0009821992	18985456	16,75918	0,000337156973	0	1
25.03.2022	14603,56	9,589021	0,0009503568	6943,73	8,845594	0,0009947729	18991856	16,75952	0,000337043337	0	0
01.04.2022	14617,43	9,589977	0,0009494545	6950,728	8,846602	0,0010073082	18998256	16,75986	0,000336929777	0	1
08.04.2022	14631,3	9,590919	0,0009485539	6957,82	8,847621	0,0010198046	19004656	16,76019	0,000336816293	0	0
15.04.2022	14645,18	9,591866	0,0009476550	6965,006	8,848654	0,0010322618	19011056	16,76053	0,000336702886	0	0
22.04.2022	14659,05	9,592813	0,0009467578	6972,286	8,849698	0,0010446794	19017456	16,76087	0,000336589556	0	0
29.04.2022	14672,92	9,593759	0,0009458623	6979,66	8,850755	0,0010570569	19023856	16,7612	0,000336476301	1	0
06.05.2022	14686,79	9,594704	0,0009449685	6987,128	8,851825	0,0010693942	19030256	16,76154	0,000336363123	1	0
13.05.2022	14700,66	9,595648	0,0009440763	6994,69	8,852907	0,0010816906	19036656	16,76188	0,000336250021	1	0
20.05.2022	14714,54	9,596591	0,0009431859	7002,346	8,854001	0,0010939460	19043056	16,76221	0,000336136995	0	1
27.05.2022	14728,41	9,597533	0,0009422971	7010,096	8,855107	0,0011061599	19049456	16,76255	0,000336024045	0	0
03.06.2022	14742,28	9,598475	0,0009414101	7017,94	8,856225	0,0011183320	19055856	16,76289	0,000335911170	0	1
10.06.2022	14756,15	9,599415	0,0009405246	7025,878	8,857355	0,0011304619	19062256	16,76322	0,000335798372	1	0
17.06.2022	14770,02	9,600355	0,0009396409	7033,91	8,858498	0,0011425494	19068656	16,76356	0,000335685649	1	0
24.06.2022	14783,9	9,601294	0,0009387588	7042,036	8,859653	0,0011545939	19075056	16,76389	0,000335573002	1	0
01.07.2022	14797,77	9,602232	0,0009378783	7050,256	8,860819	0,0011665953	19081456	16,76423	0,000335460431	1	0

