



## **Diplomová práce**

# **Analýza kryptoměn**

*Studijní program:*

N0688A140016 Systémové inženýrství a informatika

*Autor práce:*

**Bc. Karel Vacek**

*Vedoucí práce:*

Ing. Marián Lamr, Ph.D.

Ústav mechatroniky a technické informatiky

Liberec 2022





## Zadání diplomové práce

# Analýza kryptoměn

*Jméno a příjmení:*

**Bc. Karel Vacek**

*Osobní číslo:*

E20000315

*Studijní program:*

N0688A140016 Systémové inženýrství a informatika

*Zadávající katedra:*

Katedra informatiky

*Akademický rok:*

2021/2022

### Zásady pro vypracování:

1. Filosofie kryptoměn.
2. Kryptoměnové inovace a trendy.
3. Světová adopce kryptoměn.
4. Analýza blockchainových dat a investičních ukazatelů.

*Rozsah grafických prací:*  
*Rozsah pracovní zprávy:* 65 normostran  
*Forma zpracování práce:* tištěná/elektronická  
*Jazyk práce:* Čeština

### **Seznam odborné literatury:**

- ANTONOPOULOS, Andreas M., 2017. *Mastering Bitcoin: programming the open blockchain*. Second edition. Sebastopol, CA: O'Reilly. ISBN 978-1-4919-5438-6.
- ANTONOPOULOS, Andreas M. a Gavin WOOD, 2019. *Mastering Ethereum: building smart contracts and DApps*. First edition. Sebastopol, CA: O'Reilly. ISBN 978-1-4919-7194-9.
- STROUKAL, Dominik a Jan SKALICKÝ, 2021. *Bitcoin a jiné kryptopeníze budoucnosti: historie, ekonomie a technologie kryptoměn, stručná příručka pro úplné začátečníky*. Třetí rozšířené vydání. Praha: Grada Publishing. ISBN 978-80-271-1043-8.
- TĚTEK, Josef, 2021. *Bitcoin: Odluka peněz od státu*. Praha: Braiins Systems. ISBN 978-80-907975-5-0.
- PROQUEST, 2021. *Databáze článků ProQuest* [online]. Ann Arbor, MI, USA: ProQuest. [cit. 2021-10-01]. Dostupné z: <http://knihovna.tul.cz>

Konzultant: Ing. Přemysl Svoboda, odborný asistent FM TUL

*Vedoucí práce:* Ing. Marián Lamr, Ph.D.  
Ústav mechatroniky a technické informatiky

*Datum zadání práce:* 1. listopadu 2021  
*Předpokládaný termín odevzdání:* 31. srpna 2023

L.S.

doc. Ing. Aleš Kocourek, Ph.D.  
děkan

Ing. Petr Weinlich, Ph.D.  
vedoucí katedry

V Liberci dne 1. listopadu 2021

## Prohlášení

Prohlašuji, že svou diplomovou práci jsem vypracoval samostatně jako původní dílo s použitím uvedené literatury a na základě konzultací s vedoucím mé diplomové práce a konzultantem.

Jsem si vědom toho, že na mou diplomovou práci se plně vztahuje zákon č. 121/2000 Sb., o právu autorském, zejména § 60 – školní dílo.

Beru na vědomí, že Technická univerzita v Liberci nezasahuje do mých autorských práv užitím mé diplomové práce pro vnitřní potřebu Technické univerzity v Liberci.

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

Současně čestně prohlašuji, že text elektronické podoby práce vložený do IS/STAG se shoduje s textem tištěné podoby práce.

Beru na vědomí, že má diplomová práce bude zveřejněna Technickou univerzitou v Liberci v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů.

Jsem si vědom následků, které podle zákona o vysokých školách mohou vyplývat z porušení tohoto prohlášení.



## **Poděkování**

Poděkování patří všem autorům odborné literatury, která pomohla autorovi najít cenné informace do jeho diplomové práce. Dále samozřejmě nelze zapomenout na profesory, jenž provázeli autora celým navazujícím studiem, protože všechny získané vědomosti přispěly k vypracování této práce. Na závěr je pak třeba poděkovat vedoucímu práce panu Ing. Bc. Mariánu Lamrovi, Ph.D. za cenné rady, věcné připomínky a vstřícnost při konzultacích.





## **Anotace**

Předmětem diplomové práce na téma analýza kryptoměn je rozbor důležitých faktorů, které mají přímý vliv na trh, s cílem snáze predikovat chování tržních cen kryptoměn. První část práce je teoretická, kde jsou obecně vysvětleny nejdůležitější principy a technologie. Dále jsou zde popsány kryptoměnové koncepce, konkrétní kryptoměny a kryptoměnové inovace. V druhé polovině teoretické části se objevují informace o technické analýze a investorských ukazatelích. Druhá část práce je praktická, která se zaměřuje na statistiku a základní analýzu kryptoměn. Tady je možné nalézt predikční modely časových řad, model Stock to Flow a korelační analýzy.

## **Klíčová slova**

Bitcoin, blockchain, decentralizace, Ethereum, kryptoměny, technická analýza.

## **Annotation**

The subject of the diploma thesis on the topic of cryptocurrency analysis is the research of important factors that have a direct impact on the market, with the aim of more easily predicting the behavior of cryptocurrency market prices. The first part of the work is theoretical, where the most important principles and technologies are generally explained. Besides, cryptocurrency concepts, specific cryptocurrencies and cryptocurrency innovations are described here. In the second half of the theoretical part, information about technical analysis and investor indicators appears. The second part of the work is practical, which focuses on statistics and basic analysis of cryptocurrencies. Here you can find time series prediction models, Stock to Flow model and correlation analyses.

## **Keywords**

Bitcoin, blockchain, decentralization, Ethereum, cryptocurrencies, technical analysis.

# OBSAH

<b>SEZNAM OBRÁZKŮ</b> .....	<b>13</b>
<b>SEZNAM GRAFŮ</b> .....	<b>14</b>
<b>SEZNAM TABULEK</b> .....	<b>15</b>
<b>SEZNAM ZKRATEK</b> .....	<b>16</b>
<b>ÚVOD</b> .....	<b>18</b>
<b>1 FILOSOFIE KRYPTOMĚN</b> .....	<b>20</b>
1.1 BLOCKCHAIN.....	21
1.2 SATOSHI NAKAMOTO.....	22
<b>2 KRYPTOMĚNOVÉ KONCEPCE</b> .....	<b>23</b>
2.1 PROOF-OF-WORK.....	23
2.2 PROOF-OF-STAKE.....	23
<b>3 PŘÍKLADY KRYPTOMĚN</b> .....	<b>25</b>
3.1 BITCOIN.....	25
3.2 ETHEREUM.....	26
<b>4 KRYPTOMĚNOVÉ INOVACE</b> .....	<b>29</b>
4.1 CRYPTO WALLETS.....	29
4.2 LIGHTNING NETWORK.....	31
4.3 SMART CONTRACTS.....	31
4.4 DEFI.....	32
4.5 NFT.....	33
4.6 DEX.....	33
4.7 P2E.....	35
<b>5 SVĚTOVÁ ADOPCE KRYPTOMĚN</b> .....	<b>36</b>
5.1 KORONAVIROVÁ KRIZE.....	36
5.2 STIMULAČNÍ BALÍČKY.....	39
5.3 STÁTNÍ BANKROTY.....	40
5.3.1 Venezuela.....	40
5.3.2 Nigérie.....	41
5.3.3 Libanon.....	41
5.3.4 Srí Lanka.....	41
<b>6 INVESTIČNÍ UKAZATELE TECHNICKÉ ANALÝZY</b> .....	<b>43</b>
6.1 SMA.....	43
6.2 EMA.....	44
6.3 RSI.....	44
6.4 MACD.....	45

6.5	OBV .....	46
6.6	A/D.....	46
6.7	ADX .....	47
<b>7</b>	<b>STATISTICKÉ METODY.....</b>	<b>49</b>
7.1	ČASOVÉ ŘADY .....	49
7.2	REGRESNÍ ANALÝZA .....	52
7.3	KORELAČNÍ ANALÝZA.....	52
<b>8</b>	<b>ANALÝZA BITCOINOVÉHO TRHU.....</b>	<b>53</b>
8.1	PRVNÍ ANALÝZA ČASOVÝCH ŘAD.....	53
8.1.1	Fear & Greed Index.....	53
8.1.2	Vstupní data a model .....	54
8.1.3	Výstupní data a graf .....	56
8.2	DRUHÁ ANALÝZA ČASOVÝCH ŘAD .....	60
8.2.1	SMA(100) a EMA(100).....	60
8.2.2	RSI(14) .....	62
8.2.3	MACD .....	65
8.2.4	Vstupní data a model .....	67
8.2.5	Výstupní data a graf .....	69
8.3	MODEL STOCK TO FLOW .....	72
8.3.1	Vstupní data.....	73
8.3.2	Základní vzorce.....	74
8.3.3	Popis postupu .....	75
8.3.4	Výstupní graf.....	76
8.3.5	Závislost modelu .....	76
8.4	KORELAČNÍ MODELY.....	78
8.4.1	První korelační analýza .....	78
8.4.2	Druhá korelační analýza.....	81
	<b>ZÁVĚR.....</b>	<b>84</b>
	<b>CITOVANÁ LITERATURA.....</b>	<b>87</b>

## **Seznam obrázků**

Obrázek 1 – první model časové řady pro tržní cenu Bitcoinu .....	55
Obrázek 2 – druhý model časové řady pro tržní cenu Bitcoinu .....	68

## Seznam grafů

Graf 1 – vliv koronavirové krize na tržní cenu Bitcoinu.....	37
Graf 2 – vliv koronavirové krize na tržní cenu Bitcoinu v detailu.....	38
Graf 3 – výsledný graf časové řady pro tržní cenu Bitcoinu.....	57
Graf 4 – graf průběhu predikce po dobu 30 dní oproti realitě.....	58
Graf 5 – graf průběhu predikce po dobu 7 dní oproti realitě.....	59
Graf 6 – tržní cena Bitcoinu, SMA(100) a EMA(100) .....	61
Graf 7 – tržní cena Bitcoinu, SMA(100) a EMA(100) v detailu za rok 2021 .....	62
Graf 8 – tržní cena Bitcoinu a RSI .....	64
Graf 9 – tržní cena Bitcoinu a RSI v detailu za rok 2021 .....	65
Graf 10 – MACD index a signální linie .....	66
Graf 11 – MACD index a signální linie v detailu za rok 2021 .....	67
Graf 12 – výsledný graf časové řady pro tržní cenu Bitcoinu.....	69
Graf 13 – graf průběhu predikce po dobu 30 dní oproti realitě.....	70
Graf 14 – graf průběhu predikce po dobu 7 dní oproti realitě.....	71
Graf 15 – výsledný model Stock to Flow pro Bitcoin.....	76

## Seznam tabulek

Tabulka 1 – ukázková vstupní data tržní ceny za 1 bitcoin v americkém dolaru s denním razítkem .....	37
Tabulka 2 – přehled významných stimulačních balíčků .....	39
Tabulka 3 – ukázková vstupní data analýzy časových řad s denními razítky .....	55
Tabulka 4 – výstupní data predikce časové řady pro tržní cenu Bitcoinu .....	56
Tabulka 5 – výstupní analýza modelu časové řady pro tržní cenu Bitcoinu .....	59
Tabulka 6 – ukázka vstupních dat, SMA a EMA pro časovou řadu tržní ceny Bitcoinu....	61
Tabulka 7 – ukázka vstupních dat a RSI pro časovou řadu tržní ceny Bitcoinu .....	63
Tabulka 8 – ukázka vstupních dat a RSI pro časovou řadu tržní ceny Bitcoinu .....	63
Tabulka 9 – ukázka vstupních dat a MACD pro časovou řadu tržní ceny Bitcoinu .....	66
Tabulka 10 – výstupní data predikce časové řady pro tržní cenu Bitcoinu .....	69
Tabulka 11 – výstupní analýza modelu časové řady pro tržní cenu Bitcoinu .....	71
Tabulka 12 – ukázková vstupní data tržní ceny za 1 bitcoin v americkém dolaru s denním razítkem .....	75
Tabulka 13 – ukázková výstupní data mezivýpočtů potřebných parametrů a samotných výsledků v podobě SF a ceny SF .....	76
Tabulka 14 – Pearsonův korelační koeficient pro SF cenu a tržní cenu BTC.....	77
Tabulka 15 – Spearmanův korelační koeficient pro SF cenu a tržní cenu BTC .....	77
Tabulka 16 – Kendallův koeficient konkordance pro SF cenu a tržní cenu BTC .....	77
Tabulka 17 – ukázková vstupní data první korelační analýzy s denními razítky .....	79
Tabulka 18 – Pearsonův korelační koeficient pro BTC, DXY, SPX a GOLD.....	79
Tabulka 19 – Spearmanův korelační koeficient pro BTC, DXY, SPX a GOLD .....	80
Tabulka 20 – Kendallův koeficient konkordance pro BTC, DXY, SPX a GOLD.....	80
Tabulka 21 – ukázková vstupní data druhé korelační analýzy s měsíčními razítky.....	81
Tabulka 22 – Pearsonův korelační koeficient pro tržní cenu BTC, BTC hashrate, BTC Google Trends a USD Net Capital Flow .....	82
Tabulka 23 – Spearmanův korelační koeficient pro tržní cenu BTC, BTC hashrate, BTC Google Trends a USD Net Capital Flow .....	82
Tabulka 24 – Kendallův koeficient konkordance pro tržní cenu BTC, BTC hashrate, BTC Google Trends a USD Net Capital Flow .....	82

## Seznam zkratek

A/D	Accumulation/Distribution
ADL	Autoregressive Distribution Lags
ADX	Average Directional Index
AML	Anti-Money Laundering
API	Application Programming Interface
ARPA	American Rescue Plan Act
ATR	Average True Range
BIC	Bayesian Information Criterion
BIP	Bitcoin Improvement Proposal
BTC	Bitcoin
CARES	Coronavirus Aid, Relief and Economic Security Act
CCF	Cross Correlation Function
CEX	Centralized Exchange
CSV	Comma-Separated Values
CZK	Czech Koruna
DAO	Decentralized Autonomous Organization
DApps	Decentralized Applications
DeFi	Decentralized Finance
DEX	Decentralized Exchanges
DJI	Dow Jones Industrial Average
DLT	Distributed Ledger Technology
DXY	US Dollar Index
ECB	European Central Bank
EIP	Ethereum Improvement Proposal
EMA	Exponential Moving Average
ERC-20	Ethereum Request for Comment
ETH	Ethereum
EU	European Union
EUR	Euro
GUI	Graphic User Interface
KPSS	Kwiatkowski-Phillips-Schmidt-Shin
KYC	Know Your Customer



MA	Moving Average
MACD	Moving Average Convergence Divergence
MAE	Mean Absolute Error
MAPE	Mean Absolute Percentage Error
MaxAE	Maximum Absolute Error
MSE	Mean Squared Error
NTF	Non-Fungible Token
OBV	On-Balance Volume
P2E	Play to Earn
PoS	Proof of Stake
PoW	Proof of Work
RMSE	Root Mean Squared Error
RSI	Relative Strength Index
SAT	Satoshi
SF/S2F	Stock to Flow
SMA	Simple Moving Average
SPX	S&P 500 Index
SQL	Structured Query Language
TF	Transfer Functions
UNI	Uniswap
USD	United States Dollar
USDT	Tether

# Úvod

Několik velkých hospodářských krizí ukázalo světu, jak křehká je ekonomika vyspělých států, natož rozvojových zemí. Stačí se podívat třeba na Venezuelu, Libanon a Srí Lanku, jak snadno může dojít k bankrotu. Zvyšuje se tlak na automatické a digitální systémy, které jsou například ve finančnictví, bankovníctví a obecně monetární politice zaostalé. Svět nestíhá přijímat nové technologie v dostatečném tempu a tápe nad ekonomickými problémy. Vysoká inflace a neúměrně rostoucí státní dluh děsí nejednoho občana, jenž už neví, v čem má spořit a kam dát svoje těžce vydělané peníze.

Objevují se zajímavé technologie, jež přispívají k rozvoji peněz samotných a definují úplně nové způsoby, jak může probíhat platební styk. Uchopení vynálezu jménem blockchain spolu s kryptografickými metodami je přelomový nápad, který má potenciál změnit svět. Ovšem je tu stále mnoho překážek, na které mohou tyto věci bohužel narážet. Kryptoměny již dávno patří do každodenního života jakéhokoliv občana, jenž má zájem se o danou problematiku dostatečně zajímat. Existuje celá řada projektů a služeb, které tyto inovace aktivně používají. Záleží především na tom, jak se bude vyvíjet situace s regulacemi a s adopcí kryptoměn u běžných zákazníků a zprostředkovatelů. Na nich totiž stojí síla protlačit virtuální mince do místní večerky nebo na nejbližší benzínovou pumpu. Je nutné zmínit, že velké množství moderních internetových obchodů kryptoměny podporuje a je možné s nimi zaplatit nákup. Jedním příkladem za všechny je Alza, která je vůbec prvním velkým propagátorem kryptoměn ve svém e-shopu v Čechách a na Slovensku.

Tato diplomová práce pod názvem „Analýza kryptoměn“ obecně popisuje technologie, principy a podstatu kryptoměn ve světě. Práce má teoretickou a praktickou část. Teoretická část se zabývá základními pojmy, filosofií kryptoměn, kryptoměnami Bitcoin a Ethereum, kryptoměnovými koncepty a inovacemi, a investorskými praktikami včetně nejznámějších technických ukazatelů.

Praktická část obsahuje základní analýzu kryptoměn, která se opírá o časové řady, model Stock to Flow a korelační analýzy trhů. V oboru data miningu a zpracování dat jsou záznamy o tržní ceně aktiva brány jako časová řada. Právě tento model je aplikován na cenový vývoj Bitcoinu, díky čemuž lze částečně predikovat další chování trhu. Autor pak sestavil model Stock to Flow pro Bitcoin, který má v ekonomickém prostředí svoje místo. Na základě bitcoinové rezervy a ročního pří toku nových mincí lze odhadnout chování tržní ceny aktiva

v dlouhodobém horizontu. Dále se snažil dokázat, případně vyvrátit, že jsou kryptoměnové trhy závislé na dalších trzích a aktivech skrze klasické korelační analýzy.

Práce částečně zasahuje do oblasti investiční činnosti, protože je to poměrně aktuální téma napříč všemi generacemi. Kdokoliv má dnes přístup k centralizovaným burzám a různým investičním službám, kde je možné nakupovat takřka cokoliv – jako třeba akcie, indexy, podíly ve fondech, kryptoměny nebo komodity. Proto je dobré rozumět technické analýze a investičním ukazatelům, které se v praxi používají na denní bázi. Jednoduchá aplikace a pár příkladů ukazují jejich význam při investování a dělání těžkých rozhodnutí.

# 1 Filosofie kryptoměn

V dnešním světě jsou peníze vázány na danou monetární politiku země, jež měnu spravuje, a to je očividný problém. V kryptoměnové komunitě často rezonuje pojem svobodné peníze, protože jsou celosvětově dostupné a hranice států pro ně nejsou překážkou. Tím, že jsou zpravidla decentralizované, je jejich osud v rukách uživatelů.

Lepší technologie umožňují lepší kontrolu nad společností, ale právě kryptoměny se snaží prosazovat anonymitu, která se však z tohoto odvětví pomalu vytlačuje. Velká část z nich je totiž vystavena regulacím. Povinnost KYC (Know Your Customer) vznikla za účelem snazšího sledování uživatelů a dále jako ochrana AML (Anti-Money Laundering), což se daří jen částečně. Jedním z důvodů může být to, že stále existují neregulované služby.

Transparentnost obsahu, což jsou ve světě kryptoměn blockchainová data, kód systému a filosofie za projektem, má poskytnout vyšší míru bezpečnosti a komunitní podpory. To však může působit dvojsečně. Stále se objevuje velké množství podvodů a falešných projektů s jednoduchým cílem – vytáhnout z uživatelů peníze skrze jejich kryptoměny. Tyto aféry vrhají na kryptoměny negativní pohled. Avšak velký vliv na tuto problematiku má nízká edukovanost uživatelů, kteří si do tohoto investičního sektoru přišli vydělat peníze.

Během vývoje kryptoměn vznikl technologický paradox, kterému se říká kryptoměnový trojúhelník. Jedná se totiž o tři parametry – bezpečnost, kapacita (škálovatelnost) a rychlost. Tyto atributy sítě nelze samostatně maximalizovat, protože vylepšení jednoho atributu je na úkor druhého atributu apod. Každá síť tak bojuje s vybalancováním těchto parametrů. Nově vzniklé projekty se snaží problém elegantně vyřešit. Většinou se odvolávají na přelomovou technologii, což bývá jen prostředek marketingu. Existují však důmyslná řešení, která se již v praxi objevila. Ovšem většina dominantních kryptoměn z důvodu složitosti přechodu na nový model stále trpí těmito komplikacemi.

Kryptoměny jsou dostupné na specializovaných burzách, protože se jedná o virtuální peníze a akcie, které o fous utíkají regulátorům. Ovšem není nutné tyto služby používat, protože každý uživatel je schopný posílat svoje kryptoměny ze své adresy na jinou bez prostředníka. Burzy jsou dobrý vstupní bod, jak se ke kryptoměnám dostat. Poté už je vhodné používat decentralizované služby a vyhýbat se centrálním bodům kvůli zachování alespoň částečné anonymity (Stroukal a Skalický 2021).

## 1.1 Blockchain

Blockchain je chytře zabezpečený systém, který zaznamenává informace tak, že je velmi obtížné jej obelhat či napadnout. Jedná se o nejzákladnější, a zároveň nejdůležitější složku sítě, ve které technologie operuje. Každý blok je součástí zabezpečeného řetězce bloků, jenž nese informace za dané časové období. Provedená transakce je přidána na konec bloku, který je pak kryptograficky podepsán pomocí takzvaného hashe.

Technologie blockchain spadá do kategorie DLT (Distributed Ledger Technology), což teoreticky znamená, že je považován za decentralizovanou databázi, jež je řízena několika nezávislými uživateli sítě. Aby něco mohlo být označeno za DLT, musí splňovat sedm předpokladů: programovatelnost, bezpečnost, anonymitu, jednomyslnost, časové rámce, neměnnost dat a kompletní distribuci. Programovatelnost umožňuje vytvářet aplikace, které jsou nějakým způsobem navázány na funkcionality sítě. Bezpečnost je téměř vždycky řešena kryptografickými šiframi. Anonymita zaručuje maximální bezpečnost pro uživatele sítě. Jednomyslnost znamená, že datový obsah sítě, tedy záznamy na blockchainu, musí být totožný s každou instancí blockchainu jiného uživatele či zařízení. Časové rámce zaručují, že každý blok v blockchainu zapisoval data po stejnou dobu jako jeho předchůdci. Neměnnost dat je nutná pro integritu celé sítě, protože pak je zaručena její jednoznačnost a neporušitelnost. Kompletní distribuce má zajistit, že celý blockchain je dostupný pro všechny uživatele sítě (Euromoney.com 2022).

Blockchain se ukázal jako skvělý prostředek pro vytváření kryptoměn, protože splňuje mnoho ideálů, které reálné peníze (FIAT) nemají, jako například americký dolar (USD), euro (EUR) či česká koruna (CZK). Všechny ideály světových peněz jsou obsaženy v principech DLT. Primárním problémem předchozích pokusů o vytvoření lepších měn byla nedůvěra, protože vždycky byly nové peníze řízeny autoritou, která nad nimi měla velkou moc. Proto vznikla tato nová technologie, jež odstartovala rozmach kryptoměn, jako například Bitcoinu a Etherea. Tyto peníze, mince či tokeny mají jasně stanovená pravidla uvnitř sítě – nelze je zfalšovat, hacknout či kompromitovat. Nikdo je neřídí, spravují je totiž uživatelé společně. Objevuje se však úplně jiný problém s blockchainy – je jich až příliš mnoho a takové množství nemá ve světě smysl. Některé nové projekty se tak snaží používat blockchain na úplně jiné věci, jež vůbec nemusí souviset s penězi. Zpravidla se jedná o funkce, jež jsou totožné s významem běžných SQL databází. Pak zde vzniká otázka, zdali je vůbec potřeba na tyto věci využívat blockchain, když doposud klasické databáze

fungovaly dobře. Nic však neodpáře blockchainu jeho přínos v dnešním světě plného podvodů, krizí a nejistot. Vazba na finanční sféru je jasná, další odvětví se možná objeví časem.

Technologie blockchain se prozatím využívá v těchto oborech: ochrana autorských práv, decentralizované peníze, zápisy v katastru nemovitostí nebo akademické certifikáty. To znamená, že všude, kde je vyžadována decentralizovaná a sdílená kontrola nad systémem či nezkorumpovatelnost a nezměnitelnost záznamů, je vhodné aplikovat toto řešení (Hayes 2022a).

## 1.2 Satoshi Nakamoto

Byl to, nebo je to kryptograf, programátor a matematik. Znáám též jako vynálezce Bitcoinu. Neví se zcela jistě, zdali se jedná o reálné jméno či pseudonym, ani jeli to jedna osoba či rovnou celá skupina lidí. Jeho totožnost není známa, zachoval si anonymitu, která je pro většinu fanoušků Bitcoinu natolik důležitá. Vytvořil dokument, kterému se odborně říká whitepaper, kde definoval svůj vynález jménem Bitcoin. Je také autorem prvního funkčního blockchainu, který slouží dodnes pro účely Bitcoinu.

Jeho názory spatřily světlo světa v roce 2008, kdy přišla silná ekonomická krize, což byl ideální čas na takové přelomové myšlenky jako vytvořit decentralizovanou virtuální měnu. Pod přezdívkou Satoshi Nakamoto publikoval své nápady a inovativní myšlenky na odborných fórech. Sám vymyslel celý koncept virtuálních peněz na principu blockchainu a modelu proof-of-work. Dostalo se mu úspěchu, když hned několik programátorů a IT nadšenců začalo pracovat na jeho přelomové vizi. On se na vývoji také vehementně podílel a usměrňoval svoje kolegy.

Příběh Satoshiho Nakamota skončil v roce 2010, kdy jeho dílo Bitcoin bylo již plně funkční a žilo si svým životem. Svému kolegovi pak vzkázal emailem, že se na projektu už nebude nadále podílet, a že se věnuje něčemu jinému. Odchodem stvrdil svou anonymitu, a tak bitcoinová persona zůstala utajena dodnes. Nechtěl být s projektem spojován? Nechtěl ohrozit decentralizované pojetí sítě? Nechtěl se stát terčem vydírání nebo jiného fyzického nebezpečí? To se už pravděpodobně nikdo nikdy nedozví (Hayes 2022c).

## 2 Kryptoměnové koncepce

Kryptoměnovým konceptem či modelem je myšleno to, jakým způsobem bude síť ověřovat nové transakce a zapisovat výsledky. Aby kryptoměna mohla fungovat, je zapotřebí někoho, kdo prokáže, že se v daném systému nepodvádí a je zachována jakási integrita. To zpravidla dělají takzvaní těžaři a nodeři, kteří se starají o chod sítě. Podle jasně stanovených pravidel napsaných v kódu dané kryptoměny zpracovávají požadavky uživatelů a svými prostředky zabezpečují celý systém.

V praxi jsou dva relevantní způsoby, kterými se tyto mechanismy uskutečňují: proof-of-work a proof-of-stake. Oba se od sebe výrazným způsobem liší a mají svoje výhody i nevýhody. Dalšími koncepty mohou být proof-of-burn, proof-of-reputation, proof-of-replication, proof-of-spacetime nebo proof-of-history. Jejich výskyt však není tak častý (Frankenfield 2021).

### 2.1 Proof-of-work

Proof-of-work je koncept, ve kterém uživatel daného systému dokazuje hodnotu platebního prostředku skrze vynaloženou práci. Nejznámějšími projekty, jenž používají tento koncept, jsou třeba Bitcoin, Ethereum (pouze do roku 2021) a další kryptoměny postavené na těchto principech. Zpravidla se v nich vyskytuje osoba jménem těžař, která výkonem svého zařízení vykonává práci na uzavírání bloků v blockchainu. Díky výpočetnímu výkonu všech zařízení pracujících v otevřeném systému vzniká bezpečnost celé sítě. Tento koncept má jednu velkou slabinu, nejčastěji se označuje jako 51% útok. To znamená, že jeden uživatel nebo celá skupina má v systému většinu, čímž může ostatní přesvědčit o svých „pravdách“. Mohli by například pozměnit obsah napadeného bloku v blockchainu. Avšak na podobné podvody se rychle přijde, protože zfalšované transakce neodpovídají historickým datům a zůstatkům na adresách (Frankenfield 2022b).

### 2.2 Proof-of-stake

Proof-of-stake je koncept, ve kterém skupina validátorů uzamkne dopředu stanovené množství vybrané kryptoměny, čímž získají možnost ověřovat transakce příslušné sítě. Odměnou jim jsou transakční poplatky, které zpravidla platí zadavatel platby. Validátor, jenž uzamkne aktuální blok, je vybrán pseudonáhodně. Čím větší je totiž obnos uzamčených tokenů, tím je také větší šance na to, že validátor bude vybrán k uzamknutí onoho bloku. V případě, že se validátor pokusí zneužít pozici tím, že validuje špatné transakce například

z důvodu sebeobohacování, tak přijde o svůj počáteční depozit. Validátor se tak počátečním depozitem zavazuje, že bude přispívat k zabezpečení sítě, jinak o svoje peníze přijde za porušení pravidel. Tím se předchází podvodům a hrozba ztráty peněžních prostředků motivuje validátory dělat svou práci poctivě a bez postranních úmyslů. Typickými příklady tohoto způsobu ověřování bloků jsou kryptoměny Cardano a Polkadot (Frankenfield 2022c).



## 3 Příklady kryptoměn

### 3.1 Bitcoin

Bitcoin („digitální zlato“) je počítačová technologie, protokol a virtuální měna. Jedná se o první úspěšnou kryptoměnu, která se svou funkcionalitou snaží vyrovnat státním penězům, nebo je rovnou nahradit. Navíc splňuje mnoho ideálů, jak by peníze ve světě měly fungovat. Vznikl jako reakce na nestabilní monetární politiky ve světě, tedy rostoucí inflace a opakující se krize. Jeho autorem je údajný Satoshi Nakamoto, který vymyslel celý koncept Bitcoinu a popsal jej ve svém whitepaperu. Využívá technologie blockchain a konceptu proof-of-work. Měl by sloužit jako nestátní decentralizované peníze a udržitel hodnoty, tedy jako ochránce vůči rychle rostoucí inflaci. Platidlem uvnitř systému je bitcoin s malým písmenem b. Velké písmeno B se uvádí v případě, že se jedná o systém, nikoliv o jednotku v systému. Často se používá menší jednotka bitcoinu jménem satoshi, zkráceně SAT. Bitcoin je totiž dělitelný na osm desetinných míst a značí se dvakrát přeškrtnutým písmenem B (฿) v podobném stylu jako americký dolar s písmenem S (\$).

Používané nominální hodnoty bitcoinu:

- 1 SAT = 0,00000001 BTC
- 100 SAT = 0,000001 BTC (you-bit)
- 100 000 SAT = 0,001 BTC (em-bit)
- 1 000 000 SAT = 0,01 BTC (bitcent)

V roce 2012 byla založena významná nadace jménem Bitcoin Foundation, jež se spolu s komunitou stará o chod Bitcoinu a jeho případné vylepšování skrze proces BIP (Bitcoin Improvement Proposal). Díky však decentralizovanému řešení se na změnách v protokolu musí shodnout většina, což v praxi znamená, že se o všech rozhodnutích demokraticky hlasuje napříč zainteresovanými stranami. Zpravidla hlasují zástupci všech skupin – programátoři, těžaři a uživatelé.

Nové bitcoiny se do sítě emitují každých 10 minut, což je moment, kdy se uzavře 1 blok v blockchainu. Každé 4 roky se odměna za vytěžený blok půlí, až nakonec dojde k minimu a na hodnotě 21 milionů se kapacita měny úplně vyčerpá. Těžba se stará nejen o získávání nových bitcoinů, ale také o celkové zabezpečení sítě, protože všechny zařízení připojené

v síti poskytují výpočetní výkon, jenž vytváří složitost algoritmu, co spravuje šifrování bloků. Tím se pro jednotlivce stává takřka nemožné prolomit šifru bloku dříve než některému jinému počítači (Tětek 2021).

V síti jsou takzvané uzly, které mohou být reprezentovány dvěma způsoby. První jsou zařízení, jež jsou určena k těžbě, tedy k uzavírání bloků, emitaci nových bitcoinů a samotnému zabezpečení sítě. Druhá možnost jsou zařízení, která spravují blockchain Bitcoinu a distribuují údaje o blocích, tím jsou myšleny třeba proběhlé transakce či obnosy bitcoinů na adresách.

Okolo Bitcoinu vzniká celý ekosystém, ve kterém jsou těžařská uskupení, odborné firmy, obchody, vývojáři aplikací (peněženek, platebních bran, protokolů, her apod.), investoři a samozřejmě běžní uživatelé (Antonopoulos 2017).

## 3.2 Ethereum

Ethereum je open-source platforma, síť a virtuální měna. Jedná se o moderní pojetí kryptoměny, u kterého se očekává široká funkcionalita. Umožňuje uživatelům a vývojářům vytvářet na platformě další služby. Otevírá cestu k decentralizovaným aplikacím, označují se jako DApps. Mohou to být například oracle protokoly, DeFi (decentralizované finance), NTF (nezaměnitelné tokeny), hry, směnárný nebo finanční služby (půjčování, pojišťování, investování, crowdfunding). Platidlem uvnitř systému je takzvaný ether. Značí se velkým řeckým písmenem Xi ( $\Xi$ ).

Nominální hodnoty etheru:

- 1 Ether = 1000000000000000000 Wei
- 1 Ether = 1000000000000000 Kwei
- 1 Ether = 1000000000000 Mwei
- 1 Ether = 1000000000 Gwei
- 1 Ether = 1000000 Szabo
- 1 Ether = 1000 Finney
- 1 Ether = 0,001 Kether
- 1 Ether = 0,000001 Mether

- 1 Ether = 0,000000001 Gether
- 1 Ether = 0,000000000001 Tether

Autorem celého konceptu je ruský programátor Vitalik Buterin, jenž první nápad představil v roce 2013. Na projektu se také podílel anglický počítačový vědec Gavin Wood, se kterým sepsal dokument jménem Yellow Paper, tedy základní definici jejich platformy. Hlavním cílem bylo předčít potenciál Bitcoinu, který dodnes zastává spíše konzervativní zastoupení v kryptoměnách. Oba totiž chtěli, aby bylo možné nahradit centralizovaná řešení aplikací za ty decentralizovaná.

Gavin Wood pracoval jako počítačový vědec ve firmě Microsoft, kde získal hodně zkušeností. Díky tomu získal nový pohled na vývoj aplikací, což ho přivedlo k počátkům vzniku platformy Ethereum. Nakonec kvůli ideologickým neshodám s Vitalikem Buterinem se rozhodl založit vlastní projekt, který na celou problematiku pohlíží z trochu jiného úhlu. Tím projektem je úspěšný konkurent Etherea jménem PolkaDot.

Ethereum zažilo několik krušných chvil. Významným historickým okamžikem byl vznik systému DAO (Decentralized Autonomous Organisation) na platformě Etherea. Tomu se dostalo masivní podpory ze strany komunity a získal velký podíl v Ethereu, pokrýval 14 % doposud vydaných etherů. Avšak chyba v systému DAO, která nesouvisela s platformou Ethereum, umožnila hackerům dne 18. června 2016 ukrást třetinu celého fondu DAO, což v té době bylo zhruba 50 milionů amerických dolarů. Důvěra v Ethereum dostala silný zásah. Následoval takzvaný hard fork dne 23. června 2016, tedy nenávratné rozdělení sítě vlivem rozbourání základů platformy. Většina uživatelů souhlasila s násilným rozdělením sítě a následovala „nové Ethereum“. „Staré Ethereum“ se přejmenovalo na Ethereum Classic a zůstala u něj jen minorita komunity jakožto dle slov zarytých fanoušků jediné pravé Ethereum. Ethereum dalo možnost obětem hacku dostat svoje peníze zpět skrze zavedení takzvaných Smart Contracts (přeloženo jako chytré smlouvy nebo jako chytré kontrakty). Další kontroverze tak o to víc usměrnily osud Etherea. Následovaly ještě další hard forky, které definovaly podobu dnešní platformy. Za zmínku stojí hard fork jménem Byzantium dne 16. října 2017, kde bylo cílem udělat Ethereum jednodušší, rychlejší a bezpečnější. Nebo také hard fork jménem Constantinopol dne 27. února 2019, který snížil odměnu za vytěžený blok a částečně optimalizoval síť.

Stejně jako Bitcoin se Ethereum těží na příslušných zařízeních pomocí konceptu proof-of-work, čímž se zabezpečuje síť výpočetním výkonem a emitují se nové ethery každých

12 sekund jako odměna za vytěžený blok. Dle zatížení sítě je měna buď inflační, nebo deflační na základě výše odměny versus výše spálených poplatků. Na rozdíl však od Bitcoinu se k těžbě může použít jakékoliv zařízení, nemusí to být speciální těžební rig, ale klidně i klasický počítač.

V nové verzi Ethereum 2.0, která se průběžně buduje, bude koncept změněn na proof-of-stake, čímž se Ethereum stane ekologicky přijatelné. K tomuto kroku již došlo v roce 2022. Všechny změny a vývoj Etherea dnes spravuje takzvaná Ethereum Foundation skrze proces zvaný EIP (Ethereum Improvement Proposal) (Antonopoulos a Wood 2018).

## 4 Kryptoměnové inovace

Nápad vytvořit peníze založené na digitálních a kryptografických principech je přelomový už jenom sám o sobě. Zároveň se k tomuto výtvoru přidává celá řada nových technologií a vychytávek, které zpříjemňují používání těchto kryptoměn, a díky čemuž vznikají nové příležitosti. Na počátku běžely kryptoměnové systémy jen a pouze v příkazových řádcích. Kdokoliv chtěl svoje kryptoměny někam poslat nebo jen nastavit něco v síti, musel znát opravdu velké množství příkazů, s čímž byly spojené jisté uživatelské problémy. Proto postupně vznikaly různá GUI a speciální aplikace, jež zpřístupnily kryptoměny celému světu. Nemluvě o dalších inovativních službách a podsystémech, které prohloubily tuto tematiku (Stroukal a Skalický 2021).

### 4.1 Crypto Wallets

Crypto Wallet (přeloženo jako kryptoměnová peněženka) je softwarová aplikace nebo hardwarové zařízení, které uchovává tajné informace jako soukromý klíč a seed phrase (přeloženo jako přístupová fráze). Těmi uživatel přistupuje ke svým kryptoměnám. Dále slouží k ověřování transakcí a k jejich podepisování, tedy prokázání, že odesílatel transakce je opravdu majitelem prostředků dané adresy. Kryptoměny lze posílat z peněženky s danou adresou na další adresy za transakční poplatek v rámci sítě, ve které kryptoměna operuje.

Existuje celá řada implementací této inovace. Z hardwarového hlediska se vždy jedná o malá elektronická zařízení s displejem a jednoduchými ovládacími prvky. Mezi dva největší a nejznámější výrobce patří Ledger a česká firma Trezor. Softwarová řešení jsou tradiční desktopové aplikace, mobilní aplikace a rozšíření internetových prohlížečů pro okamžité použití. Nejzákladnější kryptoměnová peněženka je například Exodus. Jedná se pouze o aplikaci s možností propojit svůj pomyslný účet se zařízením od firmy Trezor. Má verze pro Android, iOS a Windows. Pyšní se přívětivým a jednoduchým uživatelským rozhraním a poměrně slušnou podporou kryptoměn. Profesionálnější peněženky jsou potom například MetaMask, Trust Wallet nebo Coinbase Wallet.

Kryptoměnové peněženky nabízí i další finanční subjekty jako burzy a platební systémy. V případě burz je tato potřeba jasná, protože zákazník musí mít přidělené místo, kam svoje kryptoměny může dočasně ukládat a později třeba obchodovat. Platební systémy kromě úschovy standardních měn, jako například USD, EUR a CZK, ke svým službám často přidávají právě kryptoměny a potřeba integrovaných peněženek je zde zcela opodstatněná.

Jedná se o firmy jako PayPal nebo Revolut, kteří svým zákazníkům nabízí nejrůznější kryptoměny (InvestPlus.cz 2022).

Při výběru ideální a bezpečné peněženky na kryptoměny může být zásadní rozdíl mezi open-source a closed-source verzemi. Open-source umožňuje nahlížet do kódu aplikace zvenčí, a dohledat tak případné problémy a slabá místa. Často se na tom podílí samotná komunita a uživatelé služby. U closed-source softwaru se spoléhá na kompetentnost dané autority, jež peněženku spravuje. Dále je pak podstatné dělení peněženek na custodial a non-custodial. Custodial řešení jsou zpravidla využívána u centralizovaných burz, což sebou přináší jisté riziko, protože za ochranu uživatelových prostředků zodpovídá služba. Naopak typ non-custodial nabízí větší bezpečnost, poněvadž uživatel přebírá plnou zodpovědnost za svůj privátní klíč a seed phrase. Ovšem to může být dvojsečné rozhodnutí, protože pokud nemá dotyčný člověk dostatečné zkušenosti na poli počítačové bezpečnosti, tak to logicky může způsobit více problémů než užitku. V takových případech se doporučuje využít asistence někoho důvěryhodného a pokročilejšího pro používání non-custodial peněženek.

Bohužel se dá jednoduše narazit na nejrůznější podvody, a může být tak poměrně náročné udržet svou peněženku v bezpečí. Je potřeba pamatovat na to, že jakmile uživateli unikne jeho privátní klíč či seed phrase, tak je zcela zaručené, že o svoje prostředky dříve nebo později přijde. Na blockchainu neexistuje technická možnost prostředky vrátit, vynutit jejich opětovné navrácení, ani se obrátit na podporu sítě, protože ta funguje zcela decentralizovaně a každý uživatel je zodpovědný za svoje prostředky. Jakmile zmizí z jeho peněženky, není cesty zpět a nikdo mu je už nevrátí.

Mezi nejčastější způsoby získání uživatelského privátního klíče či seed phrase patří běžné hackerské metody, jako například phishing nebo malware. U phishingu se může jednat o podvodné emaily a aplikace, jež se vydávají za oficiální produkty sítě či webové stránky se soutěžemi a kontroverzními nabídkami, a mnoho dalších. U malwaru to jsou zpravidla cracklé programy, které již dnes automaticky cílí na softwarové peněženky na uživatelských počítačích, což jsou typicky klasické aplikace nebo rozšíření do prohlížeče. Často je však za odcizení prostředků z peněženky zodpovědný samotný uživatel, protože nezná pravidla počítačové bezpečnosti a svůj privátní klíč nebo rovnou celou seed phrase uchovává v digitální podobě či na očích veřejnosti (Axie Infinity Limited 2022).

## 4.2 Lightning Network

Lightning Network je technologický fenomén postavený na druhé vrstvě Bitcoinu. Právě tady má fungovat jako platební vrstva pro rychlé a takřka bezplatné transakce, se kterými má klasická síť Bitcoinu občasné problémy. Především díky jednoduché škálovatelnosti a neblockchainovému řešení není nikterak omezen komplexností bitcoinové sítě. Existuje hned několik dalších způsobů mimo neblockchainové nastavby, jak dosáhnout větší škálovatelnosti. Je to například efektivnější zápis dat, zvětšení bloků, sharding nebo alternativní technologie.

Tato bitcoinová inovace vyvrací typickou kritiku, že Bitcoin nemůže fungovat pro účely každodenního života. Nutno ale poznamenat, že se celý projekt stále nachází v rané fázi a je zde pořád co zlepšovat. Autory konceptu jsou Joseph Poon a Thaddeus Dryja, kteří celý nápad zveřejnili a zkompletovali v roce 2016 ve svém whitepaperu. Nezávisle na sobě vzniká osm implementací v rozdílných programovacích jazycích: Lnd (GO), Eclair (scala), c-lightning (C), Electrum (Python), Rust-Lightning (Rust) a lnp-node (Rust).

Tato speciální nastavba přináší do systému škálovatelnost, instantní platby, mikro platby, finanční soukromí a do budoucna i možnost decentralizovaně směňovat další kryptoměny, což umožňuje technologie jménem Atomic Cross-Chain Swaps, ale bude záležet, kolik dalších kryptoměn Lightning Network přijme. V roce 2022 je stále výhradně určena pro Bitcoin.

Uzly jsou zpravidla tvořeny službami, jež síť používají k platbám, a zároveň poskytují bitcoinovou likviditu. Funguje to na principu platebních kanálů, což jsou chytré kontrakty, které v daném kanálu vytváří speciální adresu. Kanál obousměrně propojuje dvě protistrany a leží v něm ona speciální adresa, která přenáší bitcoinové mince. Odeslané bitcoiny skáčou z jednoho platebního kanálu na druhý a přepisují aktuální stavy speciálních adres, až dojdou po stanové cestě přes všechny uzly do cílové destinace. Na závěr do procesu vstupuje samotný Bitcoin jakožto systémová autorita a výsledné stavy účtů odesílatele a adresáta si zapíše na svůj blockchain (Frankenfield 2022a).

## 4.3 Smart Contracts

Smart Contract (přeloženo jako chytrá smlouva nebo jako chytrý kontrakt) je jakýkoliv protokol či software, který spravuje určité požadavky v kryptoměnách pomocí pravidel stanovených v kódu a v samotné smlouvě. Chytré smlouvy jsou zkrátka programy s jasně

stanovenými podmínkami, které jim dal programátor a plní zadanou funkci. Poprvé se tato myšlenka objevila v systému Bitcoin, ale jeho omezené možnosti nenaplňovaly požadavky komplexnějších programů. Protokol Bitcoinu je totiž velmi jednotvárný a neumožňuje takovou programátorskou svobodu. S příchodem Etherea a jeho obsáhlého skriptovacího jazyka a protokolu bylo konečně umožněno vývojářům psát svoje vlastní kódy a velké programy, které mohly pracovat uvnitř sítě, ale i mimo ni. Cílem Etherea je poskytovat velkou multifunkčnost, která by umožňovala nasazovat jakékoliv aplikace s vazbou na kryptoměny. Snaží se dostat do svého ekosystému nejen existující aplikace mimo toto odvětví, ale také přilákat úplně nové projekty.

Chytré kontrakty dokážou fungovat jako třeba účet s vícero podpisy, spravovat smlouvy z reálného života mezi uživateli, poskytovat nástroje dalším kontraktům a předávat či uchovávat veškeré potřebné informace. Kontrakty mohou spravovat například jakékoliv platby, nájmy, pojištění, peníze, akcie, fyzický majetek, pozemky apod. K těmto úkonům není potřeba žádný právník nebo notář, všechno je zastoupeno v kódu. Tímto způsobem se snaží zastoupit úkony úřadů a digitalizovat přebytečnou byrokracii. Ovšem reálné použití chytrých kontraktů je převážně u standardních aplikací, které pracují s kryptoměnami, kde zajišťují peněžní bezpečnost, jako například převody tokenů a obchodní aktivity uživatelů (Frankenfield 2022d).

#### **4.4 DeFi**

Decentralized Finance (přeloženo jako decentralizované finance) slouží pro tvorbu finančních prostředků. Nabízí služby půjčovacího a směňovacího charakteru. Obrovskou výhodou je fakt, že není potřeba prostředník, povinná registrace na dané platformě či dokladat identitu. Dalšími oblíbenými charakteristikami je minimalizace nutnosti důvěry, otevřenost kódu a dat (transparentnost), a finanční inkluze. Nejčastěji se jedná o ERC-20 tokeny v ekosystému Etherea, které je jednoznačným lídrem této podkategorie kryptoměn. V kryptoměnovém světě existuje velké množství alternativ, například na konkurenčních platformách jako Cardano, Polkadot a Binance Chain, ale také uvnitř platformy Etherea samotného. Každá taková kryptoměna, jež má služby DeFi ve svém ekosystému, má svoje další podsystémy, které umožňují DeFi tokeny volně obchodovat, směňovat, poskytovat likviditu, emitovat nové tokeny či je půjčovat dále.

Velcí investoři se často věnují takzvanému Yield Farming (přeloženo jako „výdělečné zemědělství“), což znamená, že uživatel poskytuje likviditu svými vlastními tokeny pro



nějakou službu, která mu na oplátku dává úplně jiný token jako odměnu. Tímto způsobem se může snadno emitovat nový bratrský token do oběhu. Avšak nízká regulovanost tohoto trhu otevírá okénko pro spousty skandálů a podvodů. Bohužel i dobré úmysly kolikrát končí katastroficky třeba kvůli chybě v zabezpečení daného protokolu, který token poskytuje, a celá platforma je pak vykradena hackery. Vznikají tak ztráty na tokenech v hodnotách milionů amerických dolarů (Sharma 2022b).