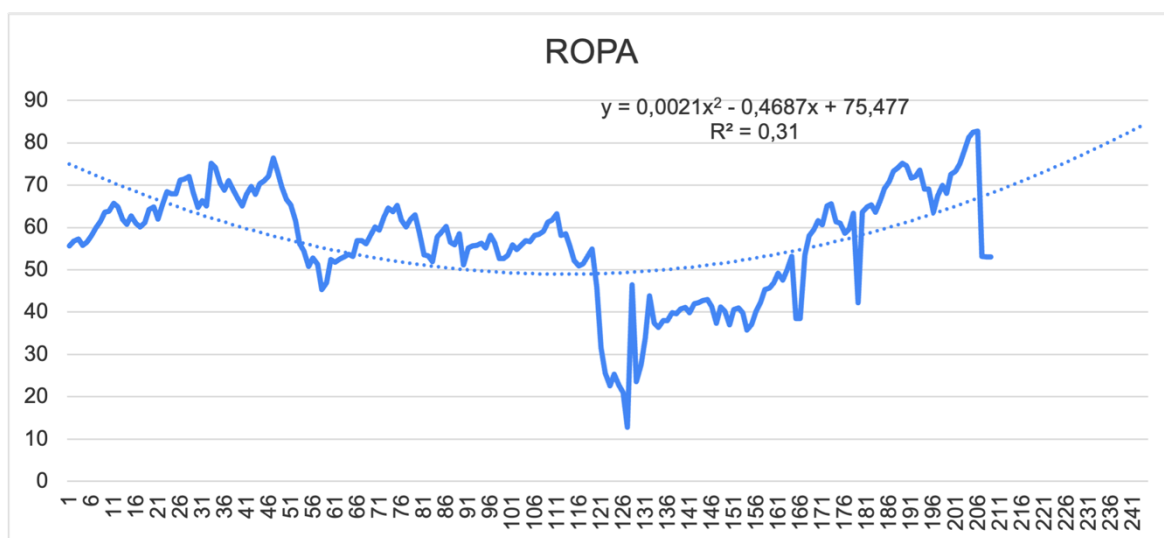
Příloha 9 Graf vývoje a trendu S&P500



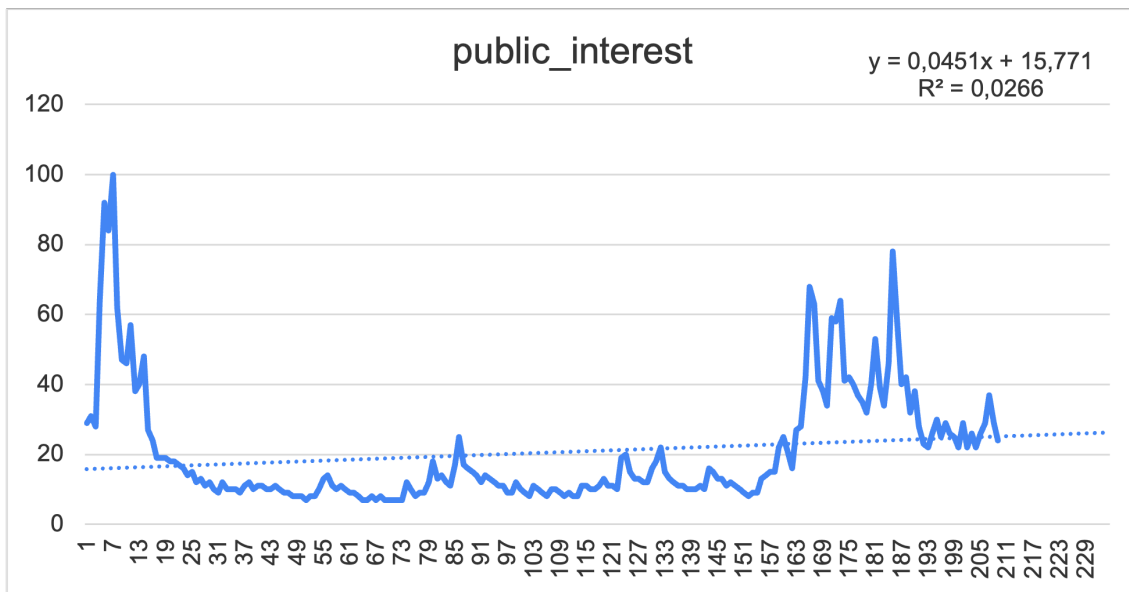
Příloha 10 Graf vývoje a trendu ZLATO



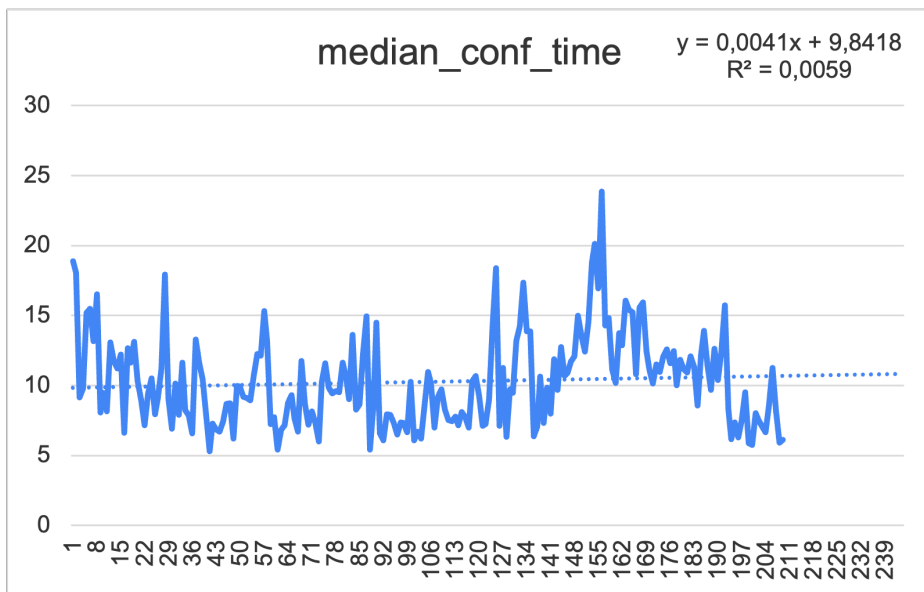