## 4.5 NFT

Non-Fungible Token (přeloženo jako nezaměnitelný token) stanovuje vlastnická práva digitálního majetku a v některých případech fyzický majetek digitalizuje právě pro vlastnické účely. Je to jakýsi transparentní doklad o vlastnictví. Dalo by se říct, že se tokenizuje cílový předmět a vytváří se mu kryptoměnová kopie, která je v rámci trhu originálem. Snaží se snadno a rychle určit majitele věci. Navíc přispívá k jednoduché přenositelnosti licence. Tato technologie způsobila velký rozmach tvorby umění, ale taky kontroverzního bizáru. Nejvíce se jako NFT emitují obrázky, ale technologicky by neměl být problém používat dokonce hudbu či video soubory (Mühlfeit 2022).

Na platformě Ethera to jsou tokeny standardu ERC-721, které jsou v rámci tohoto trhu nejdominantnější. V menším měřítku se podobné projekty také objevují u konkurenčních blockchainů. Je to finančně velmi bohatý byznys – částky za prodané NFT mohou být astronomické, řádově až miliony amerických dolarů. Problémem je však komplikovaná vymahatelnost vlastnických práv, protože za tím nestojí žádná autorita a nejsou jasně stanovená pravidla pro jejich užívání. Již několikrát se stalo, že vydání NFT proběhlo bez souhlasu jeho původního majitele a veškerý zisk šel autorovi tokenu, nikoliv autorovi originálního umění. Také se udává, že daný token je unikátní, což může být pravda v rámci jednoho blockchainu. Avšak nikoliv už v rámci ostatních blockchainů, protože nikdo nehlídá duplicitu jednoho kusu umění na vícero platformách. Nejznámějším NFT projektem jsou jednoznačně CryptoPunks, za které se již utratily desítky miliony amerických dolarů (Sharma 2022a).

## 4.6 DEX

Decentralized Exchanges (přeloženo jako decentralizované směnárny) jsou peer-to-peer tržiště, kde se setkává nabídka s poptávkou bez jakéhokoliv zásahu třetí strany. Celý systém je navržen tak, že páruje obchody automaticky skrze chytré kontrakty dané platformy, což může být například tahoun tohoto trhu Ethereum. Koncept DEX byl vytvořen z toho důvodu,

aby nebyla zapotřebí žádná autorita na řízení samotného tržiště, a nemohla tak vstupovat do směn a obchodů uživatelů systému. Zpravidla všechno funguje anonymně, tedy personální údaje nejsou vyžadovány. Pro vstup do systému se používají softwarové peněženky, které vlastní uživatel pro úschovu svých kryptoměn. Připojená peněženka pak funguje jako účet, přes který se vyřizují uživatelovy směnky a obchody. Směnárně je možné poskytovat likviditu, tedy propůjčit tokeny, aby mohla obchody snáze párovat s poptávkou. Tímto způsobem uživatel získává malý nárok na odměnu v podobě poplatků, které většinou zadavatel obchodu musel zaplatit. Celý systém je bezpečný a využívá kryptoměnových vlastností, jež se hodí pro finanční operace.

Nejznámější decentralizovaná směnárna je určitě Uniswap, který stojí za velmi úspěšným obchodovatelným tokenem se zkratkou UNI. Je určena pouze pro Ethereum a jeho ERC-20 tokeny. Jiné kryptoměny kromě tohoto standardu zde nelze směňovat, tedy pokud se nejedná o zástupný token jiné měny.

Mezi standardní centralizované směnární, v tomto případě hlavně kryptoměnové burzy, patří bezpochyby dva nejsilnější hráči na trhu jménem Coinbase a Binance. Coinbase je jedna z nejjednodušších a nejpoblárnějších burz převážně pro americký trh a také pro „ověřené kryptoměny“. Naopak Binance je profesionálnější burza s velkým množstvím různých kryptoměn se zvláštním sídlem na Maltě. Má velkou nabídku služeb a širokou uživatelskou podporu. Vytvořila vlastní blockchain jménem Binance Chain, na kterém běží její token Binance Coin. V kryptoměnových žebříčkách se dlouhodobě drží na vysokých pozicích, ovšem dostala také velkou porci kritiky pro patrnou centralizaci Binance Chainu a manipulaci trhu skrze Binance Coin, se kterým je možné snižovat burzovní poplatky. Tím snadno motivuje svoje uživatele, aby token drželi a aktivně používali (Cointelegraph.com 2022).

Výhody:

- Není potřeba ověřování identity uživatelů až na některé výjimky.
- Neexistuje riziko protistrany, protože samotné obchody jsou prováděny pomocí chytrých kontraktů.
- Lze směňovat tokeny, které nejsou zatím obchodovány na běžných centralizovaných burzách.

Nevýhody:

- Nejsou stejně uživatelsky přívětivé jako centralizované směnárny (CEX).
- Používají je převážně pokročilejší uživatelé.
- Mají většinou nižší likviditu.
- Nemusí nutně mít menší poplatky, poněvadž se poplatky za transakce jednotlivých blockchainů neustále mění (Benediktovich 2022).

## 4.7 P2E

Play to Earn (přeloženo jako „vydělávej hraním“) je herní model, ve kterém uživatel za hraní dané hry dostává tokeny, jenž reprezentují jeho finanční odměnu. Především díky dalším technologiím, jako například NFT a DEX, je možné veškeré herní předměty a tokeny volně obchodovat. Ekonomika hry je kontroverzní téma i pro samotné vývojáře. Některé modely spoléhají na pyramidový efekt, tedy aby uživatel vydělával, potřebuje k tomu nové hráče, kteří vstupují do systému. V jiných modelech se musí pravidla hry pečlivě vytvářet a neustále upravovat, aby se herní model nezhroutil. Často je taky méně profitabilní, protože těžší ze stabilní ekonomiky hry. To v praxi znamená menší výdělky, ale širší herní obsah, aby měl uživatel více prostoru, jak s předměty a tokeny dále zacházet. Ekonomika her je velmi křehká záležitost a čelí velké kritice ze strany konzervativních fanoušků kryptoměn. Často se může jednat o podvod, jak z lidí dostat jejich kryptoměny, nebo projekty nevydrží dlouho kvůli špatným rozhodnutím ohledně herního modelu a ekonomiky.

Tradiční herní průmysl funguje tak, že všechno je součástí ekosystému hry a nedovoluje dostat obsah hry mimo něj. Proto přišel P2E model, který využívá přenositelnost NFT a dává uživatelům svobodu spravovat svoje finance, herní předměty a herní tokeny.

Vývojář P2E hry vytvoří šablonu, podle které se budou nová NFT emitovat. To mohou být třeba zbraně nebo předměty ve hře, jenž uživatel normálně používá ke hraní. Dále vytvoří herní měnu, která bude součástí libovolné kryptoměny umožňující chytré kontrakty, jako například Ethereum. Ve výsledku většinu věcí, jež hra obsahuje, lze dostat mimo herní ekosystém a dále je vyměňovat či obchodovat na tržištích typu DEX s ostatními hráči. Nejznámější fenomén z této podkategorie kryptoměn je herní ekosystém pod názvem Axie Infinity nebo připravovaná hra Illuvium (Cook 2021).

## 5 Světová adopce kryptoměn

Kryptoměnová adopce může vznikat několika způsoby. Ať už třeba skrze těžební dominanci některých států díky dobrým podmínkám pro těžáře jako je levná elektřina či nulové daně z kryptoměn nebo cestou marketingu, kterou zvolil El Salvador tím, když přijal Bitcoin jako zákonné platidlo, a snaží se tak přilákat zahraniční investory a firmy.

Existují ale i přirozenější cesty, jak lidi motivovat kryptoměny nakupovat, či je dokonce používat. Koronavirová krize ukázala světu, jak mohou být státní peníze křehké, a pojmy jako inflace a státní bankrot začaly být více aktuální. S tím spojené stimulační balíčky tomu zasadily další hřebíček do rakve. To nakonec mohlo přesvědčit některé více konzervativnější investory, že existují alternativy ke státním penězům.

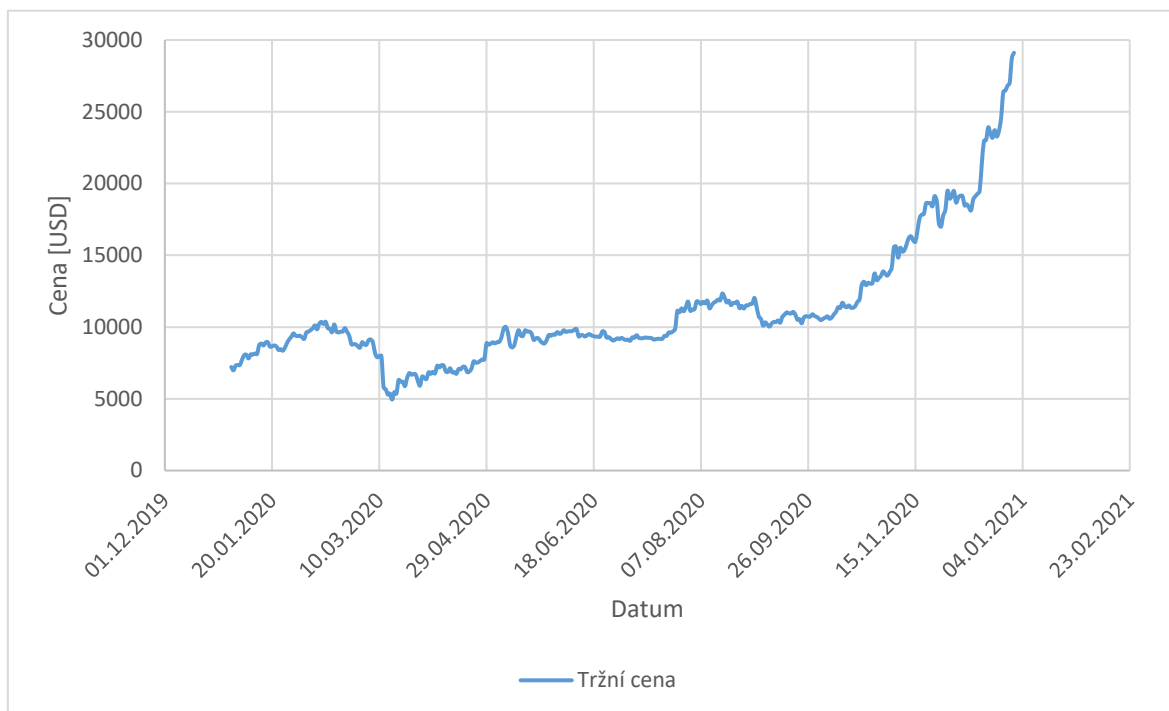
### 5.1 Koronavirová krize

Každý investor slyšel o velkém pádu všech trhů v březnu 2020 kvůli strachu z koronaviru. Je známý pod názvy jako Coronavirus Dump, Coronavirus Check nebo Coronavirus Test. Nastala oprávněná panika, která zapříčinila kaskádové prodeje a aktivace takzvaných stop loss (ochranný obchodní příkaz na otevřenou pozici). Tehdy například kryptoměnový trh odepsal během několika dní zhruba 80 % své hodnoty od lokálního maxima. Bitcoin se dostal pod \$4 000 za jednu minci. Právě u něj se začal zpochybňovat narativ takzvaného safe haven (přeloženo jako bezpečný přístav) a podle mnohých neustál těžkou zkoušku. Naopak potvrdil korelaci s akciovými trhy, které reagovaly naprosto totožně. Červené svíčky na grafu samozřejmě utrpěly i další sledované kryptoměny, jako například tehdejší velikáni Ethereum a XRP. Velké cenové propady na trzích také přispěly k myšlence obrovských stimulačních balíčků, jenž by měly zachránit trhy a obecně ekonomiku zasažených zemí (Rooney 2020).

Základním datovým souborem pro ukázkou pádu jsou naakumulovaná data o Bitcoinu, ve kterých jsou dva sloupce: datum (včetně svátků a víkendů od 1. 1. 2020 do 31. 12. 2020) a tržní cena za 1 bitcoin v americkém dolaru. Tady je ukázkou se vstupní tabulkou (Tabulka 1) a s výstupním grafem (Graf 1), jak může vypadat takový cenový výkyv a jaké jsou jeho etapy. Důležitá je oblast okolo 10. března 2020, tedy oblast velkého propadu.

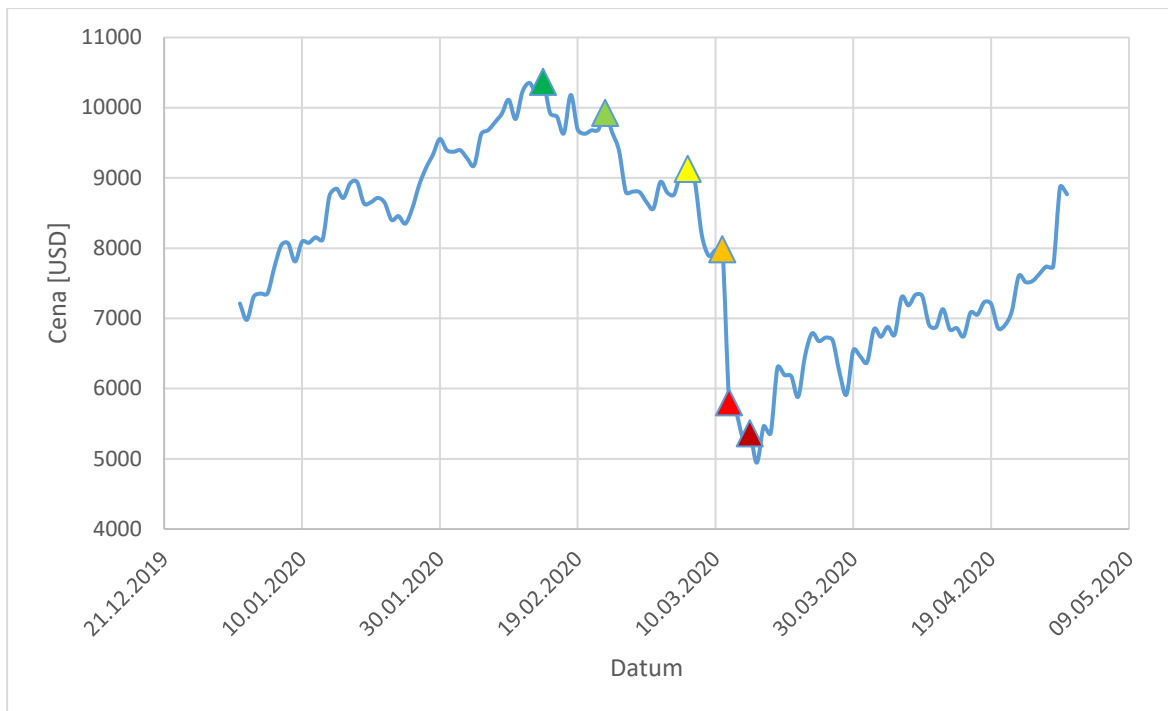
Tabulka 1 – ukázková vstupní data tržní ceny za 1 bitcoin v americkém dolaru s denním razítkem

Date	Price [USD]
01.01.2020	7211,21
02.01.2020	6979,07
03.01.2020	7307,53
04.01.2020	7353,26



Graf 1 – vliv koronavirové krize na tržní cenu Bitcoinu

Koronavirový pád v kontextu s cenovým průběhem celého roku nezaznamenal znatelný vliv na dlouhodobé chování aktiva. Jak je patrné z grafu, tržní cena Bitcoinu dohnala ztrátu do 2 měsíců, což lze považovat za opravdu rychlé zotavení trhu. Paradoxně lze konstatovat, že právě koronavirová krize nastartovala trhy, a přispěla tak k velkému rozvoji kryptoměn alespoň co se týče tržních cen těchto aktiv a zájmu o jejich používání.



Graf 2 – vliv koronavirové krize na tržní cenu Bitcoinu v detailu

Detailní graf (Graf 2) je zaměřen přímo na období koronavirového pádu od 1. 1. 2020 do 30. 4. 2020. Při detailnějším pohledu je vidět, že se jednalo téměř až o 80% pád od lokálního maxima po lokální minimum. Je to ukázková reakce trhu na stupňující se nejistotu a strach.

Psychologické fáze na trhu před pádem, během pádu a na konci pádu:

- Euphoria ▲ (přeloženo jako euforie) – nejpozitivnější část růstu ceny aktiva, který obvykle probíhá v bleskovém tempu.
- Complacency ▲ (přeloženo jako spokojenost) – stále převládá obstojná pozitivita na trhu, protože tržní cena se drží blízko lokálního maxima.
- Anxiety ▲ (přeloženo jako úzkost) – přichází první menší pád, který je našťastí pro investory brzy zastaven na takzvaném prvním větším supportu.
- Denial ▲ (přeloženo jako odmítnutí) – následuje další prudší pád na lokální minimum.
- Panic ▲ (přeloženo jako panika) – finální pád pod lokální minimum boří poslední zbytky naděje.
- Capitulation ▲ (přeloženo jako kapitulace) – většina investorů likviduje svoje investice.

Těmito stupni lidských emocí se trh samozřejmě neřídí vždycky, ale v některých případech tento model dokonale odpovídá realitě, jako například u tohoto pádu. Původně byl vytvořen na Wall Street jako vzorová ukázka ekonomických cyklů na trhu. Oficiálně se mu říká Psychology of Market Cycles (přeloženo jako psychologie tržních cyklů). Lze ho však aplikovat i na krátkodobé chování trhu (Williams 2022).

## 5.2 Stimulační balíčky

Největší stimulační balíček 2,2 bilionu amerických dolarů schválil Donald Trump dne 27. března 2020. Stal se historicky největším americkým i světovým stimulem. Cílem bylo zachránit americké trhy, které byly silně zdevastované koronavirovou krizí. Dále tím chtěl podpořit americké rodiny, zdravotní systém, malé podniky a letecký průmysl. Byl označen zkratkou CARES (Coronavirus Aid, Relief and Economic Security Act) (The Investopedia Team 2022a).

Další významný stimulační balíček přinesl do americké ekonomiky Joe Biden. Jednalo se o finanční pomoc v hodnotě 1,9 bilionu amerických dolarů, která nese označení ARPA (American Rescue Plan Act). Byl odsouhlasen všemi zákonodárnými orgány a samotným prezidentem USA 11. března 2021. Balíček cílil především na podporu amerických domácností, městské správy, lokálních vlád a také na financování školství. Zařadil se tak na 2. místo největších záchranných balíčků v historii USA. Schválený stimul samozřejmě prohloubil schodek, který se dostal na částku 3,5 bilionu amerických dolarů, což je asi 16 % HDP země (Tan 2021) (Haagensen 2022). Přehledné srovnání stimulačních balíčků je v následující tabulce (Tabulka 2).

*Tabulka 2 – přehled významných stimulačních balíčků*

<b>Tehdejší prezident</b>	<b>Datum schválení</b>	<b>Velikost balíčku [USD]</b>
Barack Obama	17. února 2009	0,8 bilionu
Donald Trump	27. března 2020	2,2 bilionu
Joe Biden	11. března 2021	1,9 bilionu

Evropy se týká především záchranný fond finanční pomoci pro země platící eurem jménem euroval (Evropský stabilizační mechanismus). Velké drama způsobil na Slovensku v letech 2011 a 2012, kdy se jednalo o jeho přijetí v poslanecké sněmovně, což zaznamenalo vlnu kontroverze ve společnosti a ve slovenské politice. Ve stejné době se navíc řešila tíživá

situace Řecka, kdy se dokonce mluvilo o jeho krachu. Obavy o budoucnost eura, které je v rukách ECB (European Central Bank), se nedotýkají v takovém měřítku České republiky, protože její nativní měnou je česká koruna. Ovšem jako členský stát EU (European Union) je ovlivňována celkovou situací evropského trhu (Charvát 2011).

Přítok nových peněz do finančního systému mnohdy znamená zvýšenou likviditu na trhu. Je prokázáno, že poměrně velká část finanční podpory skončí právě v různých investičních aktivech, což se dá časem pozorovat na příslušných grafech tržní ceny. Je to pomalý jev. Ovšem je složité takové věci dokazovat v krátkodobém horizontu, protože trh reaguje na spousty signálů. Mnoho investorů může spekulovat na základě nepotvrzené informace či prvotního návrhu, který může mít vliv na cenový vývoj aktiva. V praxi to tedy znamená, že už jenom projednávání takového stimulu například v kongresu může přesvědčit některé spekulanty, aby si otevřeli takzvaný long, tedy nakoupí určité aktivum a doufají, že se jeho cena zhodnotí v dosažitelném horizontu, aby jej následně prodaly. Říká se tomu „*buy the rumor, sell the news*“ (Stroukal a Skalický 2021).

### **5.3 Státní bankroty**

Hned několik států zažilo velké problémy, když jejich centrální banka nedokázala zachránit jejich nativní měnu. Příkladem může být Venezuela, Nigérie, Libanon či Srí Lanka. To vyvolalo vlny nepokojů ve všech zmíněných zemích a hromadné vybírání peněz z bank a bankomatů. Mnohdy lidi čekají dlouhé hodiny, ale na záchranu jejich úspor je zpravidla pozdě. Buď se ke svým penězům vůbec nedostanou, nebo nemají žádnou hodnotu. Na řadu pak přichází otázka, kam si odkládat část své výplaty na horší časy v případě podobné katastrofy. Mnohdy se jako dobrý tip uvádí zlato, index S&P 500 nebo právě kryptoměny, hlavně tedy Bitcoin či Ethereum.

#### **5.3.1 Venezuela**

Mezinárodní ratingová agentura S&P Global Ratings dne 13. listopadu 2017 oficiálně deklarovala takzvaný selektivní bankrot Venezuely. Venezuelský zahraniční dluh je takřka nesplacitelný. Celkový dluh činí již téměř 200 miliard amerických dolarů. Země pochází procesem restrukturalizace a pravděpodobně budou zabaveny venezuelská aktiva především v oblasti ropy. Problém domácího dluhu skončil u hyperinlace, která byla na konci roku 2017 na roční úrovni zhruba 700 %. USA již dříve na Venezuelu uvalila těžké sankce. Posléze se přidala také Evropská unie. Ze země přichází reportáže, jak obyvatelé vyhazují a pálí svou měnu – Venezuelský bolívar. Turistům z této bankovky skládají origami nebo



různé ozdobné předměty. Bolívar nemá takřka žádnou hodnotu. Lidi mají často problém dostat se k zahraničním měnám, jako například k americkému dolaru, kvůli přísným sankcím a nedostatku finančních služeb. Proto jednou z posledních možností bývá Bitcoin, do kterého se snaží přesunout svoje zbytky kupní síly. Situace je zoufalá pro všechny strany. Kromě drobné pomoci od Ruska a Číny je země ponechána na pospas svému osudu (Křeček 2017).

### **5.3.2 Nigérie**

Nigérie zažívá těžké časy nejen kvůli koronavirové krizi, ale také kvůli problémům ve vládě. Inflace rychle roste, spotřebitelské ceny s tím jdou společně ruku v ruce nahoru a velká nezaměstnanost vlivem přelidnění země prohlubuje problém. Zkorumpovaná vláda špatně reaguje a u monetární politiky dělá jednu chybu za druhou. V tehdejších počátcích krize se země proslavila tím, že velká část populace shodou okolností začala používat Bitcoin a aktivně investovat do kryptoměn. Mohl za to velký nárůst služeb a poměrně jednoduchý přístup k zprostředkovatelům směny. V některých obchodech se dokonce objevily QR kódy na zaplacení nákupu pomocí bitcoinů (Lacina 2021).

### **5.3.3 Libanon**

Na Libanon dopadla těžká ekonomická krize, která má prapočátky ve špatném politickém vladaření. Samozřejmě velký vliv měla také koronavirová krize. Zkolaboval zdravotní systém, státní měna i hospodářství. Většina obyvatelstva drasticky zchudla i na místní poměry a prchá ze země. Jedná se o desetitisíce uprchlíků. Libanonská libra spadla oproti americkému dolaru takřka na svoje historické dno. Tento stav lze považovat za státní bankrot a kolaps libanonské centrální banky. Situaci se snaží hasit nová vláda, ale tento rozjetý vlak je již téměř nemožné zastavit. Poslední zbytky peněžní hodnoty se obyvatelé snaží směnit do amerického dolaru, nastala tak dolarová horečka. V zemi totiž nejsou příliš populární kryptoměny ani další aktiva, takže společnost spoléhá na tradiční valuty (Macháček 2021).

### **5.3.4 Srí Lanka**

Srí Lanka je dlouhodobě na hraně státního bankrotu, protože má obrovský zahraniční dluh, který již nadále nemůže splácet. Země se potýká s nedostatkem základních surovin, kvůli čemuž nastaly masivní nepokoje. Srílanská rupie zažívá znatelný pád a pozastavený import některého zboží zhoršuje podmínky v zemi. Velká neúroda a stagnující obchod situaci příliš nepomáhají. Je otázkou času, než přijde hon na banky a bankomaty. Státní měna by takový směnový nápor nemusela vydržet. Nejpravděpodobněji se lidé budou obracet na americký dolar, ale není vyloučeno, že někteří využijí kryptoměnových aktiv jako třeba Bitcoinu. Bude

záležit hlavně na dalších prohlášeních ministerstva financí a akcích vlády, která historicky podnikala spíše špatné kroky. Není potom divu, že náznaky krize přišly už před koronavirem (Dulínek 2022).

## 6 Investiční ukazatele technické analýzy

Investiční ukazatele jsou součástí každé technické analýzy dobrého investora, která vychází z matematických předpokladů a tržních mechanismů. U kryptoměnového trhu se používají totožné technické ukazatele jako u devizového trhu, akciového trhu a trhu s komoditami. Obzvláště u kryptoměn jsou hodně populární díky široké adopci a velké popularitě tohoto nového odvětví. Technická analýza jde ruku v ruce s fundamentální analýzou, jež se snaží stanovit vnitřní hodnotu aktiva na základě subjektivních informací.

Obchodníci častokrát při analýze aktiva používají několik různých technických indikátorů současně. Možností mají hned několik. Proto si obchodníci musí vybrat ty indikátory, které jim vyhovují nejvíce a seznámit se s jejich funkcionalitou. Případně mohou kombinovat technické indikátory se subjektivnějšími formami technické analýzy, jako je například sledování vzorů a formací ve grafu, aby přišli s obchodními nápady. Technické indikátory mohou být také začleněny do automatizovaných obchodních systémů vzhledem k jejich kvantitativní povaze, jako například nákupních a prodejních botů.

Technické ukazatele se dělí na dvě základní kategorie:

- překrývací indikátory – používají stejné měřítko jako ceny aktiva a jsou vyneseny přes samotný cenový graf. Příkladem mohou být klouzavé průměry, Bollingerova pásma nebo Fibonacciho linie.
- oscilující indikátory – oscilují mezi lokálním minimem a maximem, a jsou vykresleny nad nebo pod cenovým grafem. Příkladem mohou být stochastické oscilátory, MACD nebo RSI (The Investopedia Team 2022b).

Mezi klasické nástroje patří třeba SMA, EMA, MACD a RSI. Tyto a mnohé další ukazatele pomáhají investorům lépe pochopit chování trhu a snáze předvídat jeho následné pohyby. Kromě těchto technických ukazatelů se používají další metriky, které vycházejí z reálných dat o dané kryptoměně, jako například hashrate sítě, počet nových uživatelů, aktivní počet adres, uhrazené poplatky za transakce apod. Zpravidla jsou tato data veřejná a snadno dostupná na různých analytických portálech (Binance Academy 2022d).

### 6.1 SMA

Simple Moving Average (přeloženo jako klouzavý průměr) patří mezi základní varianty klouzavých průměrů MA (Moving Average). Klasické klouzavé průměry MA se nejčastěji

používají k vyhlazování grafů. Opírají se o minulá data, díky čemuž se považují za zpožděné indikátory a pozorovatele trendu. U indikátoru SMA se vstupní data berou ze stanoveného časového období, ze kterého se vytváří průměrné hodnoty pro celý datový soubor. Každá průměrná hodnota v datovém balíčku se spočítá z předchozích hodnot, jejichž počet je přesně stanoven a je pro všechny průměry stejný. Pokud by se například jednalo o SMA(20), tak by aktuální hodnota vznikla z předchozích 20 hodnot, ze kterých se počítal průměr. Takto získaný průměr se stanoví pro celý datový soubor, aby se zpožděním kopíroval graf zvoleného aktiva. Nutno podotknout, že veškerá vstupní data mají stejnou váhu bez ohledu na to, jak nedávno byly zadána. Naopak nejnovější dostupná data mají větší relevanci u exponenciálního klouzavého průměru, jenž se zkráceně označuje EMA.

Ideálním příkladem z praxe je kombinace SMA s periodou 50 a SMA s periodou 100. Nákupní signál vzniká v moment, kdy SMA(50) zespondu protne SMA(100) a následně vzroste tržní cena aktiva (Binance Academy 2022c).

## 6.2 EMA

Exponential Moving Average (přeloženo jako exponenciální klouzavý průměr) patří mezi pokročilejší varianty klouzavých průměrů MA. Indikátor EMA je hodně podobný své jednodušší verzi SMA, protože oba poskytují analýzu založenou na minulých datech. Ovšem výpočet je trochu složitější, jelikož dává větší váhu novějším datům. Obecně se uvádí, že EMA lépe reaguje na náhlé výkyvy trhu. V praxi se nejčastěji používá u krátkodobých obchodů. Někdy se doporučuje používat jak SMA, tak EMA pro krátkodobý a dlouhodobý kontext.

V praxi je poměrně rozšířenou kombinací EMA s periodou 20 a EMA s periodou 50. Když EMA(20) zespondu protne EMA(50), tak se jedná o rostoucí trend. Opačně pokud EMA(20) seshora protne EMA(50), tak se jedná o klesající trend (Binance Academy 2022c).

## 6.3 RSI

Relative Strength Index (přeloženo jako index relativní síly) je momentum indikátor, který měří velikost a rychlost pohybů cen či sledovaných dat. Vytvořil ho John Welles Wilder v roce 1978, kdy byl představen v jeho knize jménem *New Concepts in Technical Trading Systems* (přeloženo jako *Nové koncepty v technických obchodních systémech*) a aktivně se používá dodnes. Indikátor RSI standardně měří změny v ceně aktiva za 14 period, které mohou být vyjádřeny 14 dny na denních grafech, 14 hodinami na hodinových grafech apod.

Ve vzorci vystupuje průměrný zisk, který je vydělen průměrnou ztrátou. Data jsou pak reprezentována na stupnici od 0 do 100. Když se hybnost zvyšuje a cena roste, znamená to, že o nákup aktiva je velký zájem. Pokud hybnost klesá, je to známkou toho, že se zvyšuje prodejní tlak. Tímto způsobem označuje situaci aktiva na trhu buď jako překoupenou nebo přeprodanou. Zatímco skóre RSI 30 nebo méně naznačuje, že aktivum je pravděpodobně blízko svého dna, tedy přeprodaný tržní stav. Hodnoty RSI nad 70 bodů říkají, že je cena aktiva pravděpodobně blízko svého maxima za dané období, tedy nastal překoupený tržní stav (Binance Academy 2022a).

## 6.4 MACD

Moving Average Convergence Divergence (přeloženo jako klouzavý průměr konvergence a divergence) je momentum indikátor, který se používá k sledování trendů a hybnosti aktiva. Byl vyvinut na konci 70. let 19. století investorem Geraldem Appelem. Poskytuje signály na základě minulých cenových pohybů, čímž se řadí mezi zpožděné indikátory. Mnoho obchodníků jej používá k odhalení potenciálních vstupních a výstupních bodů. Indikátor MACD je generován odečtením dvou exponenciálních klouzavých průměrů EMA, čímž se vytvoří hlavní čára představující přímo MACD. Ta se pak použije k výpočtu dalšího exponenciálního klouzavého průměru EMA, jenž představuje signální čáru. K tomu se přidá MACD histogram, který je vypočítán na základě rozdílů mezi těmito dvěma čarami. Histogram spolu s dalšími dvěma čarami kolísá nad a pod středovou čarou, které se říká nulová čára.

Indikátor MACD se skládá ze tří prvků pohybujících se kolem nulové čáry:

- MACD čára, jež pomáhá určit vzestupnou nebo sestupnou hybnost neboli tržní trend. Vypočítá se odečtením dvou exponenciálních klouzavých průměrů EMA (1).

$$\text{MACD čára} = \text{EMA}(12) - \text{EMA}(26) \quad (1)$$

- signální čára, která vznikne aplikováním exponenciálního klouzavého průměru EMA zpravidla s periodou 9 na MACD čáru. Kombinovaná analýza signální čáry s MACD čarou může být užitečná při odhalování potenciálních zvrátů nebo vstupních a výstupních bodů (2).

$$\text{Signální čára} = \text{EMA}(9)[\text{MACD čára}] \quad (2)$$

- MACD histogram, který představuje grafické znázornění divergence a konvergence MACD čáry a signální čáry. Jinými slovy, histogram se vypočítá na základě rozdílů mezi těmito dvěma čarami (Binance Academy 2022b) (3).

$$\text{MACD histogram} = \text{MACD čára} - \text{signální čára} \quad (3)$$

## 6.5 OBV

On-Balance Volume je momentum indikátor, jenž se používá v technické analýze k měření nákupního či prodejního tlaku. Vyvinul ho Joe Granville v 70. letech 19. století. Jeho indikátor byl považován za revoluční a dodnes je stále velmi populární mezi obchodníky. Zohledňuje objem obchodů, které mohou tlačit cenu aktiva nahoru nebo dolů. Jedná se o kumulativní typ indikátoru, což znamená, že když jde cena aktiva nahoru, je aktuální peněžní objem přičten do kumulativní hodnoty OBV. Naopak, když jde cena dolů, je aktuální peněžní objem odečten od kumulativní hodnoty OBV. Pokud tedy OBV roste, tak jsou obchodníci ochotni vstoupit na trh a tlačit cenu výše. Když OBV klesá, objem prodeje převyšuje objem nákupu, což naznačuje nižší ceny. Tímto způsobem pak funguje jako nástroj pro potvrzování trendu.

- Pokud je nynější zavírací tržní cena vyšší než včerejší zavírací tržní cena aktiva (4):

$$\text{OBV} = \text{OBV}_{n-1} + \text{zobchodovaný objem} \quad (4)$$

- Pokud je nynější zavírací tržní cena nižší než včerejší zavírací tržní cena aktiva (5):

$$\text{OBV} = \text{OBV}_{n-1} \quad (5)$$

- Pokud se nynější zavírací tržní cena rovná včerejší zavírací tržní ceně aktiva (6):

$$\text{OBV} = \text{OBV}_{n-1} - \text{zobchodovaný objem} \quad (6)$$

Dále je důležité sledovat takzvanou divergenci. Ta nastává, když ukazatel a tržní cena jdou různými směry, tedy proti sobě nebo od sebe. Pokud cena roste, ale hodnota OBV klesá, mohlo by to znamenat, že trend není podporován silnými kupci (takzvanými velrybami) a mohl by se brzy obrátit (Hayes 2022b).

## 6.6 A/D

Accumulation/Distribution (přeloženo jako akumulace/distribuce) je kumulativní indikátor, který používá peněžní objemy a tržní ceny k určení, zda se zásoby aktiva hromadí, nebo distribuují. Rozdíly mezi cenou aktiva a objemem dávají obchodníkům vědět, jak silný je trend. Pokud cena roste, ale indikátor klesá, tak to naznačuje, že objem nákupu nebo

akumulace nemusí být dostatečný k podpoře růstu ceny a může dojít k náhlému poklesu. Čára A/D napovídá, jak faktory nabídky a poptávky ovlivňují cenu aktiva. Hodnota A/D a tržní cena se mohou pohybovat stejným směrem nebo opačným směrem. V obou případech se řeší pouze pohyb A/D.

Dále se určuje, zda byla tržní cena zavřena v horní nebo dolní části svého rozpětí (7). Tato hodnota se pak vynásobí peněžním objemem (8). Když například aktivum zavře blízko svého maxima za vybrané období, a zároveň je to podpořeno vysokým objemem, tak to povede k velkému A/D skoku. Naopak, pokud cena skončí blízko horní části rozsahu, ale objem je nízký, nebo pokud je objem vysoký, ale cena skončí spíše uprostřed rozsahu, pak se A/D neposune o tolik nahoru. Stejná pravidla pak platí, když tržní cena zavře v dolní části cenového rozpětí v daném období. Jak moc hodnota A/D poklesne určuje velikost objemu a uzávěrka ceny (Mitchell 2022) (9).

MFM = Money Flow Multiplier (násobitel zobchodovaných objemů)

Close = Closing Price (zavírací tržní cena)

Low = Low Price for the Period (nejnižší tržní cena v daném intervalu)

High = High Price for the Period (nejvyšší tržní cena v daném intervalu)

MFV = Money Flow Volume (míra zobchodovaných objemů)

$$\text{MFM} = \frac{(\text{close} - \text{low}) - (\text{high} - \text{close})}{\text{high} - \text{low}} \quad (7)$$

$$\text{MFV} = \text{MFM} \times \text{zobchodovaný objem} \quad (8)$$

$$\text{A/D} = \text{A/D}_{n-1} + \text{MFV} \quad (9)$$

## 6.7 ADX

Average Directional Index (přeloženo jako průměrný směrový index) je momentum indikátor, který se používá k určení síly trendu. Trend může být samozřejmě vzestupný i sestupný, což definují dva doprovodné indikátory: negativní směrový indikátor (-DI) a pozitivní směrový indikátor (+DI). Proto ukazatel ADX běžně obsahuje tři samostatné čáry, které pomáhají určit, jestli má vůbec smysl obchod realizovat, případně jaký typ obchodu: short nebo long. ADX se identifikuje jako silný trend, když je hodnota ADX nad 25 body. Za slabý trend se označuje, když je hodnota ADX pod 20 body. Navíc křížení čar -DI a +DI lze použít ke generování obchodních signálů. Pokud se například čára +DI protne nad čarou -DI a hodnota ADX je nad 20 body, nebo ideálně dokonce nad 25, pak je to

potenciální signál k nákupu. Na druhou stranu, pokud  $-DI$  protne  $+DI$  a hodnota  $ADX$  je nad 20 nebo 25 body, pak je to příležitost vstoupit do potenciálního obchodu typu short. Překřížení je také možné použít k ukončení aktuálních obchodů. Pokud má obchodník otevřený obchod typu long, tak jej ukončí v moment, co  $-DI$  protne  $+DI$ . Tento indikátor se skládá z několika částí a dalšího ukazatele jménem  $ATR$  (Average True Range), čímž se jeho výpočet lehce komplikuje a nikdy se nepočítá manuálně. Sice patří do rodiny klasické technické analýzy, ale často jej používají pouze zkušenější obchodníci (Mitchell 2021).



## 7 Statistické metody

### 7.1 Časové řady

Časové řady jsou věcně a prostorově srovnatelná pozorování, která jsou jednoznačně seřazena podle času od minulosti do přítomnosti. Mohou být například ekonomického, technologického nebo přírodovědného druhu. Dělí se do dvou základních kategorií: okamžikové a intervalové. Číselná řada může být buď stacionární, nebo nestacionární. Stacionární řada je taková řada, u které se jak střední hodnota (průměr), tak rozptyl nemění v závislosti na čase. Cílem je predikce (extrapolace), porozumění zákonitostí časových řad, nalezení neočekávaných odchylek nebo vyrovnání (interpolace).

V případě některých chybějících hodnot v datovém souboru je možné tyto data doplnit průměrem/mediánem, trendem či speciálním modelem. Samotná časová řada se skládá z trendu (označeno T), cyklické složky (označené C), sezónní složky (označeno S) a reziduální složky (označené E). Trend je lineární tendence řady, cyklické složky jsou nepravidelné výkyvy s dlouhou periodou, sezónní složky jsou pravidelné kolísání s danou periodou a reziduální složky jsou považovány zpravidla za šum.

Bílý šum je posloupnost nezávislých náhodných veličin s nulovou střední hodnotou a konstantním rozptylem. Náhodná procházka je pak časová řada, která je tvořena kumulativním součtem bílého šumu. Jednou z oblastí použití bílého šumu je akustika, ve které je definován jako náhodný signál se stejným výkonem v jakémkoli pásmu stejné šířky. Používá se například v sirénách pohotovostních vozidel a v elektronické hudbě.

U časových řad se často vyskytuje několik druhů klouzavých průměrů, které mají řady vyhladit, čímž se snižuje jejich rozptyl a šum. Mezi ně patří symetrické, předpovědní, zpožděné a dopřední klouzavé průměry. Tyto průměry hrají významnou roli v investorské činnosti jako jeden z ukazatelů na grafu tržní ceny obchodovaného aktiva. Výsledná křivka se označuje MA, tedy z angličtiny Moving Average.

K vytváření modelů existují různé metody, které se uplatňují podle požadavků na výsledný model. Je to například metoda sezónního očišťování, metoda modelování trendu, metoda sestavení modelu dekompozicí a metoda sestavení modelu regrese.

Míra shody ověřuje kvalitu modelu a sleduje rozdílnost skutečnosti a samotné předpovědi. Slouží k tomu parametry jako koeficient determinace (R-Squared), MSE (Mean Squared

Error), RMSE (Root Mean Squared Error), MAE (Mean Absolute Error), MaxAE (Maximum Absolute Error), MAPE (Mean Absolute Percentage Error) a BIC (Bayesian Information Criterion). Pomocí stacionárních funkcí je možné vyjádřit sílu vztahu mezi hodnotami řady vzdálených určitý počet období. Mezi stacionární funkce patří ACF a PACF. ACF měří vztah skrze korelační koeficient, u PACF (P jako parciální) je použit parciální korelační koeficient.

Pro vyrovnávání neboli interpolaci časové řady existuje několik základních modelů. Mezi ně patří model exponenciálního vyrovnání, který se dělí na jednoduchý a lineární, a sezónní model vyrovnání. U exponenciálního vyrovnání se předpokládá, že vliv bodů na předpověď exponenciálně klesá do minulosti, čímž klade větší důraz na poslední záznamy. Sezónní vyrovnání se hodí u časových řad, kde je známý trend a sezónnost.

Dále je tu Boxova-Jenkinsova metodologie, která hledá závislosti současné hodnoty na minulých. K tomu slouží například model ARIMA (složeno ze zkratk procesů AR, I a MA). V modelu se nachází náhodná složka v podobě bílého šumu a samotný model se skládá ze tří procesů: autoregresní proces (AR), integrovaný proces (I) a proces klouzavých průměrů (MA). AR je závislost současné hodnoty na lineární funkci minulých hodnot. MA definuje závislost na lineární funkci minulých chyb. I představuje proces náhodné procházky, který určuje závislost na lineární funkci minulých hodnot s koeficienty 1. Procesy AR a MA je možné rozšířit o operátor zpětného posunutí označený B. Ten se používá k jednoduchému zápisu komplexnějších procesů a umožňuje snadnou úpravu rovnice procesu do logického tvaru. Pro zjednodušení celého modelu je možné použít model ARMA bez procesu náhodné procházky, kde je možné zaměňovat AR za MA a naopak. Další alternativou, jež se používá pro zavedení sezónních procesů, je SARIMA (S jako sezónní).

Pro další porozumění modelu se používá trend. Existuje několik typů: deterministický trend (lineární), stochastický trend (prvního řádu), stochastický a deterministický trend (prvního řádu), a ve výjimečných případech kvadratický trend. Právě charakteristika trendu v modelu má významný vliv na kvalitu výsledné předpovědi.

Potom lze provést takzvaný test jednotkového kořene, aby se odhalil stochastický trend (jednotkový kořen), protože rozlišovat různé typy trendů není v praxi jednoduchým úkolem. V případě, že je polynom roven 0 v bodě 1, tak má řada jednotkový kořen. Rovnici řady je možné napsat za pomoci polynomu operátoru zpoždění B. Realizace testu jednotkového

kořene se standardně provádí Dickeyovým-Füllerovým testem v základní podobě nebo v rozšířené verzi, či také pomocí KPSS (Kwiatkowski-Phillips-Schmidt-Shin) testu.

Pokud by byla potřeba zkoumat vliv dalších řad právě na zkoumanou řadu, tak se k tomu používá ARIMA s nezávislými proměnnými. Problém je autokorelace, tedy nevhodnost používat klasickou regresi. Avšak je možné modelovat závislé případy dle potřeby.

Druhy vlivu nezávislých časových řad realizované TF (Transfer Functions):

- TF čitatel (Numerator):
  - vliv aktuálních a minulých hodnot prediktoru na aktuální hodnotu zkoumané řady.
- TF jmenovatel (Denominator):
  - vliv není možné identifikovat jednoduchým způsobem.
- TF posun (Transfer):
  - vliv prediktoru v období je na zpoždění b nulový.
- TF diference (Difference):
  - vliv na zkoumanou řadu má diference prediktoru (Weisinger 2022).

Další možností je použít ADL (Autoregressive Distribution Lags) model, ve kterém se dá modelovat například diference, ale již se neuvažuje sezónnost. Ovšem je možné tuto vlastnost vhodně nahradit. Vystupuje zde proměnná  $Y$ , jež závisí na vlastních zpožděných hodnotách a na zpožděných hodnotách  $X$  v modelu se zpožděními residui  $\epsilon$ .

CCF (Cross Correlation Function) vyjadřuje sílu vztahu mezi dvěma časovými řadami s různým posunem. Funkce je tvořena korelačními koeficienty, jak už napovídá název. Výsledná hodnota se spočítá pro každou hodnotu posunu zvlášť v obou směrech.

Dekompozice časové řady ukazuje několik důležitých vlastností, které pomáhají lépe pochopit chování časové řady.

- Additive nebo také Additive Patch je náhlý bodový šok v záznamu, což se projevuje velkým a rychlým nárůstem či poklesem na grafu.
- Seasonal Additive je pravidelný bodový šok v záznamu, jenž se opakuje pouze u sezónní časové řady.

- Level Shift je náhlý schodovitý šok, který si svou hodnotu zachovává.
- Local Trend je lineární trend v časové řadě, který začíná v jakýkoliv moment záznamu, ale pokračuje až do konce řady.
- Temporary Change nebo také Transient Change je geometricky klesající trend v časové řadě, který začíná v jakýkoliv moment záznamu, ale pokračuje až do konce řady.
- Innovational je náhlý bodový šok v reziduích, co generují časovou řadu. To se projevuje velkým a rychlým nárůstem či poklesem na grafu (Arlt et al. 2002).

## 7.2 Regresní analýza

Regrese zkoumá především jednostranné závislosti proměnné  $y$  na proměnné  $x$ . Nezávislá proměnná je brána jako příčina a závislá proměnná jako důsledek. U regresní analýzy se klade důraz na směr závislosti, takže se určuje, která proměnná je závislá, a která naopak nezávislá. Závislost se zpravidla modeluje skrze matematickou funkci, které se říká regresní funkce (Hendl 2021).

## 7.3 Korelační analýza

Korelace je vzájemný vztah dvou veličin. Pokud se mezi dvěma veličinami potvrdí korelace, je pravděpodobné, že jsou veličiny na sobě závislé. Ve statistice pojem korelace znamená vzájemný lineární vztah mezi dvěma veličinami  $x$  a  $y$ . Je to jedna ze základních metod posuzování lineární závislosti. Zabývá se hlavně intenzitou vztahu dvou veličin a klade se na to větší důraz než na směr závislosti. Míru korelace vyjadřuje korelační koeficient, jenž může nabývat hodnot od  $-1$  až do  $+1$ . Pojem korelace („correlatió“) pochází z latiny a přesně vystihuje míněný význam, protože to znamená „vzájemnou souvislost“ (Hendl 2021).

## 8 Analýza bitcoinového trhu

### 8.1 První analýza časových řad

Tato analýza využívá vlastností časových řad. Cílem výsledného modelu je predikovat chování zkoumané řady v daném časovém horizontu. V tomto případě byla zvolena tržní cena Bitcoinu a predikovaným obdobím je 1 týden (7 dní) a 1 měsíc (30 dní).

Analýza časových řad pro svoje predikce bere v potaz zadané parametry, které pak mohou mít přímý vliv na cenový vývoj Bitcoinu. Pro tento model, který zkoumá bitcoinovou tržní cenu (price), byly vybrány tyto indikátory: zobchodované peněžní objemy za bitcoiny (volume), výpočetní výkon bitcoinové sítě (hashrate), .FGI (komunitní index Fear & Greed, tedy strach a chamtivost na bitcoinovém trhu) a .SPX (index S&P 500, tedy 500 největších obchodovatelných podniků v USA). Tečka před zkratkou označuje, že se jedná o index.

Důvody výběru těchto ukazatelů:

- zobchodované peněžní objemy za bitcoiny – celkový počet peněz, který proteče centralizovanými burzami pro kryptoměny, má vliv na likviditu a cenové výkyvy aktiva.
- výpočetní výkon bitcoinové sítě – počet zapojených výpočetních zařízení do bitcoinové sítě odpovídá samotné výnosnosti této činnosti, která je ovlivněna aktuální cenou za 1 bitcoin, odměnou za 1 blok a počtem těžařů v systému, tedy dostupným výpočetním výkonem.
- .FGI – komunitní indexy, jako je například tento, jsou stále více populární a překvapivě dobře dokážou odhadnout náladu na trhu, která má přímý vliv na cenový vývoj Bitcoinu.
- .SPX – nejvýraznější udavatel trendu pro ostatní trhy, protože díky širokému pokrytí velkého množství amerických podniků ukazuje náladu na trhu.