Příloha 11 Graf vývoje a trendu ROPA



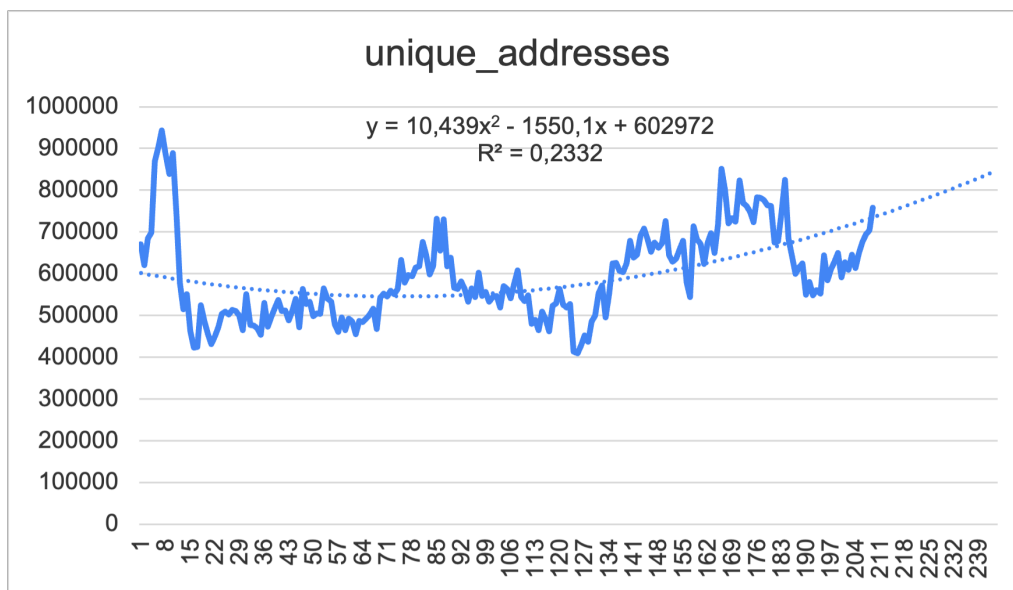
Příloha 12 Graf vývoje a trendu public_interest



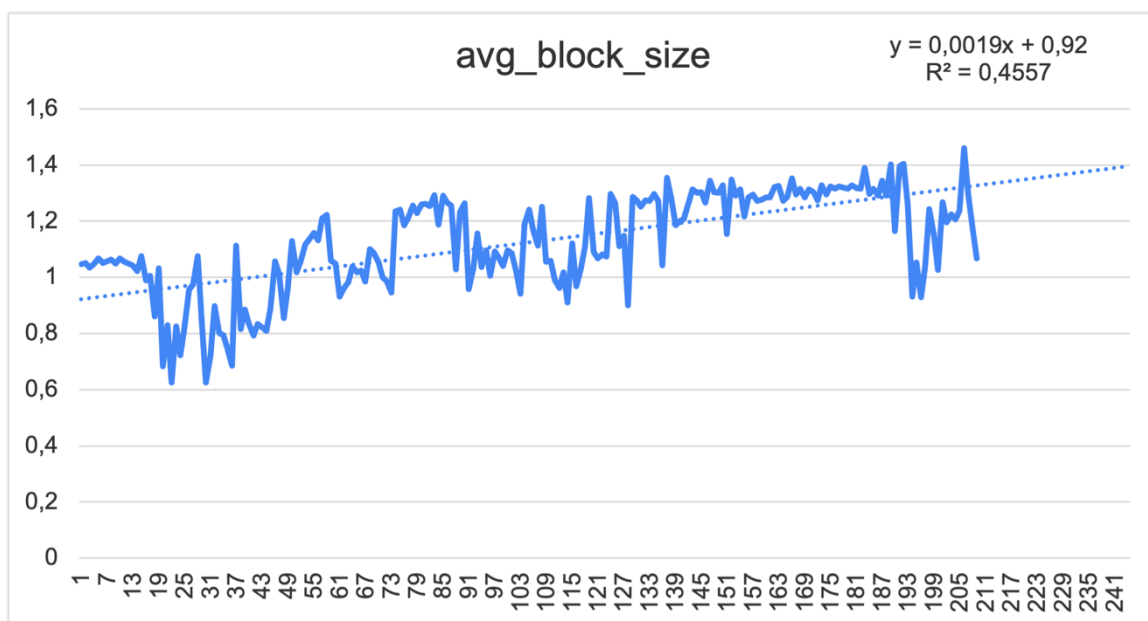
Příloha 13 Graf vývoje a trendu median_conf_time



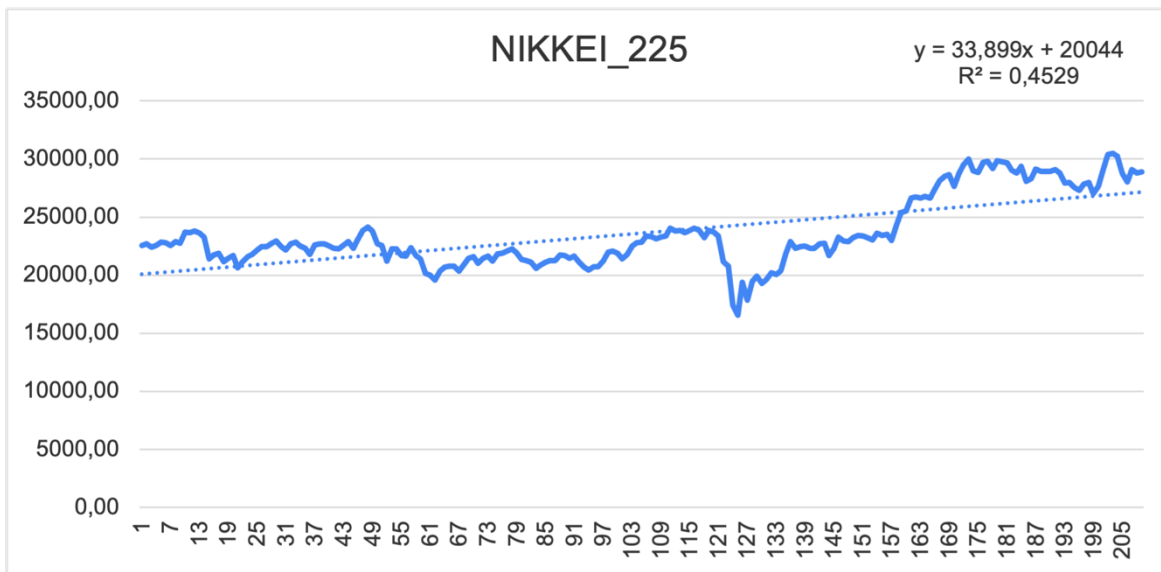
Příloha 14 Graf vývoje a trendu unique_addresses



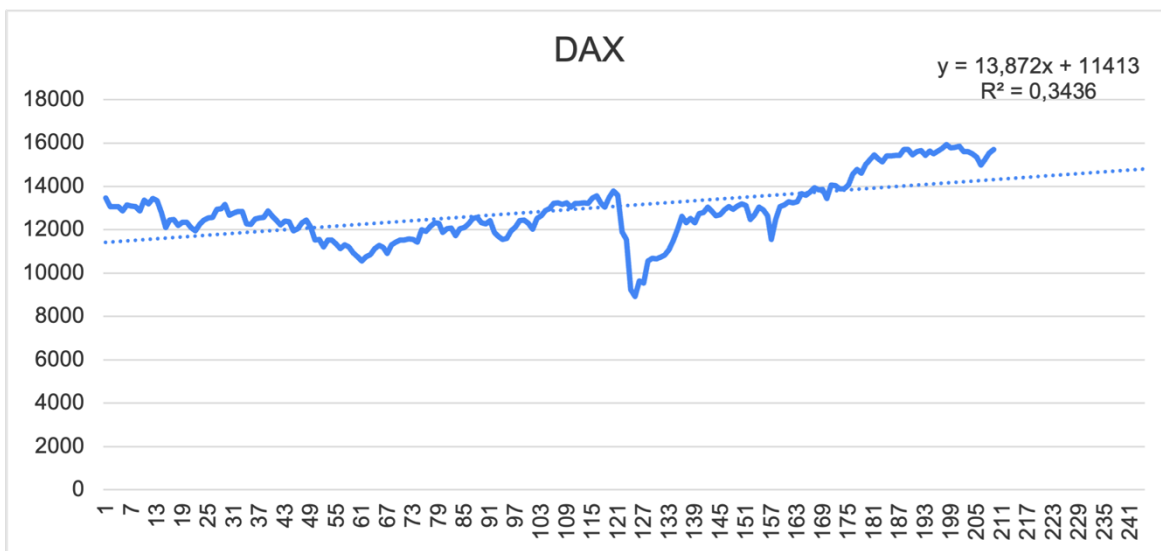
Příloha 15 Graf vývoje a trendu Avg_block_size