#### 8.1.1 Fear & Greed Index

Fear & Greed Index (přeloženo jako index strachu a chamtivosti) je komunitní index, který zkoumá náladu na trhu, aktuálně pouze pro kryptoměnu Bitcoin. Má bodovou škálu od 0 do 100, přičemž 0 znamená extreme fear (přeloženo jako extrémní strach) a naopak 100 extreme greed (přeloženo jako extrémní chamtivost). Extrémní strach může být známkou toho, že se

investoři bojí situace na trhu, což by mohla být dobrá příležitost k nákupu. Na druhou stranu, když jsou investoři příliš chamtiví, tak to může znamenat, že brzy proběhne cenová korekce trhu. Index se spočítá z několika hodnotících složek podle příslušných vah: cenová volatilita (25 %), moment hybnosti a zobchodované objemy (25 %), sociální média (15 %), dotazníkové průzkumy (15 %), dominance Bitcoinu (10 %) a trendy (10 %).

Vysvětlení hodnotících kategorií:

- cenová volatilita – vezmou se průměry za 30 a 90 dní, které se porovnají s aktuální volatilitou a stanoví se známka podle interní škály.
- moment hybnosti a zobchodované objemy – není přesně známo, které momenty hybnosti jsou využívány. U zobchodovaných objemů i momentů hybnosti se opět vezmou průměry za 30 a 90 dní, které jsou následně porovnány s aktuálními hodnotami.
- sociální média – sleduje se aktivita na Redditu a Twitteru. Díky částečně zautomatizované analýze se vyhodnocují počty příspěvků a hashtagů s klíčovými slovy.
- dotazníkové průzkumy – na platformě StrawPoll probíhají pravidelná dotazníková šetření pro 2 000 až 3 000 respondentů.
- dominance Bitcoinu – porovnává se dominance Bitcoinu vůči zbytku trhu, tedy altcoinům. Rostoucí dominance altcoinů může znamenat větší spekulativnost na trhu a nedůvěru v Bitcoin. Pokud roste dominance Bitcoinu, tak se upevňuje jeho první místo v žebříčku kryptoměn.
- trendy – používají se standardně Google Trends, kde se sleduje hned několik metrik (Krambs 2022).

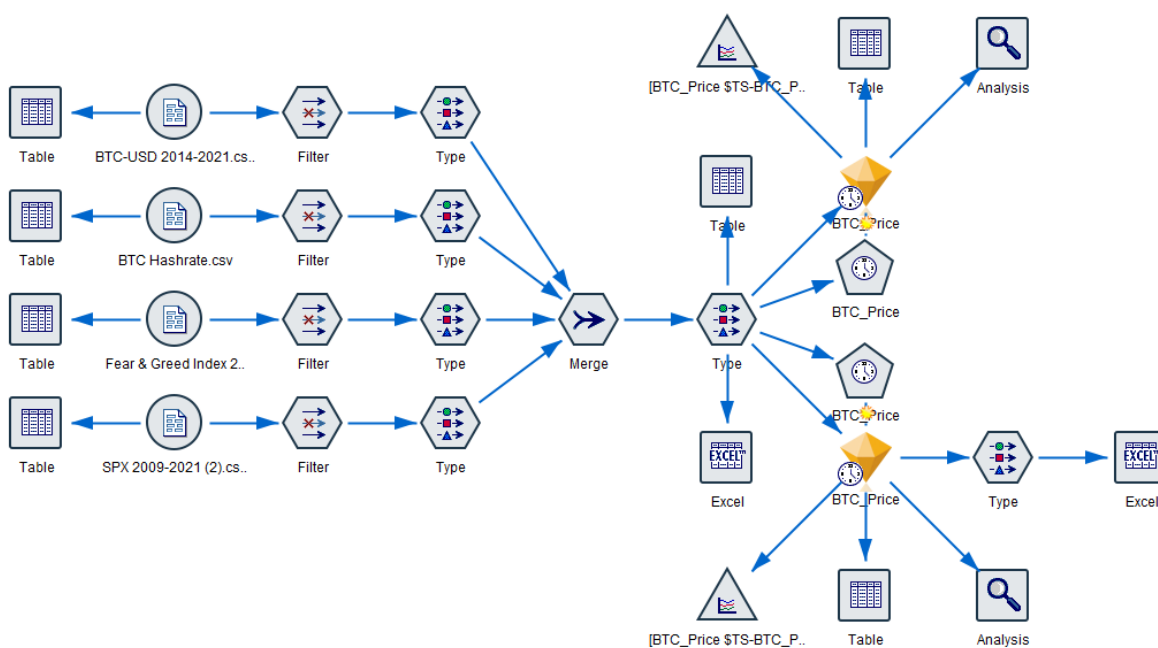
### 8.1.2 Vstupní data a model

Data o tržní ceně Bitcoinu, zobchodovaných peněžních objemech za bitcoiny a indexu S&P 500 byly staženy z analytického portálu Stooq, který je nashromáždil z příslušných burz – samozřejmě zde chybí údaje z víkendů a ze svátků, protože v tyto dny jsou burzy zavřené. Data o bitcoinovém hashratu pochází z databanky portálu Nasdaq Data Link. Údaje o komunitním indexu Fear & Greed pochází z API oficiální stránky ukazatele jménem Alternative. Za pomoci programu IBM SPSS Modeler 18.3 byla data sjednocena podle

datumů a po drobných úpravách se ně aplikoval model časových řad. Záznamy začínají dnem 1. 2. 2018 a končí dnem 11. 1. 2022, jenž byl zvolen náhodně a nemá žádný konkrétní význam. Celkem má soubor po veškerých úpravách 993 řádků, tedy 993 dnů s hodnotami výše zmiňovaných indexů a ukazatelů (Tabulka 3).

Tabulka 3 – ukázková vstupní data analýzy časových řad s denními razítky

Date	BTC Price [USD]	BTC Volume [USD/day]	BTC Hashrate [TH/s]	FGI Value	SPX Price [USD]
01.02.2018	9170,54	9959400448	20703948	30	2821,98
02.02.2018	8830,75	12726899712	21739145	15	2762,13
05.02.2018	6955,27	9285289984	23938940	11	2648,94
06.02.2018	7754,00	13999800320	24293141	8	2695,14



Obrázek 1 – první model časové řady pro tržní cenu Bitcoinu

Na schématu (Obrázek 1) jsou vidět všechny použité uzly, jež posloužily k vytvoření výsledného modelu časové řady.

Popis jednotlivých kroků ve schématu:

- 1) Datové balíčky ve formátu .csv jsou přidány do modelu uzlem „Var. File“.
- 2) Záznamy projdou základní kontrolou uzlem „Table“.
- 3) Zbytečné sloupce jsou vyřazeny uzlem „Filter“.

- 4) Vybraným sloupcům je nastaven správný typ uzlem „Type“.
- 5) Data jsou sjednocena uzlem „Merge“ podle klíče „Date“.
- 6) Sloupcům výsledné datové struktury je opět nastaven správný typ uzlem „Type“.
- 7) Datový balíček je vyexportován uzlem „Excel“ pro další účely.
- 8) Na data je aplikována predikce budoucích hodnot uzlem „Time Series“ pro dobu 30 dní v první části a 7 dní v části druhé.
- 9) Výsledky jsou vyhodnoceny uzly „Table“, „Multiplot“ a „Analysis“.
- 10) Všechna data jsou znovu přetypována uzlem „Type“ a exportována uzlem „Excel“.

### 8.1.3 Výstupní data a graf

Model vytvořil nové sloupce, ve kterých se podle zadaných pravidel uzlu „Time Series“ nachází hodnoty predikce pro dalších 30 dní v první části a 7 dní v části druhé (Tabulka 4).

Popis nově vzniklých sloupců v datovém souboru:

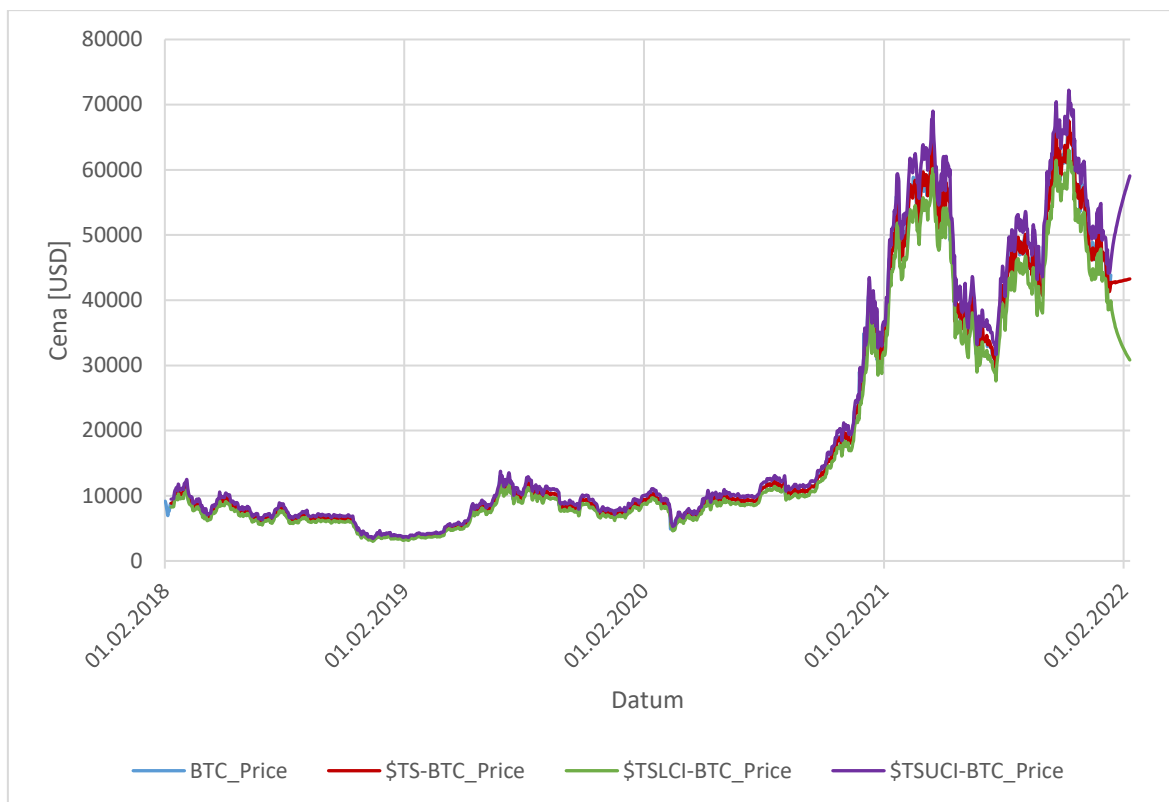
- \$TS-BTC\_Price – vygenerovaná data modelu pro každý sloupec původních dat.
- \$TSLCI-BTC\_Price – hodnota nižšího intervalu spolehlivosti pro každý sloupec generovaných dat modelu.
- \$TSUCI-BTC\_Price – hodnota horního intervalu spolehlivosti pro každý sloupec generovaných dat modelu.
- \$FutureFlag – hodnota typu true (1) a false (0), jež označuje status predikce.

Model automaticky naváže na poslední datum v datovém balíčku a od následujícího datumu aktivuje status predikce hodnotou true (1) indikátorem \$FutureFlag.

Tabulka 4 – výstupní data predikce časové řady pro tržní cenu Bitcoinu

Date	\$FutureFlag	\$TS-BTC_Price [USD]	\$TSLCI-BTC_Price [USD]	\$TSUCI-BTC_Price [USD]
12.01.2022	1	42736,50459	39896,97905	45722,90471
13.01.2022	1	42641,80021	38924,76291	46615,23550
14.01.2022	1	42658,55606	38243,50439	47439,96781
15.01.2022	1	42738,87273	37724,14502	48230,68762

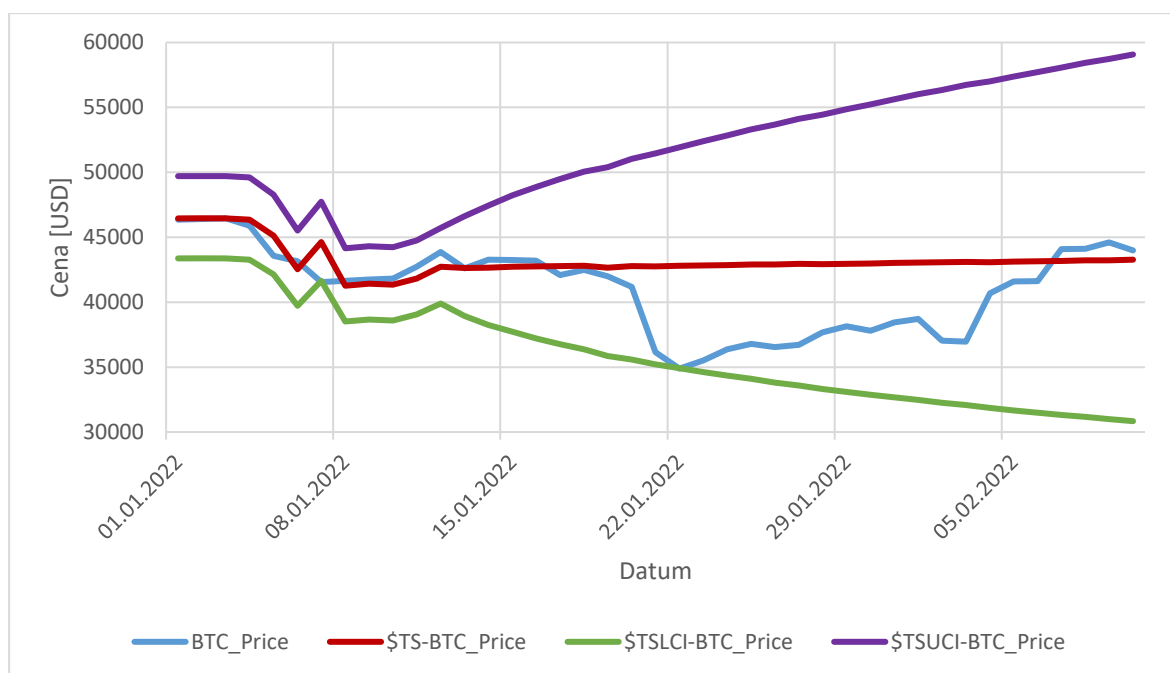




Graf 3 – výsledný graf časové řady pro tržní cenu Bitcoinu

Graf (Graf 3) ukazuje průběh tržní ceny Bitcoinu spolu s třemi stupni predikce dle principů časových řad. Na ose x jsou dny a na ose y jsou ceny v americkém dolaru. Jak je vidět na grafu, predikce je zde opravdu obtížná a v rámci výsledku dost nepřesná. Bylo by vhodné pro další modelování implementovat více ukazatelů. Avšak je již dopředu jasné, že predikce nebude nikdy dokonalá, protože na tržní cenu aktiva má vliv příliš mnoho externích vlivů. Kdyby bylo natolik snadné predikovat ceny aktiv v daném časovém horizontu, tak by každý na svých investicích musel profitovat.

Čeho je dobré si všimnout je, že model vytvořil tři scénáře chování ceny. \$TS-BTC\_Price (červená křivka) je nejvíce konzervativní a odhaduje jen malý pád ceny, nebo také v tomto případě zjevnou konsolidaci trhu. \$TSLCI-BTC\_Price (zelená křivka) je naopak skeptický a predikuje poměrně výrazný cenový pád. Nejpozitivnější je \$TSUCI-BTC\_Price (fialová křivka), který cenu posílá nahoru. Tímto stylem se vytvoří takzvaný predikční koridor.



Graf 4 – graf průběhu predikce po dobu 30 dní oproti realitě

Na grafu (Graf 4) je vidět detail predikce pro 30 dní. Od 1. 1. 2022 do 11. 1. 2022 jsou data předem stanovena a vychází z modelu časových řad. Od 12. 1. 2022 začíná predikce až do 10. 2. 2022 a reálná data jsou doplněna po samotné analýze pro porovnání. Čára BTC\_Price představuje reálnou tržní cenu z burzovních dat, \$TS-BTC\_Price je hlavní predikční linie a \$TSLCI-BTC\_Price spolu s \$TSUCI-BTC\_Price vytváří predikční koridor. Zde je možné pozorovat, že se realita (modrá křivka) odchýlila směrem dolů a dotkla se dolní hrany koridoru. Následně začala opět stoupat k predikčnímu kanálu a zakončuje měsíční odhad téměř totožně s hodnotami modelu časové řady. Nutno podotknout, že se může jednat o náhodu. Ovšem není možné tuto domněnku ověřit, protože vytvářet odhad pro dobu delší než 30 dnů je zavádějící a nepřesné kvůli množství dostupných dat.

Výsledky základní analýzy časové řady pro tržní cenu Bitcoinu a porovnání predikce s realitou:

Tabulka 5 – výstupní analýza modelu časové řady pro tržní cenu Bitcoinu

Minimální chyba (Minimum Error):	-6 868,787
Maximální chyba (Maximum Error):	5 212,646
Střední chyba (Mean Error):	14,701
Střední absolutní chyba (Mean Absolute Error):	474,806
Standardní odchylka (Standard Deviation):	921,930
Lineární korelace (Linear Correlation):	0,999
Výskyty (Occurrences):	1 471

Tato tabulka (Tabulka 5) ukazuje všechny údaje o chybách a odchylkách modelu od možné reality. Díky tomu, že byla reálná data známá již v době zpracovávání analýzy, tak je možné porovnat výsledky s realitou. Cenová predikce modelu končí datem 10. 2. 2022 a cena za 1 bitcoin byla v té době v rozmezí od \$43 239,05 do \$45 861,19. Nejbližše těmto hodnotám je červená křivka \$TS-BTC\_Price s predikcí \$43 273,51. Modrá křivka \$TSLCI-BTC\_Price tipovala \$30 839,65 a zelená křivka \$TSUCI-BTC\_Price odhadovala \$59 076,21.

V druhém pokusu analýzy je testována predikce pro 7 dní. Model je naprosto totožný, pouze se změnilo nastavení uzlu pro délku predikce. Cílem je porovnat, jestli se model v menším časovém horizontu chová přesněji.



Graf 5 – graf průběhu predikce po dobu 7 dní oproti realitě

Na grafu (Graf 5) je vidět detail predikce pro 7 dní. Od 1. 1. 2022 do 11. 1. 2022 jsou data předem stanovena a vychází z modelu časových řad. Od 12. 1. 2022 začíná predikce až do 18. 1. 2022 a reálná data jsou doplněna po samotné analýze pro porovnání. Čára BTC\_Price opět představuje reálnou tržní cenu, \$TS-BTC\_Price je hlavní predikční linie a \$TSLCI-BTC\_Price spolu s \$TSUCI-BTC\_Price vytváří predikční koridor. Jak je možné vidět, realita se od hlavní predikce příliš neliší. Obě čáry se téměř kopírují a potvrzují stejný trend konsolidace. Aplikovaný uzel pro základní analýzu hlásí stejná data, protože se jedná o stejný model, jen predikce je výrazně kratší. Z výsledků je možné usuzovat, že model časové řady je více reprezentativní pro kratší časový horizont. Výstupem je střední trend, horní hranice (maximum) a dolní hranice (minimum). Tyto údaje mohou investorovi přiblížit chování daného aktiva v krátkém horizontu. Ovšem nikdy nedokážou přesně určit tržní cenu aktiva pro stanovený výhled.

## 8.2 Druhá analýza časových řad

Tento model využívá dat technické analýzy, které si autor sám spočítal. Vytvořená datová matice s ukazateli SMA(100), EMA(100), RSI(14) a MACD je vstupem predikčního modelu časové řady, jenž si dává za cíl odhadnout budoucí tržní cenu za 1 bitcoin. Zvoleným predikovaným obdobím je opětovně 1 týden (7 dní) a 1 měsíc (30 dní).

### 8.2.1 SMA(100) a EMA(100)

SMA (klouzavý průměr) a EMA (exponenciální klouzavý průměr) jsou nejzákladnější ukazatele technické analýzy. Byl zvolen střednědobý až dlouhodobý interval pro výpočet indikátoru. V tomto případě je to 100 dní, protože použitý datový balíček obsahuje velké množství dat, díky čemuž se nabízí použít větší interval. Sice pak ukazatel reaguje pomaleji na velké cenové výkyvy, ale je dlouhodobě reprezentativnější. Vstupní data jsou obsažena v souboru .csv, kde se nachází celkem 4 197 záznamů se sloupci: datum (date), tržní cena (price), otevírací cena trhu (open), denní maximum (high), denní minimum (low), zobchodované peněžní objemy za den (volume) a procentuální změna oproti předchozímu dni (change). Z toho jsou reálně použité jen některé sloupce. Data pochází z analytického portálu Stooq.

SMA(100) se spočítá jednoduše, je to vlastně průměr tržních hodnot za 100 dní. Tento vzorec se aplikuje pro celý datový soubor (10):

$x_n$  = tržní hodnota

$n$  = interval hodnot pro výpočet = 100 dní

$$SMA(n) = \frac{(x_1 + x_2 + \dots + x_n)}{n} \quad (10)$$

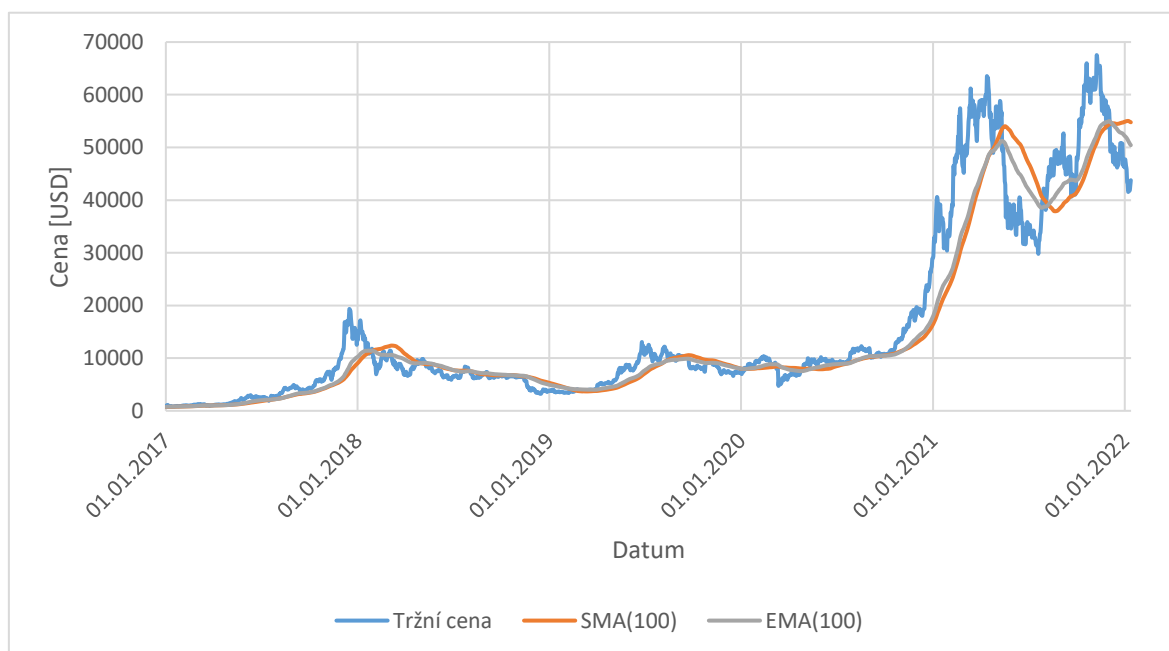
EMA(100) má dva způsoby výpočtu, základní a rozšířenou verzi. V tomto případě se použije základní verze. Opět je tento vzorec aplikován pro celý datový soubor (11):

$$EMA(n) = (\text{tržní cena} - \text{předchozí EMA}(n)) \times \frac{2}{n + 1} + \text{předchozí EMA}(n) \quad (11)$$

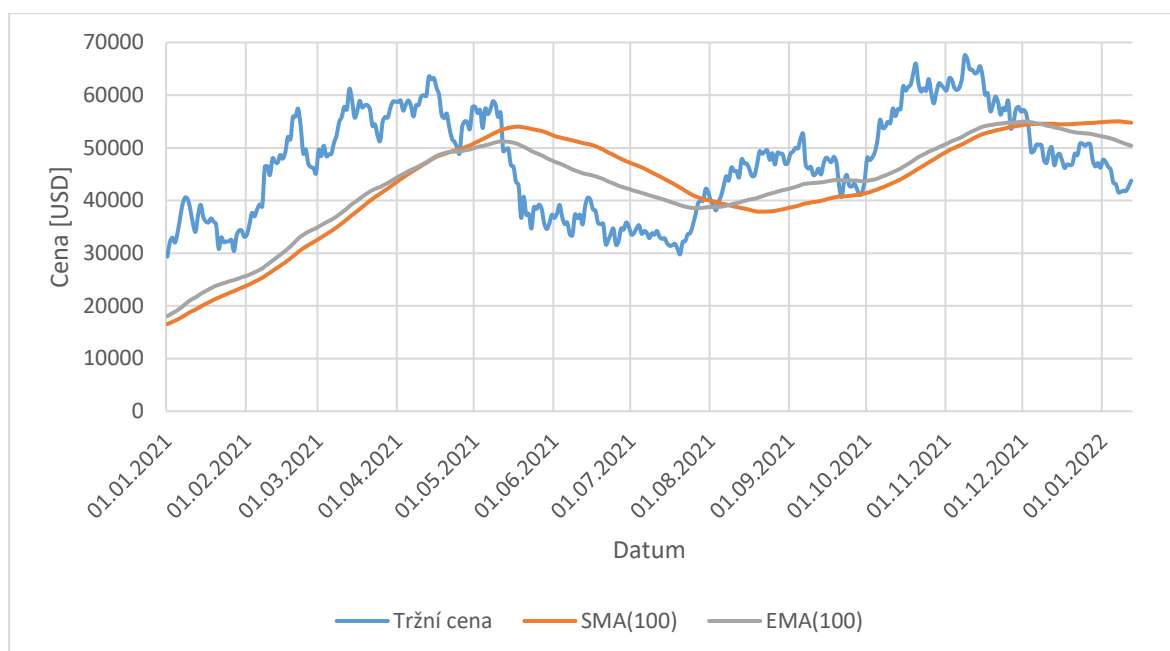
V následující tabulce (Tabulka 6) jsou ukázková vstupní a výstupní data, která jsou vložena do grafů (Graf 6 a Graf 7) s bitcoinovým vývojem v čase.