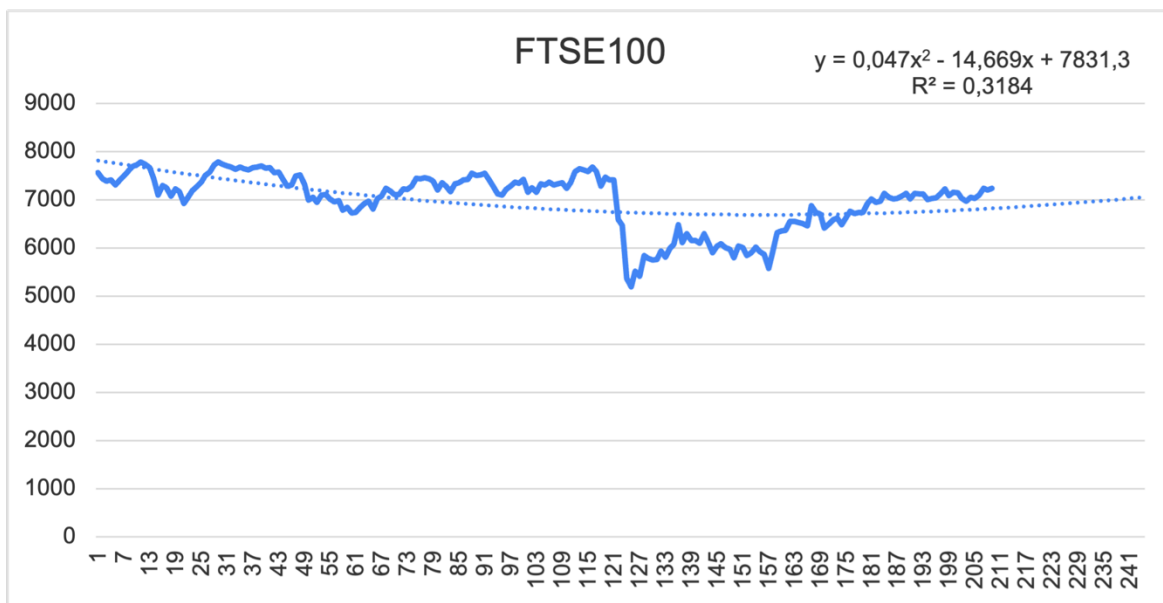
Příloha 16 Graf vývoje a trendu NIKKEI225



Příloha 17 Graf vývoje a trendu DAX



Příloha 18 Graf vývoje a trendu FTSE100



Příloha 19 Nepoužitý model I

Model 177: OLS, za použití pozorování 2017-12-01:2021-10-29 (T = 205)
 Závisle proměnná: ld_BTC

	koeficient	směr. chyba	t-podíl	p-hodnota	
const	-0,00914155	0,0153969	-0,5937	0,5534	
ld_miners_revenue	0,519697	0,0359905	14,44	2,73e-032	***
ld_ETHER_1	-0,0557856	0,0311765	-1,789	0,0752	*
ld_hash_rate	-0,380967	0,0552699	-6,893	8,03e-011	***
Dummy_inc	0,0220975	0,0108305	2,040	0,0427	**
Dummy_dec	-0,0383484	0,0112270	-3,416	0,0008	***
ld_SP500	0,146233	0,245383	0,5959	0,5519	
ld_ZLATO_1	-0,309248	0,162137	-1,907	0,0580	*
ld_ROPA_3	0,0582883	0,0311168	1,873	0,0626	*
ld_public_inte~_2	0,0442717	0,0202770	2,183	0,0302	**
ld_median_conf_t~	0,0274267	0,0192738	1,423	0,1564	
ld_unique_addr~_1	0,104021	0,0540449	1,925	0,0558	*
ld_Avg_block_size	0,112827	0,0454977	2,480	0,0140	**
ld_NIKKEI225	-0,483555	0,237786	-2,034	0,0434	**
ld_DAX	0,661806	0,279133	2,371	0,0188	**
ld_FTSE100	-0,0851352	0,300327	-0,2835	0,7771	
ld_total_btc_1	40,0710	20,7947	1,927	0,0555	*