Tabulka 6 – ukázka vstupních dat, SMA a EMA pro časovou řadu tržní ceny Bitcoinu

Date	Price [USD]	SMA(100)	EMA(100)
12.01.2022	43775,30	54774,27	50425,77
11.01.2022	42733,20	54828,79	50560,12
10.01.2022	41832,20	54883,46	50718,24
09.01.2022	41848,30	54941,80	50897,76



Graf 6 – tržní cena Bitcoinu, SMA(100) a EMA(100)



Graf 7 – tržní cena Bitcoinu, SMA(100) a EMA(100) v detailu za rok 2021

## 8.2.2 RSI(14)

RSI (index relativní síly) patří mezi pokročilejší ukazatele, podle kterého se často dělají investorská rozhodnutí, zatímco SMA a EMA se používají spíše pro účely pozorování trhu. Pro výpočet RSI je potřeba několik mezivýpočtů. Nejprve je tedy klíčové zjistit takzvaný pohyb nahoru a pohyb dolů. Tyto dva nově vzniklé sloupce reprezentují absolutní hodnotu, o kterou se tržní cena aktiva změnila od předchozího dne. Pokud se tržní cena změnila v opačném směru, tak je na místě výsledku hodnota 0 a výsledný rozdíl se projeví ve druhém sloupci a obráceně. K těmto sloupcům se pak vytvoří další dva sloupce, které nesou názvy průměrný pohyb nahoru a průměrný pohyb dolů. Oba v tomto případě berou průměr za posledních 14 dní z předchozích nově přidaných sloupců. Interval 14 dnů je běžně používaná hodnota pro tento typ ukazatele. Podíl sloupce Average Upward Movement (průměrný pohyb nahoru) a Average Downward Movement (průměrný pohyb dolů) je RSI index.

Následná hodnota RSI(14) se spočítá tímto způsobem (12):

$n = \text{interval hodnot pro výpočet} = 14 \text{ dní}$

$$RSI(n) = 100 - \frac{100}{RSI \text{ index} + 1} \quad (12)$$

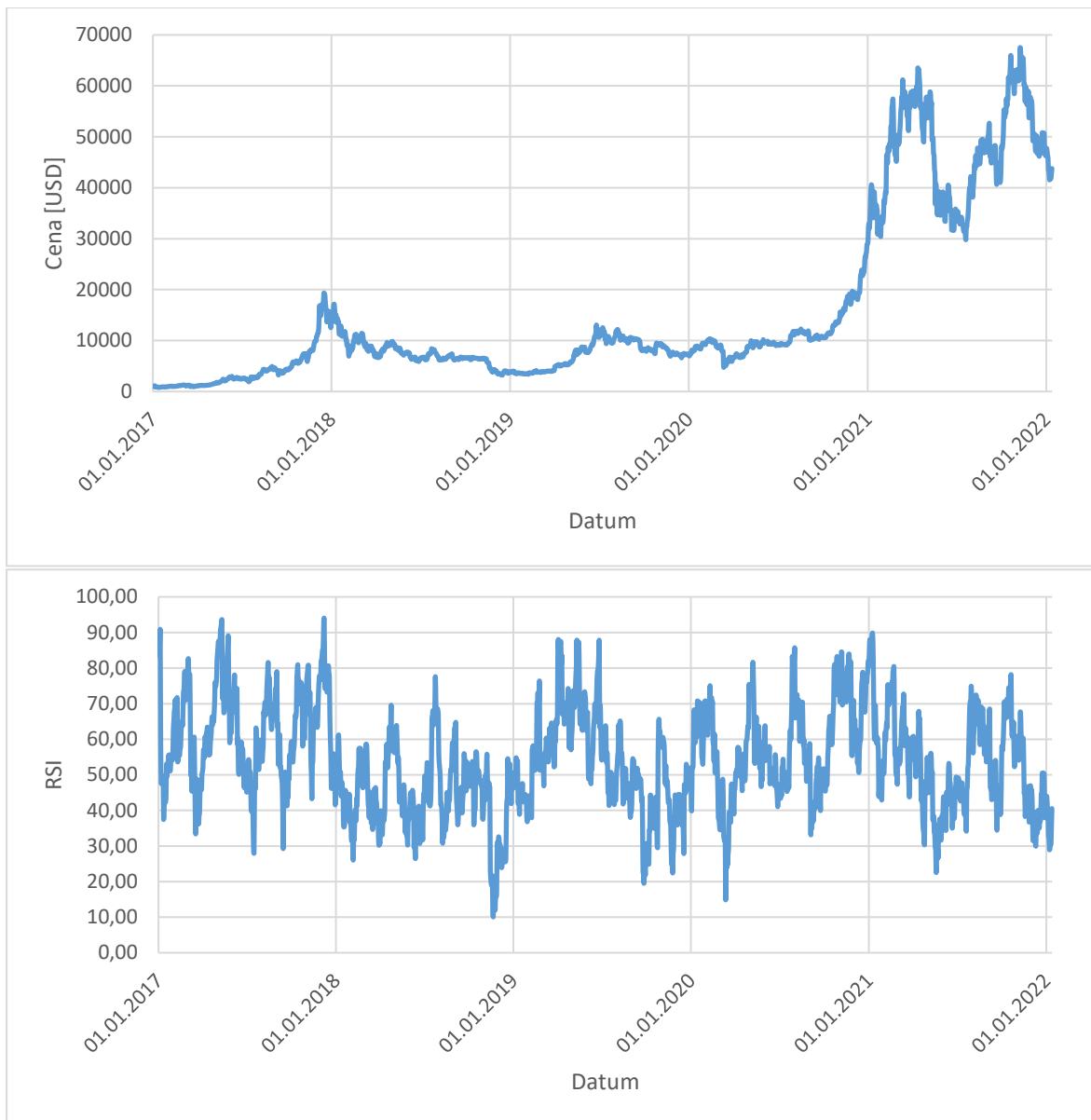
V následujících tabulkách (Tabulka 7 a Tabulka 8) jsou ukázková vstupní a výstupní data, která jsou vložena do dvojice spojených grafů (Graf 8 a Graf 9).

*Tabulka 7 – ukázka vstupních dat a RSI pro časovou řadu tržní ceny Bitcoinu*

<b>Price [USD]</b>	<b>Change [USD]</b>	<b>Upward Movement</b>	<b>Downward Movement</b>
43775,30	1042,10	1042,10	0,00
42733,20	901,00	901,00	0,00
41832,20	-16,10	0,00	16,10
41848,30	176,30	176,30	0,00

*Tabulka 8 – ukázka vstupních dat a RSI pro časovou řadu tržní ceny Bitcoinu*

<b>Average Upward Movement</b>	<b>Average Downward Movement</b>	<b>Relative Strength</b>	<b>RSI</b>
374,0388	549,0594	0,6812	40,5199
322,6495	591,2947	0,5457	35,3030
278,1610	636,7789	0,4368	30,4021
299,5580	684,5234	0,4376	30,4404



*Graf 8 – tržní cena Bitcoinu a RSI*





Graf 9 – tržní cena Bitcoinu a RSI v detailu za rok 2021

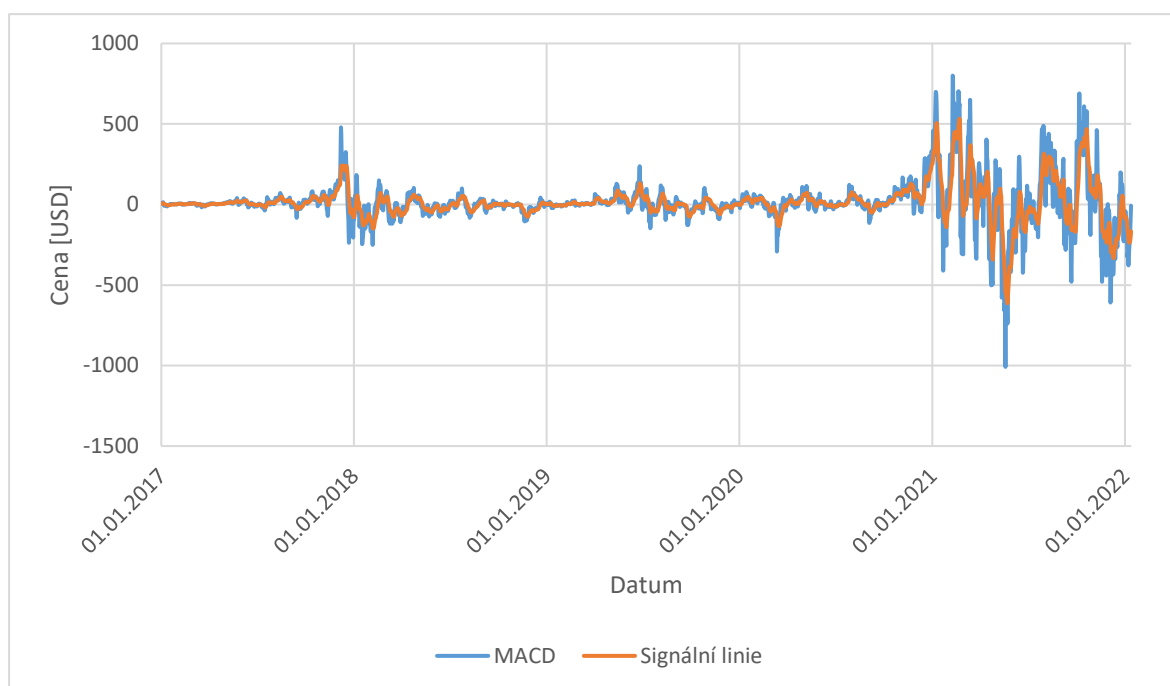
### 8.2.3 MACD

MACD (klouzavý průměr konvergence a divergence) je technický ukazatel, který dává investorovi signál, kdy vstupovat na trh, nebo kdy likvidovat svou pozici. Prvotně je nutné si spočítat EMA(12) a EMA(26), přičemž postup výpočtu je zmíněný výše u SMA(100) a EMA(100). Ovšem v tomto případě se pracuje s odlišným počtem dní, tedy 12 dní a 26 dní podle pravidel tohoto indikátoru. Rozdíl těchto dvou hodnot je pak MACD index. K této hodnotě se musí ještě dopočítat signální linie, která je reprezentována EMA(9) a každé protnutí těchto dvou čar je signál k akci (nákup či prodej) investorovi.

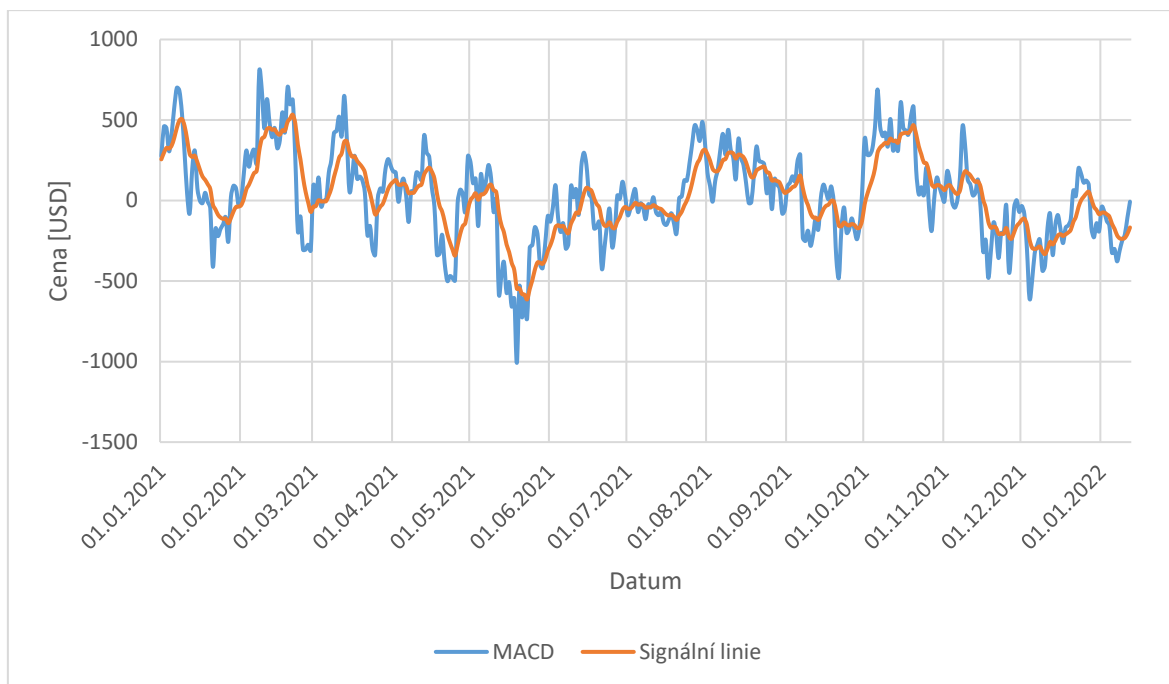
V následující tabulce (Tabulka 9) jsou ukázková vstupní a výstupní data, která jsou vložena do grafů (Graf 10 a Graf 11).

Tabulka 9 – ukázka vstupních dat a MACD pro časovou řadu tržní ceny Bitcoinu

Price [USD]	EMA(12)	EMA(26)	MACD	Signal
43775,30	43852,28	43859,54	-7,26	-167,14
42733,20	43866,28	43973,10	-106,82	-207,11
41832,20	44072,30	44283,48	-211,19	-232,19
41848,30	44479,59	44727,65	-248,07	-237,44



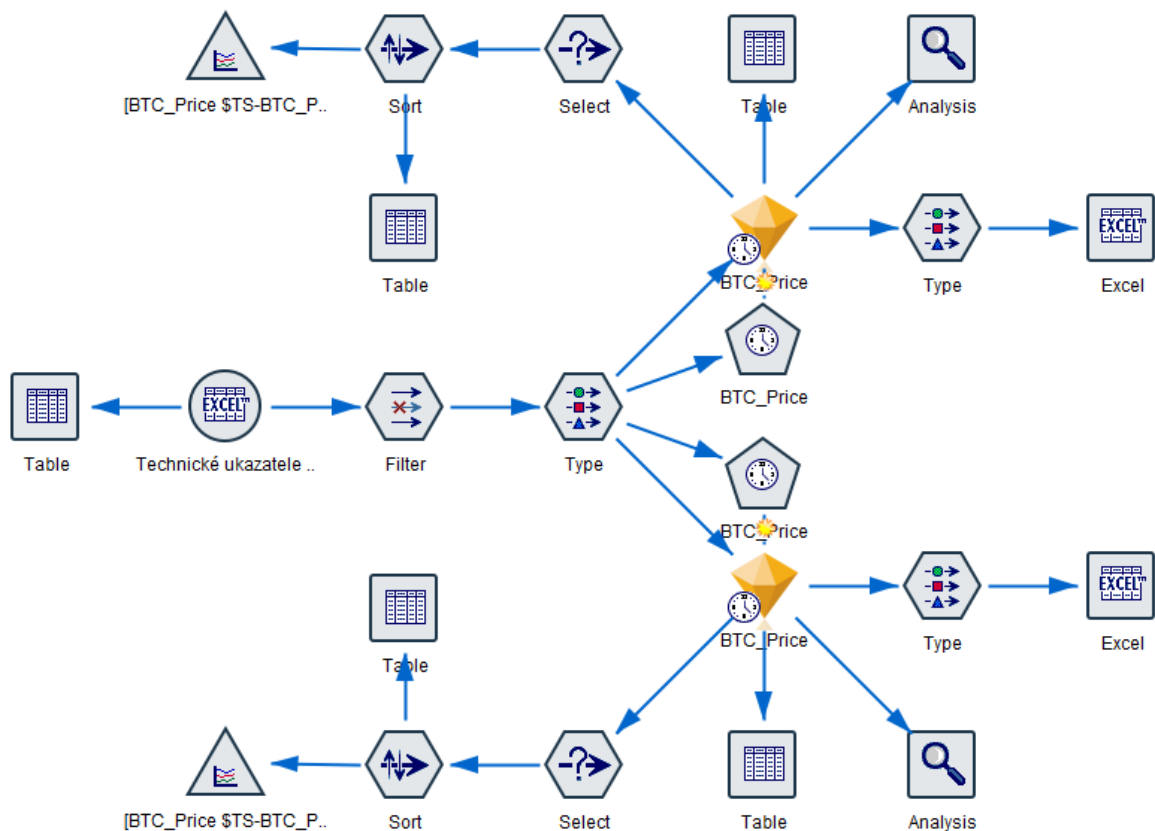
Graf 10 – MACD index a signální linie



Graf 11 – MACD index a signální linie v detailu za rok 2021

#### 8.2.4 Vstupní data a model

Data o tržní ceně Bitcoinu opět pochází z analytického portálu Stooq, který je nashromáždil z burz dle stejných pravidel jako u předešlé analýzy. Za pomoci programu IBM SPSS Modeler 18.3 byla data upravena pro model časových řad. Záznamy začínají dnem 18. 7. 2010 a končí dnem 12. 1. 2022, jenž byl zvolen náhodně a nemá žádný konkrétní význam. Celkem má soubor 4 197 řádků, tedy 4 197 dnů s hodnotami výše zmiňovaných technických ukazatelů.



Obrázek 2 – druhý model časové řady pro tržní cenu Bitcoinu

Na schématu (Obrázek 2) jsou vidět všechny použité uzly, jež posloužily k vytvoření výsledného modelu časové řady. Lehce se liší od předchozí analýzy, protože data již byla předpřipravená v dokumentu typu Excel. Většinu příslušných ukazatelů jakožto testovaných dat zde bylo nejprve nutné spočítat.

Popis jednotlivých kroků ve schématu:

- 1) Dokument ve formátu .xlsx je přidán do modelu uzlem „Excel“.
- 2) Záznamy projdou základní kontrolou uzlem „Table“.
- 3) Zbytečné sloupce jsou vyřazeny uzlem „Filter“.
- 4) Vybraným sloupcům je nastaven správný typ uzlem „Type“.
- 5) Na data je aplikována predikce budoucích hodnot uzlem „Time Series“ pro dobu 30 dní a pak také 7 dní.
- 6) Reprezentativní data jsou vybrána uzlem „Select“. Za reprezentativní jsou považovány všechny záznamy od 1. 1. 2016, protože cenový vývoj je do té doby příliš malý a pro měřítko výsledného grafu nepatrný.

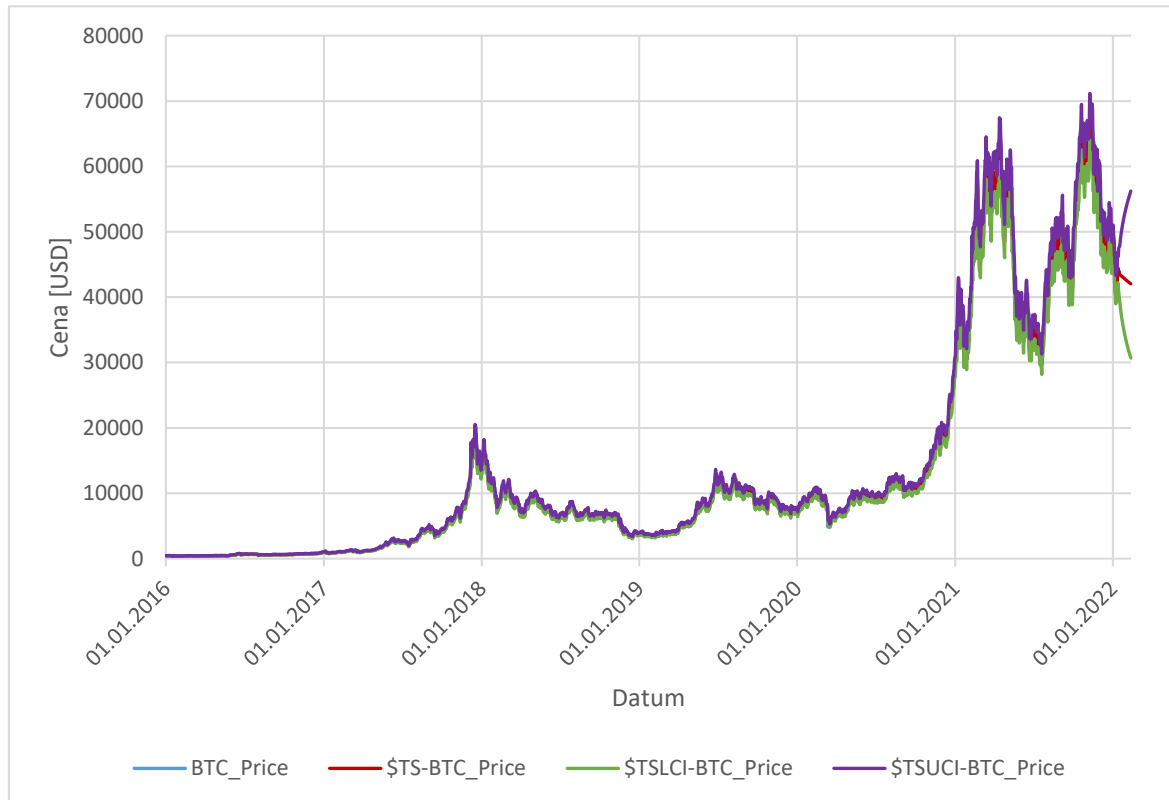
- 7) Použité kritérium:  $Date \geq \text{datetime\_date}(2016,01,01)$ .
- 8) Data jsou seřazena uzlem „Sort“.
- 9) Výsledky jsou vyhodnoceny uzly „Table“, „Multiplot“ a „Analysis“.
- 10) Všechna data jsou znovu přetypována uzlem „Type“ a exportována uzlem „Excel“.

### 8.2.5 Výstupní data a graf

Model časových řad vytvořil stejné sloupce jako u předešlé analýzy (Tabulka 10). Jejich význam je tedy popsán výše.