Střední hodnota závisle proměnné 0,009880
 Sm. odchylka závisle proměnné 0,111374
 Součet čtverců reziduí 0,634773
 Sm. chyba regrese 0,058107
 Koeficient determinace 0,749144
 Adjustovaný koeficient determinace 0,727795
 F(16, 188) 35,08969
 P-hodnota(F) 8,21e-48
 Logaritmus věrohodnosti 301,3112
 Akaikovo kritérium -568,6223
 Schwarzovo kritérium -512,1311
 Hannan-Quinnovo kritérium -545,7730
 rho (koeficient autokorelace) -0,145345
 Durbin-Watsonova statistika 2,266385

zde je poznámka o zkratkách statistik modelu

Pomine-li se konstanta, p-hodnota byla nejvyšší pro proměnnou 142 (ld_FTSE100)

Test normality reziduí -

Nulová hypotéza: chyby jsou normálně rozdělené
 Testovací statistika: Chí-kvadrát(2) = 5,85996
 s p-hodnotou = 0,0533981

Whiteův test heteroskedasticity -

Nulová hypotéza: není zde heteroskedasticita
 Testovací statistika: LM = 185,91
 s p-hodnotou = P(Chí-kvadrát(150) > 185,91) = 0,02468

LM test pro autokorelaci až do řádu 1 -

Nulová hypotéza: žádná autokorelace
 Testovací statistika: LMF = 4,71729
 s p-hodnotou = P(F(1, 187) > 4,71729) = 0,0311196

Příloha 20 Nepoužitý model II

Model 257: OLS, za použití pozorování 2017-12-01:2021-10-29 (T = 205)

Závisle proměnná: l_BTC

HAC standardní chyby, šířka okénka 4 (Bartlettovo jádro)

	koeficient	směr. chyba	t-podíl	p-hodnota	
const	-55,1520	13,9571	-3,952	0,0001	***
l_SP500_3	0,762420	0,186053	4,098	6,21e-05	***
l_miners_revenue	0,684673	0,0545890	12,54	1,40e-026	***
l_ROPA_2	0,198819	0,0479477	4,147	5,11e-05	***
l_fed_funds_ra~_3	-0,0482556	0,0213057	-2,265	0,0247	**
l_Avg_block_size	0,198664	0,0590903	3,362	0,0009	***
l_public_inter~_2	0,0465166	0,0264208	1,761	0,0799	*
l_ETHER	0,0458898	0,0237872	1,929	0,0552	*
ld_hash_rate	-0,231315	0,0345498	-6,695	2,44e-010	***
l_unique_address~	0,378381	0,0816838	4,632	6,76e-06	***
l_n_transactions	-0,375495	0,0692328	-5,424	1,79e-07	***
l_VIX_3	0,173032	0,0329008	5,259	3,93e-07	***
l_total_btc_1	2,47323	0,944655	2,618	0,0096	***
l_ZLATO_4	0,165920	0,135471	1,225	0,2222	
ld_NASDAQ_3	-0,151504	0,0983489	-1,540	0,1251	
ld_DOWJONES_1	0,170814	0,106449	1,605	0,1103	
l_NIKKEI225	0,236541	0,153856	1,537	0,1259	
ld_difficulty	0,202203	0,0876777	2,306	0,0222	**

Střední hodnota závisle proměnné 9,369131
 Sm. odchylka závisle proměnné 0,797892
 Součet čtverců reziduí 0,972116
 Sm. chyba regrese 0,072100
 Koeficient determinace 0,992515
 Adjustovaný koeficient determinace 0,991834
 F(17, 187) 1398,428
 P-hodnota(F) 4,9e-187
 Logaritmus věrohodnosti 257,6249
 Akaikovo kritérium -479,2497
 Schwarzovo kritérium -419,4355
 Hannan-Quinnovo kritérium -455,0563
 rho (koeficient autokorelace) 0,426016
 Durbin-Watsonova statistika 1,127645

zde je poznámka o zkratkách statistik modelu

Pomine-li se konstanta, p-hodnota byla nejvyšší pro proměnnou 134 (l_ZLATO_4)