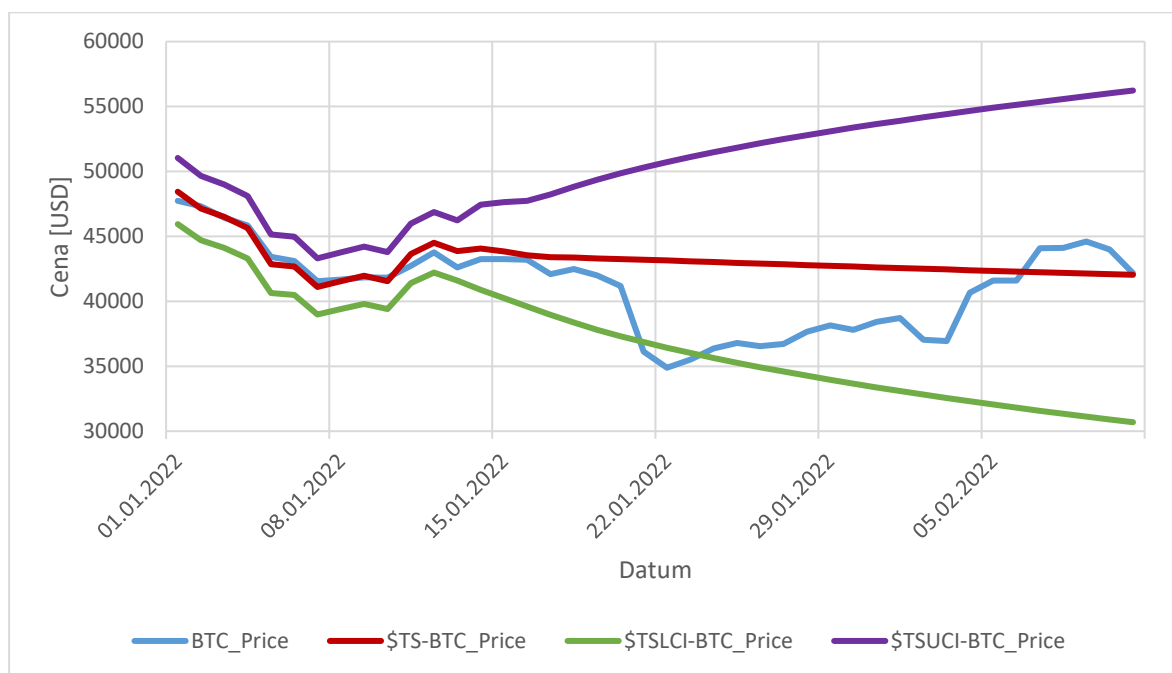
Tabulka 10 – výstupní data predikce časové řady pro tržní cenu Bitcoinu

Date	\$FutureFlag	\$TS-BTC_Price [USD]	\$TSLCI-BTC_Price [USD]	\$TSUCI-BTC_Price [USD]
13.01.2022	1	43871,80194	41609,88733	46223,42218
14.01.2022	1	44065,68731	40878,76950	47432,78915
15.01.2022	1	43833,08451	40248,58214	47648,45810
16.01.2022	1	43537,35203	39612,09244	47743,20851



Graf 12 – výsledný graf časové řady pro tržní cenu Bitcoinu

Tento graf (Graf 13) znázorňuje průběh tržní ceny Bitcoinu spolu s třemi stupni predikce dle principů časových řad, které tvoří predikční koridor. Na ose x jsou dny a na ose y jsou ceny v americkém dolaru. Dolní i horní hranice je méně odchýlená od predikční linie, protože dle analýzy modelu časových řad je tento případ přesnější. To ovšem neznamená, že se na výsledky modelu dá více spolehnout. Je zde stále hodně faktorů, které ovlivňují chování trhu. Tyto ukazatele by bylo možné implementovat i do první analýzy časových řad. Avšak nabízelo se vytvořit porovnání obou balíčků dat – první datový balíček vycházel z korelace trhů a druhý datový balíček sleduje technické ukazatele přímo dané tržní ceny.



Graf 13 – graf průběhu predikce po dobu 30 dní oproti realitě

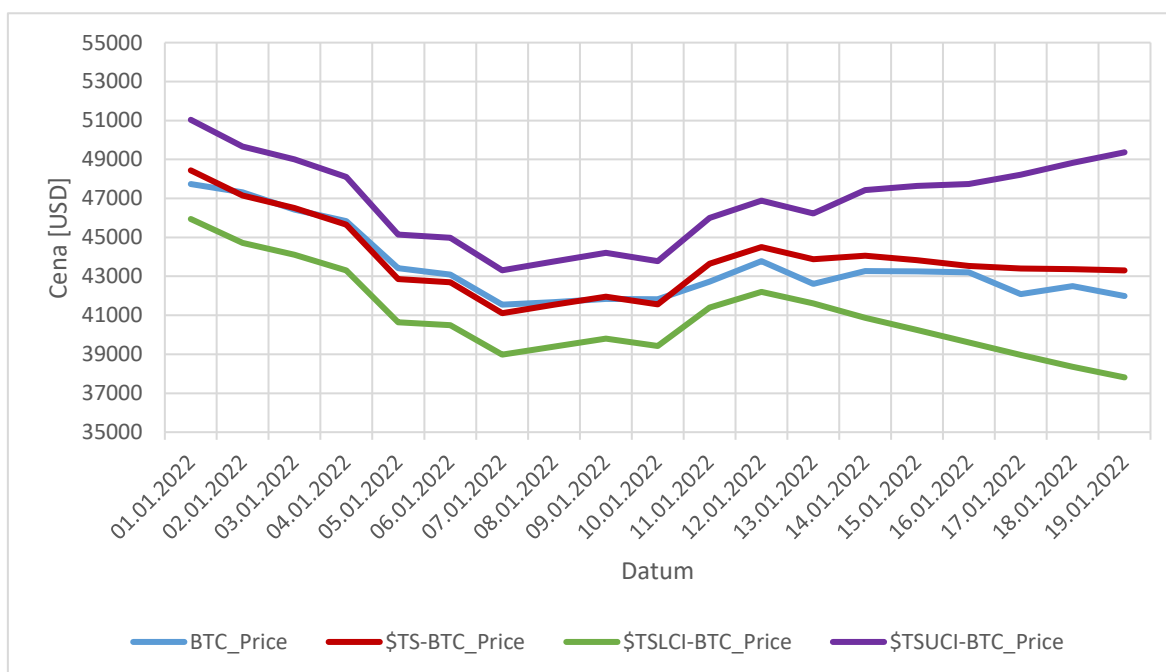
Na grafu (Graf 13) je vidět detail predikce pro 30 dní. Od 1. 1. 2022 do 12. 1. 2022 jsou data předem stanovena a vychází z modelu časových řad. Od 13. 1. 2022 začíná predikce až do 11. 2. 2022 a reálná data jsou doplněna po samotné analýze pro porovnání. Opět je možné pozorovat podobný scénář jako u prvního modelu, kde došlo k dotyku dolního intervalu a následné vrácení hodnoty do predikčního rámce. Ovšem v tomto případě reálný průběh na chvíli spadl pod dolní interval, protože se dle analýzy tento model tváří přesněji, díky čemuž tam nevznikla taková rezerva na případné výkyvy. Je možné pozorovat shodu reality a predikce na konci modelu časových řad jako tomu bylo u prvního případu, jelikož jsou modely postaveny na podobných principech.

Výsledky základní analýzy časové řady pro tržní cenu Bitcoinu a porovnání predikce s realitou (Tabulka 11):

Tabulka 11 – výstupní analýza modelu časové řady pro tržní cenu Bitcoinu

Minimální chyba (Minimum Error):	-2 173,994
Maximální chyba (Maximum Error):	1 152,864
Střední chyba (Mean Error):	-4,969
Střední absolutní chyba (Mean Absolute Error):	44,431
Standardní odchylka (Standard Deviation):	122,859
Lineární korelace (Linear Correlation):	1,0
Výskyty (Occurrences):	4 204

Ve srovnání s analýzou předchozího modelu je možné pozorovat výrazné zlepšení minimální a maximální chyby. To může být způsobené množstvím dostupných dat, protože všechny technické ukazatele lze dopočítat z burzovních údajů. Tento model pracoval s 4 197 řádky oproti 1 471 řádkům v předchozím případě. Na druhou stranu by se dalo očekávat, že technické ukazatele, které se používají poměrně běžně v investorské sféře nebo třeba u automatizovaných obchodních botů, budou fungovat dobře v predikčních modelech, když mají takovou váhu.



Graf 14 – graf průběhu predikce po dobu 7 dní oproti realitě

Na grafu (Graf 14) je vidět detail predikce pro 7 dní. Od 1. 1. 2022 do 12. 1. 2022 jsou data předem stanovena a vychází z modelu časových řad. Od 13. 1. 2022 začíná predikce až do

19. 1. 2022 a reálná data jsou doplněna po samotné analýze pro porovnání. Realita poměrně dobře kopíruje predikční linii jako tomu bylo u první analýzy.

### 8.3 Model Stock to Flow

Stock to Flow je číslo, které ukazuje, kolik let je při současném produkčním tempu zapotřebí k dosažení aktuální zásoby. Matematicky se jedná o poměr mezi existující zásobou (stock) a přítokem (flow) nových jednotek. Čím je číslo vyšší, tedy výsledek, tím je vyšší cena. Tento model však neřeší poptávkovou stranu problému, pouze jeho nabídku. Proto se odhad ceny u Stock to Flow modelu může významně lišit od reálné tržní ceny. Často se používá právě pro odhad ceny za váhovou jednotku zlata a stříbra nebo ceny za 1 bitcoin (PlanB 2019).

Model Stock to Flow u Bitcoinu je velmi populární, protože spekulativně predikuje tržní cenu za 1 bitcoin v dlouhém časovém horizontu, což je pro amatérského investora minimálně zajímavá informace. V tomto případě dává obzvlášť smysl jej použít, protože Bitcoin má jasně stanovenou inflační křivku. Ta mohla vzniknout jen díky jasně stanoveným pravidlům v samotném kódu kryptoměny, kde je také popsáno, v jakém množství budou mince distribuovány těžařům. Odměna za vytěžený blok je pevně daná a každé 4 roky dochází k jejímu snížení o polovinu. Tomuto procesu a dnu, ve kterém k rozpůlení odměny dojde, se říká halving (takzvané půlení).

Právě díky těmto faktům se nabízelo takový model vytvořit. Poprvé s ním přišel uživatel, který si přezdívá Plan B. Ten s touto myšlenkou přišel v březnu 2019, kdy na svém Twitteru zveřejnil článek popisující tento model a obhajoval jeho pravdivost. Poukázal na to, že ukazatel silně koreluje s celkovou tržní kapitalizací Bitcoinu, a tím pádem je snadné na něj navázat určité predikční modely jako je Stock to Flow.

Spousta analytiků se tento model snažila vyvrátit. Častými argumenty jsou, že Bitcoin je dostatečně otevřený a má velkou likvidnost. Většina veřejných informací je tedy rychle obsažena v jeho aktuální tržní ceně. Nebo se také opakovaně objevuje kritika na poptávkovou stranu trhu, kterou Stock to Flow nezohledňuje, což je vidět hned na několika dalších kryptoměnách. Sám Plan B prohlásil, že pokud tržní cena nedosáhne na \$100 000 do konce roku 2021, tak bude jeho model zneplatněn. Shodou nepříznivých okolností jako je například pandemie COVID-19 a celosvětová krize obecně většiny trhů se jeho prognóza nenaplnila a Bitcoin si na svých \$100 000 ještě musí počkat. Ovšem je zde stále naděje, že



tržní cena Bitcoinu alespoň dosáhne na průměrnou hodnotu predikce v modelu ve 4. cyklu (Tětek 2020).

### 8.3.1 Vstupní data

Na jeden cyklus v Bitcoinu, který je dlouhý přibližně 4 roky, připadá zhruba 210 000 bloků, což je asi 144 bloků denně. Tato čísla poslouží jako základ pro bitcoinový model Stock to Flow.

Pro sestavení modelu je nutné znát zásobu bitcoinů a přítok nových bitcoinů do systému. Maximální zásoba je daná samotným bitcoinovým kódem, kde je hodnota 21 000 000 BTC pevně ukotvená. Avšak přítok se musel spočítat, protože každé 4 roky (1 bitcoinový cyklus) se změní na základě odměny za 1 blok. Naštěstí jsou známé přesné dny, kdy došlo ke změnám odměny za blok v minulosti a k tomuto období se jednoduchou matematikou zjistí roční odměna. Počet emitovaných bitcoinů za 10 minut v daném období je pevně stanovený, tato částka se vynásobí 6 (hodinový přítok), pak 24 (denní přítok) a na závěr 365,25 (roční přítok včetně přechodového roku).

Dále je potřeba si uvědomit, že očekávaná délka bloku versus reálná délka bloku se může častokrát lišit. V praxi to funguje tak, že si sama bitcoinová síť určuje složitost algoritmu na základě dostupného výkonu. Podle tohoto výkonu je poměrně snadné zjistit, za jak dlouho dojde k uhodnutí čísla, kterým se uzavře blok, a ten se zdárně připojí do blockchainu. Cílem je, aby to trvalo přesně 10 minut. Po tuto dobu se pálí elektrická energie a těžební stroje se snaží požadované číslo najít. Ovšem zde nastává ten problém, dostupný výkon v síti je proměnlivý a k přepočítání potřebné náročnosti algoritmu dochází jednou za 14 dní. Proměnlivost výkonu je naprosto běžný jev, protože je udáván veškerou výpočetní silou v celé síti a mění se připojováním a odpojováním těžebních strojů.

Základní údaje:

- celková zásoba – 21 000 000 BTC (zhruba 1 000 000 BTC zamčených autorem Satoshi Nakamotoem, práce uvažuje včetně těchto „ztracených mincí“).
- průměrná délka bloku – 10 minut (každých 14 dní dochází k úpravě složitosti algoritmu, aby délka bloku odpovídala 10 minutám podle dostupného výkonu v síti).

Odměny za 1 blok podle cyklů:

- 1. cyklus (3. 1. 2009 – 29. 11. 2013) – 50 BTC za 10 minut (zhruba 2 629 800 BTC za rok).
- 2. cyklus (29. 11. 2013 – 16. 12. 2017) – 25 BTC za 10 minut (zhruba 1 314 900 BTC za rok).
- 3. cyklus (16. 12. 2017 – 10. 12. 2021) – 12,5 BTC za 10 minut (zhruba 657 450 BTC za rok).
- 4. cyklus (10. 12. 2021 – ~2024) – 6,25 BTC za 10 minut (zhruba 328 725 BTC za rok).

Zde je možné vidět, že 1 bitcoinový cyklus netrvá přesně 4 roky, ale pouze se k této hodnotě blíží. Samozřejmě záleží na tom, jak velká proměnlivost výkonu v síti byla. Pro přehlednost modelu se pracuje s délkou jednoho roku upravenou o přechodný rok.

Počet vytěžených bitcoinů za 1 rok ve 4. cyklu:

- 6,25 BTC za 10 minut (stanovená odměna za 1 blok ve 4. cyklu).
- 37,5 BTC za hodinu (vynásobeno 6x).
- 900 BTC za den (vynásobeno 24x).
- 328 725 BTC za rok (vynásobeno 365,25x).

### 8.3.2 Základní vzorce

Zde je ukázkové dosazení do dvou základních vzorců s průběžným vysvětlením. Používané hodnoty byly zaokrouhleny na vhodný řád pro zřetelnější ukázkou výpočtu (13):

$$\text{Flow} = 328\,725 = \sim 330\,000 \text{ (přítok nových bitcoinů za 1 rok ve 4. cyklu)}$$

$$\text{Stock} = \sim 18\,800\,000 \text{ (dostupná zásoba bitcoinů v systému na konci roku 2021)}$$

$$\text{Stock to Flow Ratio [years]} = \frac{\text{stock}}{\text{flow}} = \frac{18\,800\,000}{330\,000} = \sim 57 \text{ let} \quad (13)$$

Výsledná hodnota 57 let odpovídá počtu roků při aktuální zásobě a přítoku, který je potřebný pro úplné vyčerpání maximální zásoby bitcoinů. Tedy v tomto případě to znamená, že s aktuálními daty by trvalo vytěžit všechny bitcoinové mince zhruba 57 let. Ovšem to není

pravda, protože každé 4 roky se tato hodnota zvětší, jelikož se odměna za 1 blok zmenší podle vnitřní filosofie Bitcoinu, která mu byla takto nastavena.

$$\begin{aligned} \text{Stock to Flow Model Price [USD]} &= e^{-1,84} \times \text{SF}^{3,36} \\ &= e^{-1,84} \times 57^{3,36} = \sim \$126\,096 \end{aligned} \quad (14)$$

Výsledná hodnota \$126 096 znamená odhadovanou cenu modelem Stock to Flow, okolo které by měla oscilovat tržní cena za 1 bitcoin ve 4. cyklu (14). Denní uzavírka 12. 1. 2022 je \$43 860,48. Měsíční uzavírka za leden 2022 je \$38 431,67. Nutno zmínit, že touto dobou byl celý akciový trh a kryptoměnový trh v korekci (Bybit Learn 2021).

### 8.3.3 Popis postupu

Na úvod je nutné podotknout, že některé z uvedených hodnot jsou pouze odhady a neodpovídají přesným číslům. Zpravidla se jedná se o teoretické hodnoty, jež se vůči reálným/praktickým mohou mírně lišit. Nikterak však neznehodnocují ukázkou modelu Stock to Flow v praxi.

K výpočtu posloužila naakumulovaná data z bitcoinové sítě, ve kterých se nachází celkový počet vytěžených bitcoinů k určitému dni včetně svátků a víkendů od 2. 1. 2009 do 11. 1. 2022. Následně se spočítal odhad roční odměny bitcoinů těžařům, tedy roční přítok nových bitcoinů do celého systému. Za pomoci těchto údajů a celkové zásoby bitcoinů uvedené výše se spočítal koeficient SF (Stock to Flow Ratio [years]), což je odhad doby, za kterou se vytěží všechny bitcoiny. Pak už se jen spočítala modelová cena SF (Stock to Flow Model Price [USD]), která se vynesla do grafu oproti reálným uzavřeným cenám bitcoinu za den z historických dat Bitcoinu na burzách a mimo ně. Cenové údaje jsou ode dne 18. 7. 2010, protože do té doby se tokeny Bitcoinu nikde oficiálně neobchodovaly a končí dnem 11. 1. 2022 jako data o vytěžené zásobě. Ukázka použitých vstupních a výstupních dat je vypsána v následujících tabulkách (Tabulka 12 a Tabulka 13).

*Tabulka 12 – ukázková vstupní data tržní ceny za 1 bitcoin v americkém dolaru s denním razítkem*

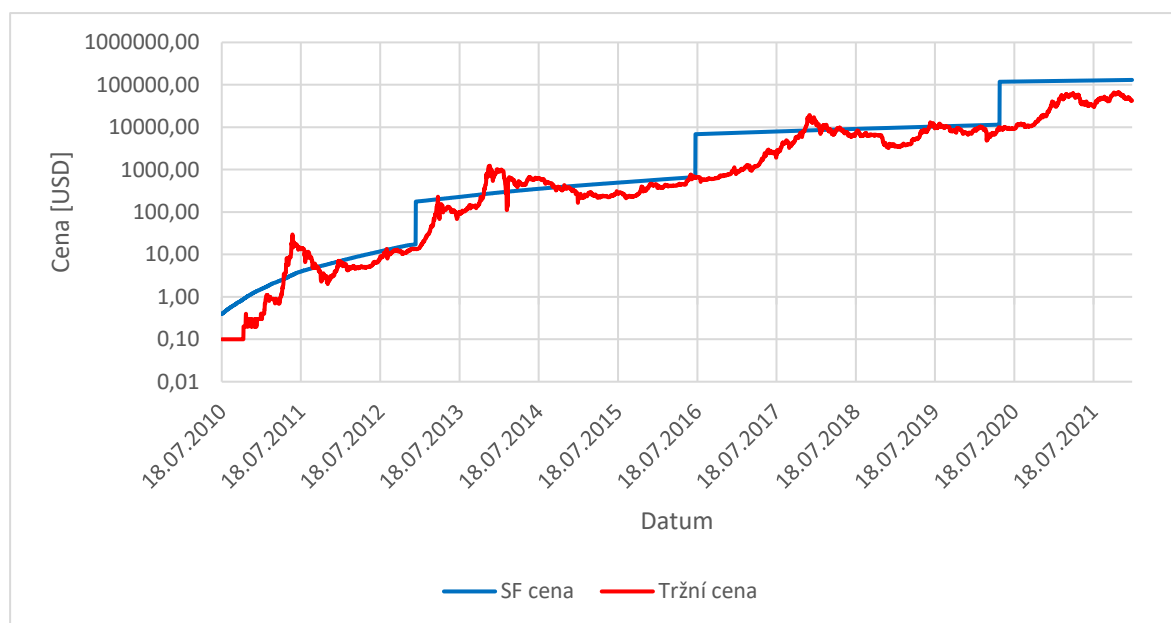
Date	Price [USD]	Open [USD]	High [USD]	Low [USD]	Volume [USD]	Change [%]
11.01.2022	42733,20	41829,10	43090,20	41287,60	6178000,00	2,15 %
10.01.2022	41832,20	41848,90	42243,80	39697,00	8550000,00	-0,04 %
09.01.2022	41848,30	41681,20	42764,40	41260,90	3751000,00	0,42 %
08.01.2022	41672,00	41551,30	42304,40	40574,30	5254000,00	0,30 %

Tabulka 13 – ukázková výstupní data mezivýpočtů potřebných parametrů a samotných výsledků v podobě SF a ceny SF

Date	Amount [BTC]	Reward [Year]	SF [Years]	SF Price [USD]
11.01.2022	18926306,25	328725	57,57489163	130401,16
10.01.2022	18925431,25	328725	57,57222983	130380,91
09.01.2022	18924556,25	328725	57,56956803	130360,66
08.01.2022	18923681,25	328725	57,56690623	130340,40

### 8.3.4 Výstupní graf

Modrá křivka na příslušném grafu (Graf 15) popisuje, jak by se měla tržní cena za 1 bitcoin vyvíjet dle dostupné nabídky na čase na základě modelu Stock to Flow. Červená křivka ukazuje reálnou cenu za 1 bitcoin na čase. Měřítko je záměrně logaritmické, protože lépe ukazuje průběh obou křivek.



Graf 15 – výsledný model Stock to Flow pro Bitcoin

### 8.3.5 Závislost modelu

Model Stock to Flow často slouží pro odhad ceny mnoha aktiv s omezenou zásobou a se stanoveným přítokem do rezervy. Právě u Bitcoinu fungoval podle očekávání zhruba do roku 2021, kdy celosvětová krize ovlivnila jeho cenový vývoj a principiální mezery samotného modelu způsobily, že model Stock to Flow přestal fungovat. Bylo to takřka nevyhnutelné.

Tato analýza zkoumá závislost modelu Stock to Flow a reálnou tržní cenu Bitcoinu. Graf již ukázal jistou podobu a závislost obou veličin, kterou analýza jen potvrzuje. Všechny ukazatele totiž dokazují poměrně silnou korelaci. Ovšem přesnost modelu nadále slábne, čímž závislost obou veličin postupně klesá, jak se predikovaná cena a reálná cena čím dál víc liší.

Model vypočítal Pearsonův korelační koeficient, Spearmanův korelační koeficient a Kendallův koeficient konkordance (Tabulka 14, Tabulka 15 a Tabulka 16).

Pearsonův korelační koeficient  $r = r$  se pohybuje mezi  $-1$  (nepřímá závislost) a  $1$  (přímá závislost).

Spearmanův korelační koeficient  $r = r$  se pohybuje mezi  $-1$  (nepřímá závislost) a  $1$  (přímá závislost).

Kendallův koeficient konkordance  $W = W$  se pohybuje mezi  $0$  (žádná shoda) a  $1$  (úplná shoda).

*Tabulka 14 – Pearsonův korelační koeficient pro SF cenu a tržní cenu BTC*

<b>Pearsonův test</b>	<b>SF Price</b>	<b>BTC Price</b>
<b>SF Price</b>	1,000	0,847
<b>BTC Price</b>	0,847	1,000
<b>n</b>	4 758	4 196

*Tabulka 15 – Spearmanův korelační koeficient pro SF cenu a tržní cenu BTC*

<b>Spearmanův test</b>	<b>SF Price</b>	<b>BTC Price</b>
<b>SF Price</b>	1,000	0,962
<b>BTC Price</b>	0,962	1,000
<b>n</b>	4 758	4 196

*Tabulka 16 – Kendallův koeficient konkordance pro SF cenu a tržní cenu BTC*

<b>Kendallův test</b>	<b>SF Price</b>	<b>BTC Price</b>
<b>SF Price</b>	1,000	0,842
<b>BTC Price</b>	0,842	1,000
<b>n</b>	4 758	4 196

n = počet záznamů

Pearsonův korelační koeficient označil, že tržní cena Bitcoinu má poměrně silnou přímou závislost s predikovanou cenou modelu Stock to Flow.

Kendallův koeficient konkordance udává, že tržní cenu Bitcoinu se silně blíží úplné shodě s cenou modelu Stock to Flow.

A na závěr Spearmanův korelační koeficient označil, že tržní cena Bitcoinu má poměrně silnou přímou závislost s predikovanou cenou modelu Stock to Flow.

Podle všech spočítaných koeficientů je zřejmé, že zde existuje závislost mezi zkoumanými veličinami. Tato analýza tedy potvrzuje, že má model Stock to Flow vcelku slušnou přesnost a lze se jím řídit při odhadu tržní ceny za 1 bitcoin. Ovšem jak je výše zmíněno, v posledních měsících nenaplnuje svoje predikce a velká část kryptoměnové komunity ho dávno zatratila. Důležité bude porovnání reality a predikce na konci bitcoinového cyklu v roce 2024.