LM test pro autokorelaci až do řádu 1 -

Nulová hypotéza: žádná autokorelace

Testovací statistika: LMF = 48,0181

s p-hodnotou = $P(F(1, 186) > 48,0181) = 6,70639e-011$

Whiteův test heteroskedasticity -

Nulová hypotéza: není zde heteroskedasticita

Testovací statistika: LM = 192,354

s p-hodnotou = $P(\text{Chí-kvadrát}(170) > 192,354) = 0,115321$

Test normality reziduí -

Nulová hypotéza: chyby jsou normálně rozdělené

Testovací statistika: Chí-kvadrát(2) = 5,02485

s p-hodnotou = 0,0810716

Příloha 21 Nepoužitý model III

Model 254: OLS, za použití pozorování 2017-12-01:2021-10-29 (T = 205)

Závisle proměnná: 1_BTC

HAC standardní chyby, šířka okénka 4 (Bartlettovo jádro)

	koeficient	směr. chyba	t-podíl	p-hodnota	
const	-55,7355	13,7178	-4,063	7,14e-05	***
1_SP500_3	0,730346	0,187697	3,891	0,0001	***
1_miners_revenue	0,686978	0,0558587	12,30	7,99e-026	***
1_ROPA_2	0,210974	0,0507171	4,160	4,86e-05	***
1_fed_funds_ra~_3	-0,0488934	0,0219790	-2,225	0,0273	**
1_Avg_block_size	0,200394	0,0592653	3,381	0,0009	***
1_public_inter~_1	0,0433874	0,0268013	1,619	0,1072	
1_ETHER	0,0532767	0,0272208	1,957	0,0518	*
ld_hash_rate	-0,224858	0,0373136	-6,026	8,82e-09	***
1_unique_address~	0,363552	0,0812909	4,472	1,34e-05	***
1_n_transactions	-0,378365	0,0681857	-5,549	9,78e-08	***
1_VIX_3	0,154169	0,0388022	3,973	0,0001	***
1_total_btc_1	2,57281	0,950992	2,705	0,0075	***
1_ZLATO_4	0,208306	0,147598	1,411	0,1598	
1_DAX_2	-0,125091	0,178901	-0,6992	0,4853	
ld_NASDAQ_3	-0,166774	0,0954327	-1,748	0,0822	*
ld_DOWJONES_1	0,136525	0,116228	1,175	0,2416	
1_NIKKEI225	0,257906	0,152563	1,690	0,0926	*
ld_difficulty	0,179690	0,0881223	2,039	0,0429	**

Střední hodnota závisle proměnné 9,369131
 Sm. odchylka závisle proměnné 0,797892
 Součet čtverců reziduí 0,973050
 Sm. chyba regrese 0,072329
 Koeficient determinace 0,992508
 Adjustovaný koeficient determinace 0,991783
 F(18, 186) 1296,240
 P-hodnota (F) 6,3e-185
 Logaritmus věrohodnosti 257,5264
 Akaikovo kritérium -477,0528
 Schwarzovo kritérium -413,9156
 Hannan-Quinnovo kritérium -451,5153
 rho (koeficient autokorelace) 0,425935
 Durbin-Watsonova statistika 1,134961

zde je poznámka o zkratkách statistik modelu

Pomine-li se konstanta, p-hodnota byla nejvyšší pro proměnnou 74 (1_DAX_2)

Whiteův test heteroskedasticity -

Nulová hypotéza: není zde heteroskedasticita

Testovací statistika: LM = 200,165

s p-hodnotou = $P(\text{Chi-kvadrát}(189) > 200,165) = 0,275096$

Test normality reziduí -

Nulová hypotéza: chyby jsou normálně rozdělené

Testovací statistika: Chi-kvadrát(2) = 5,42715

s p-hodnotou = 0,0662994

LM test pro autokorelaci až do řádu 1 -

Nulová hypotéza: žádná autokorelace

Testovací statistika: LMF = 47,4885

s p-hodnotou = $P(F(1, 185) > 47,4885) = 8,41959e-011$