## **8.4 Korelační modely**

### **8.4.1 První korelační analýza**

První korelační analýza porovnává cenový vývoj Bitcoinu oproti .DXY (index amerického dolaru), .SPX (index S&P 500, tedy 500 největších obchodovatelných podniků v USA) a .GOLD (index zlata).

Důvody výběru těchto ukazatelů:

- .DXY – často se uvádí, že investoři platící americkým dolarem nakupují cenné papíry a obecně investují v moment, kdy síla amerického dolaru slábne.
- .SPX – nejvýraznější udavatel trendu pro ostatní trhy, protože díky širokému pokrytí velkého množství amerických podniků ukazuje náladu na trhu. Dále se nabízí .DJI neboli Dow Jones Industrial Average (přeloženo jako Dow Jonesův index), jenž obsahuje pouze 30 amerických blue-chip (označení pro největší a nejziskovější společnosti) podniků. Avšak je výrazně menší a nemusí přesně vyjadřovat náladu na trhu, nýbrž pouze daného sektoru, který pokrývá.
- .GOLD – Bitcoin se opakovaně přirovnává ke zlatu. Proto se mu také s trochou nadsázky přezdívá digitální zlato. Dává smysl tyto dvě komodity porovnávat, protože obě mají stejný význam – ochrana finančních prostředků před inflací a znehodnocením.

Veškeré získané údaje byly staženy z analytického portálu Stooq, který je nashromáždil z burz – samozřejmě zde chybí údaje z víkendů a svátků, protože v tyto dny jsou burzy zavřené. Za pomoci programu IBM SPSS Modeler 18.3 byla data sjednocena do jednoho souboru a spárována se všemi daty. Záznamy začínají dnem 19. 7. 2010 a končí dnem 12. 1. 2022, jenž byl zvolen náhodně a nemá žádný konkrétní význam. Celkem má soubor 2 889 řádků, tedy 2 889 dnů s hodnotami výše zmiňovaných komodit a indexů. Ukázka použitých dat je vypsaná v následující tabulce (Tabulka 17).

*Tabulka 17 – ukázková vstupní data první korelační analýzy s denními razítky*

Date	BTC [USD]	SPX [USD]	DXY [USD]	GOLD [USD/oz]
19.07.2010	0,08080	1071,25	82,513	1183,35
20.07.2010	0,07474	1083,48	82,747	1191,25
21.07.2010	0,07921	1069,59	83,393	1185,55
22.07.2010	0,05050	1093,67	82,595	1193,70

Pro vyřešení korelační analýzy byl použit program IBM SPSS Statistics, který měl potvrdit či případně vyvrátit korelaci těchto čtyř ukazatelů. Jednalo se o programovou funkci Analyze → Correlate → Bivariate. V investorské sféře je tato informace důležitá, protože umožňuje snáze predikovat chování ostatních trhů na základě jednoho trhu – nejčastěji právě díky indexu S&P 500. Anglický termín, který se používá pro označení ztráty závislosti dvou a více trhů, se nazývá decoupling. Bitcoinová komunita silně doufá v naplnění tohoto stavu, protože pak by byl Bitcoin jako komodita nezávislý a hůře ovlivnitelný světovými trhy.

Model tedy vypočítal Pearsonův korelační koeficient, Spearmanův korelační koeficient a Kendallův koeficient konkordance (Tabulka 18, Tabulka 19 a Tabulka 20).

*Tabulka 18 – Pearsonův korelační koeficient pro BTC, DXY, SPX a GOLD*

Pearsonův test	BTC	DXY	SPX	GOLD
<b>BTC</b>	1,000	0,250	0,838	0,532
<b>DXY</b>	0,250	1,000	0,622	-0,237
<b>SPX</b>	0,838	0,622	1,000	0,357
<b>GOLD</b>	0,532	-0,237	0,357	1,000
<b>n</b>	2 889	2 889	2 889	2 889

Tabulka 19 – Spearmanův korelační koeficient pro BTC, DXY, SPX a GOLD

Spearmanův test	BTC	DXY	SPX	GOLD
BTC	1,000	0,568	0,963	0,189
DXY	0,568	1,000	0,658	-0,355
SPX	0,963	0,658	1,000	0,159
GOLD	0,189	-0,355	0,159	1,000
n	2 889	2 889	2 889	2 889

Tabulka 20 – Kendallův koeficient konkordance pro BTC, DXY, SPX a GOLD

Kendallův test	BTC	DXY	SPX	GOLD
BTC	1,000	0,367	0,836	0,133
DXY	0,367	1,000	0,443	-0,242
SPX	0,836	0,443	1,000	0,100
GOLD	0,133	0,242	0,100	1,000
n	2 889	2 889	2 889	2 889

n = počet záznamů

Výsledky Pearsonova korelačního koeficientu ukazují, že .BTC (bitcoinový index) má poměrně slabou přímou závislost s .DXY (dolarovým indexem). Dále má poměrně silnou přímou závislost s .SPX (akciovým indexem) a střední přímou závislost s .GOLD (indexem zlata).

Výsledky Kendallova koeficientu konkordance říkají, že se .BTC (bitcoinový index) slabě blíží žádné shodě s .DXY (dolarovým indexem). Dále se silně blíží úplné shodě s .SPX (akciovým indexem) a žádné shodě s .GOLD (indexem zlata).

A na závěr výsledky Spearmanova korelačního koeficientu udávají, že .BTC (bitcoinový index) má střední přímou závislost s .DXY (dolarovým indexem). Dále má poměrně silnou přímou závislost s .SPX (akciovým indexem) a slabou přímou závislost s .GOLD (indexem zlata).

Z výsledků tedy plyne, že tržní cena Bitcoinu opravdu koreluje s akciovými indexy, jako například s indexy .SPX a .DJI. Naopak index amerického dolaru má slabý až střední vliv na cenový vývoj Bitcoinu. V případě tržní ceny zlata je možné konstatovat, že by neměla mít žádný vliv.



### 8.4.2 Druhá korelační analýza

Druhá korelační analýza porovnává cenový vývoj Bitcoinu oproti bitcoinovému hashratu (výpočetní výkon bitcoinové sítě), míře vyhledávání slova „Bitcoin“ ve vyhledávači Google (míra zájmu o Bitcoin) a toku amerického dolarového kapitálu (celosvětová míra zájmu o americký dolar).

Důvody výběru těchto ukazatelů:

- BTC hashrate (výpočetní výkon bitcoinové sítě) – cenový vývoj Bitcoinu má velký vliv na výnosnost bitcoinových těžebních farem, které na základě ceny mohou zapojovat, nebo odpojovat těžební stroje (bitcoinové rigy).
- BTC Google Trends (míra vyhledávání slova „Bitcoin“ ve vyhledávači Google) – míra zájmu o Bitcoin například ve vyhledávači Google může být spojena s jeho cenovými výkyvy.
- USD Net Capital Flow (míra zájmu o americký dolar) – tok amerického dolaru, který je spojován s mírou zájmu o něj, může mít nepřímý vliv na investice obecně.

Data o bitcoinovém hashratu pochází z databanky portálu Nasdaq Data Link. Údaje o toku amerického dolaru byly vyexportovány z analytického portálu Investing.com, který sleduje pohyby amerického kapitálu. A přehled míry zájmu o slovo „Bitcoin“ ve vyhledávači Google byl stažen přímo z oficiální stránky Google Trends. Data mají měsíční razítka, protože je to nejsnazší způsob, jak získat celý soubor záznamů. Záznamy začínají měsícem červenec 2010 a končí měsícem leden 2022. Za pomoci programu IBM SPSS Modeler 18.3 byla data sjednocena do jednoho souboru a spárována se všemi daty. Celkem má soubor 139 řádků, tedy 139 měsíců s hodnotami výše zmiňovaných ukazatelů. Ukázka použitých dat je vypsána v následující tabulce (Tabulka 21).

Tabulka 21 – ukázková vstupní data druhé korelační analýzy s měsíčními razítky

Date	Price [USD]	Hashrate [TH/s]	Trend	Flow [USD]
2010-07	0,07	0,00	0	-9100000000
2010-08	0,06	0,01	0	74300000000
2010-09	0,06	0,01	0	19400000000
2010-10	0,19	0,03	0	85600000000

Model opět vypočítal Pearsonův korelační koeficient, Spearmanův korelační koeficient a Kendallův koeficient konkordance (Tabulka 22, Tabulka 23 a Tabulka 24).

*Tabulka 22 – Pearsonův korelační koeficient pro tržní cenu BTC, BTC hashrate, BTC Google Trends a USD Net Capital Flow*

<b>Pearsonův test</b>	<b>Price</b>	<b>Hashrate</b>	<b>Trend</b>	<b>Flow</b>
<b>Price</b>	1,000	0,842	0,741	0,213
<b>Hashrate</b>	0,842	1,000	0,628	0,218
<b>Trend</b>	0,741	0,628	1,000	0,217
<b>Flow</b>	0,213	0,218	0,217	1,000
<b>n</b>	139	139	139	139

*Tabulka 23 – Spearmanův korelační koeficient pro tržní cenu BTC, BTC hashrate, BTC Google Trends a USD Net Capital Flow*

<b>Spearmanův test</b>	<b>Price</b>	<b>Hashrate</b>	<b>Trend</b>	<b>Flow</b>
<b>Price</b>	1,000	0,962	0,961	0,075
<b>Hashrate</b>	0,962	1,000	0,905	0,083
<b>Trend</b>	0,961	0,905	1,000	0,090
<b>Flow</b>	0,075	0,083	0,090	1,000
<b>n</b>	139	139	139	139

*Tabulka 24 – Kendallův koeficient konkordance pro tržní cenu BTC, BTC hashrate, BTC Google Trends a USD Net Capital Flow*

<b>Kendallův test</b>	<b>Price</b>	<b>Hashrate</b>	<b>Trend</b>	<b>Flow</b>
<b>Price</b>	1,000	0,846	0,842	0,046
<b>Hashrate</b>	0,846	1,000	0,740	0,055
<b>Trend</b>	0,842	0,740	1,000	0,061
<b>Flow</b>	0,046	0,055	0,061	1,000
<b>n</b>	139	139	139	139

n = počet záznamů

Výsledky Pearsonova korelačního koeficientu ukazují, že tržní cena Bitcoinu má poměrně silnou přímou závislost s bitcoinovým hashratem. Dále má poměrně silnou přímou závislost s bitcoinovými Google Trends a poměrně slabou přímou závislost s USD Net Capital Flow.

Výsledky Kendallova koeficientu konkordance říkají, že se tržní cena Bitcoinu silně blíží úplné shodě s bitcoinovým hashratem. Dále se silně blíží úplné shodě s bitcoinovými Google Trends a žádné shodě s USD Net Capital Flow.

A na závěr výsledky Spearmanova korelačního koeficientu udávají, že tržní cena Bitcoinu má poměrně silnou přímou závislost s bitcoinovým hashratem. Dále má poměrně silnou přímou závislost s bitcoinovými Google Trends a slabou přímou závislost s USD Net Capital Flow.

Z výsledků tedy plyne, že tržní cena Bitcoinu opravdu koreluje s bitcoinovým hashratem a bitcoinovými Google Trends. Naopak USD Net Capital Flow nemá na cenový vývoj Bitcoinu žádný vliv.

## Závěr

Cílem této diplomové práce na téma analýza kryptoměn bylo především potvrdit či vyvrátit vliv různých faktorů na tržní ceny kryptoměn a pokusit se predikovat chování trhu. Byly provedeny predikční modely časové řady, model Stock to Flow a dvě velké korelační analýzy. Všechny základy, podklady a předpoklady pro praktickou část jsou rozprostřeny napříč teoretickou částí.

První třetina celkové analýzy zkoumá predikční vlastnosti časových řad a snaží se je aplikovat na chování tržní ceny Bitcoinu. Tato samotná analýza je rozdělena na dvě základní části podle typu vstupních dat.

První část této analýzy se zaměřuje na model časové řady ze vstupních dat, které vychází z korelace ostatních trhů, nálady na trhu a bitcoinových vlastností. Predikce byla aplikována na 7 dní a na 30 dní vybraného období. Ukázalo se, že je výhodnější použít menší interval predikce, protože je zde menší riziko větší chyby. Model dokáže částečně odhadnout trend trhu, jeho potenciální minimum a potenciální maximum. Spoléhat na přesnou hodnotu výsledné predikce určitě nelze, protože existuje celá řada externích vlivů, které mohou trhy ovlivňovat. Ovšem v tomto případě se model trefil a reálná data se pohybovala v predikčním koridoru, a dokonce skončila na predikční linii.

Druhá část čerpala z ukazatelů technické analýzy. Tady vystupuje více dat, protože vstupy modelu časové řady bylo nutné nejdříve spočítat z historických dat o tržní ceně Bitcoinu a nemuselo se tolik spoléhat na již získaná data. Opět byla aplikována predikce na 7 dní a na 30 dní stejného období jako u první části. Zajímavé zde je, že test modelu časové řady vyhodnotil mnohem menší potenciální odchylky (střední chybu) oproti realitě než u první části, která byla trojnásobně méně přesná. To může být způsobeno větším počtem vstupních dat zhruba čtyřnásobně. Na druhou stranu valná většina obchodníků a investorů skrze tyto technické ukazatele opravdu obchoduje, z čehož lze usuzovat, že chování těchto indikátorů má na trh znatelný vliv. Co se týče rozdílů predikce a reality, tak tam nedošlo k zásadním změnám oproti výsledkům první části. Realita je téměř po celou dobu v predikčním koridoru. Také je nutné připustit, že investiční ukazatele mají svoje pravidla užívání a nelze je přesně zapojit do analýzy za použití pouhých číselných dat.

Z obou částí lze tedy usuzovat, že model časových řad dává smysl u vývoje tržní ceny daného aktiva a jeho analýza přináší jisté výsledky. Ty je ovšem nutné brát s rezervou, protože mají spíše ukázkový charakter a naznačují jakýsi trend či potenciál trhu.

Model Stock to Flow využívá stanovené rezervy a přítoku nových bitcoinů do systému. Tento model se používá u různých komodit, takže dává smysl jej aplikovat i na odhad tržní ceny Bitcoinu díky jeho vlastnostem. Nejprve bylo nutné spočítat některé další hodnoty pro jednotlivé dny, jako třeba roční přítok nových bitcoinů z dostupných dat a potřebnou dobu pro dosažení bitcoinové zásoby. Posléze se na získané hodnoty aplikoval Stock to Flow vzorec pro odhad tržní ceny. Zprvu se výsledný graf tvářil, že realita opravdu sleduje vynesenu křivku z odhadu tržní ceny modelu Stock to Flow. Korelační analýza potvrdila jistou závislost, ale v posledních měsících, či dokonce letech se realita odchyluje od odhadu. Toto je možné pozorovat pouhým okem a významná závislost obou veličin je způsobena převážně počátečními daty. Bude zajímavé pozorovat, na jaké částky se tržní cena Bitcoinu dostane před dalším takzvaným pūlením, které by mělo potvrdit, či vyvrátit významnost tohoto modelu.

Na závěr proběhly dvě korelační analýzy, které zkoumaly, jaká další data mají vliv na tržní cenu Bitcoinu. V obou modelech se pracovalo s Pearsonovým korelačním koeficientem, se Spearmanovým korelačním koeficientem a také s Kendallovým koeficientem konkordance. Cílem bylo zjistit, jaké další trhy nebo bitcoinové vlastnosti napřímou ovlivňují chování kryptoměnového trhu, a hlavně tedy samotného Bitcoinu jakožto významného udavatele trendu v kryptoměnách.

V první korelační analýze se pracovalo převážně s indexy, které jsou zrcadlem všech okolních trhů a obecné nálady investorů. Jednalo se tedy o S&P 500, dolarový index a tržní cenu zlata. V kryptoměnové komunitě se udává, že všechny tyto tři vedlejší veličiny mohou hýbat s tržní cenou Bitcoinu. Výsledky tohoto modelu potvrdily silnou přímou závislost tržní ceny Bitcoinu s indexem S&P 500. U dolarového indexu vyšla nízká až střední přímá závislost a u zlata pouze zanedbatelná přímá závislost. Pro běžného investora to znamená, že pohyby indexu S&P 500 mohou výrazně ovlivňovat tržní cenu Bitcoinu a měl by případně pozorněji spravovat svoje investice v době zvýšené volatility těchto trhů.

Ve druhé korelační analýze došlo na bitcoinová data a tok amerického dolaru. Zde se používalo podstatně méně záznamů, protože časové razítko bylo nastaveno po měsících z důvodu lepší interpretace vybraných parametrů. Obsahem modelu byla data o výkonu

bitcoinové sítě a míře zájmu o Bitcoin skrze portál Google Trends. K tomu se přidal tok amerického dolaru, který by mohl mít vliv na kapitál firem a investorů jakožto potenciálních držitelů kryptoměn. Za použití stejných koeficientů se určila míra závislosti. Ukázalo se, že bitcoinová data mají silnou přímou závislost s tržní cenou Bitcoinu, zatímco tok amerického dolaru má naprosto zanedbatelnou přímou závislost, tedy nemá žádný vliv na tržní cenu Bitcoinu. Takže se vyplatí sledovat výkon bitcoinové sítě a míru zájmu o Bitcoin, na základě kterých si lze udělat představu, jakým směrem se trh ubírá.

Ideálním scénářem by bylo sledovat všechny silně závislé veličiny s tržní cenou Bitcoinu a dle určité metodiky přiřadit váhu jednotlivým atributům. Podle chování vícero parametrů najednou může investor maximalizovat kvalitu svého rozhodování na trhu. Obecně platí, že čím více dat modely mají, tím lepší jsou pak závěry.

## Citovaná literatura

ANTONOPOULOS, Andreas M., 2017. *Mastering Bitcoin*. Druhé vydání. Sebastopol: O'Reilly Media, Inc. ISBN 978-1-4919-5438-6.

ANTONOPOULOS, Andreas M. a Gavin WOOD, 2018. *Mastering Ethereum*. Sebastopol: O'Reilly Media, Inc. ISBN 978-1-4919-7189-5.

ARLT, Josef, Markéta ARTLOVÁ a Eva RUBLÍKOVÁ, 2002. *Analýza ekonomických časových řad s příklady*. První vydání. Praha: Vysoká škola ekonomická. ISBN 80-245-0307-7.

AXIE INFINITY LIMITED, 2022. How to Keep Your Account Secure. *Sky Mavis* [online] [vid. 2022-10-05]. Dostupné z: <https://support.axieinfinity.com/hc/en-us/articles/4405346996251-How-to-Keep-Your-Account-Secure>

BENEDIKTOVICH, Dmitry, 2022. Decentralizované burzy (DEX) - Srovnání pro rok 2022 » Finex.cz. *Finex.cz* [online]. [vid. 2022-09-30]. Dostupné z: <https://finex.cz/rubrika/kryptomeny/decentralizovane-burzy/>

BINANCE ACADEMY, 2022a. Co je ukazatel RSI? *Binance Academy* [online] [vid. 2022-05-18]. Dostupné z: <https://academy.binance.com/cs/articles/what-is-the-rsi-indicator>

BINANCE ACADEMY, 2022b. MACD Indicator Explained. *Binance Academy* [online] [vid. 2022-05-18]. Dostupné z: <https://academy.binance.com/en/articles/macd-indicator-explained>

BINANCE ACADEMY, 2022c. Moving Averages Explained. *Binance Academy* [online] [vid. 2022-05-18]. Dostupné z: <https://academy.binance.com/en/articles/moving-averages-explained>

BINANCE ACADEMY, 2022d. Průvodce fundamentální analýzou kryptoměn. *Binance Academy* [online] [vid. 2022-05-18]. Dostupné z: <https://academy.binance.com/cs/articles/a-guide-to-cryptocurrency-fundamental-analysis>

BYBIT LEARN, 2021. Bybit Learn | Bitcoin Stock-to-Flow Model: Will Scarcity Help Retain BTC's Long-Term Value? *Bybit Learn* [online] [vid. 2022-05-18]. Dostupné z: <https://learn.bybit.com/investing/bitcoin-stock-to-flow-model/>

COINTELEGRAPH.COM, 2022. What are decentralized exchanges, and how do DEXs work? *Cointelegraph* [online] [vid. 2022-05-18]. Dostupné z: <https://cointelegraph.com/defi-101/what-are-decentralized-exchanges-and-how-do-dexs-work>

COOK, Matthew, 2021. Jak vydělat peníze hraním her | Alza.cz. *Alza* [online] [vid. 2022-05-18]. Dostupné z: <https://www.alza.cz/jak-vydelat-penize-hranim-her>

DULÍNEK, Jakub, 2022. Srí Lanka se chce vyhnout bankrotu, pozastavila splácení zahraničního dluhu - *Novinky.cz*. *Novinky.cz* [online] [vid. 2022-05-18]. Dostupné z: <https://www.novinky.cz/zpravy/ekonomika/181111-sri-lanka-se-chce-vyhnut-bankrotu-pozastavila-splaceni-zahranicniho-dluhu-181111>

z: <https://www.novinky.cz/ekonomika/clanek/sri-lanka-se-chce-vyhnout-bankrotu-pozastavila-splaceni-zahranicniho-dluhu-40393670>

EUROMONEY.COM, 2022. Blockchain Explained: What is blockchain? | Euromoney Learning. *Euromoney* [online] [vid. 2022-05-18]. Dostupné z: <https://www.euromoney.com/learning/blockchain-explained/what-is-blockchain>

FRANKENFIELD, Jake, 2021. Consensus Mechanism (Cryptocurrency). *Investopedia* [online] [vid. 2022-09-27]. Dostupné z: <https://www.investopedia.com/terms/c/consensus-mechanism-cryptocurrency.asp>

FRANKENFIELD, Jake, 2022a. Lightning Network Definition. *Investopedia* [online] [vid. 2022-09-27]. Dostupné z: <https://www.investopedia.com/terms/l/lightning-network.asp>

FRANKENFIELD, Jake, 2022b. Proof of Work (PoW). *Investopedia* [online] [vid. 2022-09-27]. Dostupné z: <https://www.investopedia.com/terms/p/proof-work.asp>

FRANKENFIELD, Jake, 2022c. Proof-of-Stake (PoS). *Investopedia* [online] [vid. 2022-09-27]. Dostupné z: <https://www.investopedia.com/terms/p/proof-stake-pos.asp>

FRANKENFIELD, Jake, 2022d. What Are Smart Contracts on the Blockchain and How They Work. *Investopedia* [online] [vid. 2022-09-27]. Dostupné z: <https://www.investopedia.com/terms/s/smart-contracts.asp>

HAAGENSEN, Erik, 2022. American Rescue Plan. *Investopedia* [online] [vid. 2022-09-27]. Dostupné z: <https://www.investopedia.com/american-rescue-plan-definition-5095694>

HAYES, Adam, 2022a. Blockchain Facts: What Is It, How It Works, and How It Can Be Used. *Investopedia* [online] [vid. 2022-09-27]. Dostupné z: <https://www.investopedia.com/terms/b/blockchain.asp>

HAYES, Adam, 2022b. On-Balance Volume (OBV). *Investopedia* [online] [vid. 2022-05-18]. Dostupné z: <https://www.investopedia.com/terms/o/onbalancevolume.asp>

HAYES, Adam, 2022c. Who Is Satoshi Nakamoto? *Investopedia* [online] [vid. 2022-05-18]. Dostupné z: <https://www.investopedia.com/terms/s/satoshi-nakamoto.asp>

HENDL, Jan, 2021. Základy Matematiky, Logiky a Statistiky Pro Sociologii a Ostatní Společenské Vědy V Příkladech. *ProQuest Ebook Central* [online]. Dostupné z: <https://www.proquest.com/legacydocview/EBC/6658947?accountid=17116>

CHARVÁT, Jan, 2011. Slovensko nakonec euroval schválilo. *Radio Prague International* [online] [vid. 2022-09-27]. Dostupné z: <https://cesky.radio.cz/slovensko-nakonec-euroval-schvalilo-8559726>

INVESTPLUS.CZ, 2022. Peněženky pro kryptoměny, kde uchovat virtuální měny, co je TREZOR? *InvestPlus* [online] [vid. 2022-05-18]. Dostupné z: <https://investplus.cz/investice/penezenky-pro-kryptomeny-kde-uchovat-virtualni-meny-co-je-trezor/>



KRAMBS, Tobies, 2022. Crypto Fear & Greed Index - Bitcoin Sentiment. *Alternative.me* [online] [vid. 2022-11-22]. Dostupné z: <https://alternative.me/crypto/fear-and-greed-index/>

KŘEČEK, Štěpán, 2017. Venezuela stojí nad propastí bankrotu | Kurzy.cz. *Kurzy.cz* [online] [vid. 2022-05-18]. Dostupné z: <https://www.kurzy.cz/zpravy/438053-venezuela-stoji-nad-propasti-bankrotu/>

LACINA, Jiří, 2021. Nigérie je ve velkých problémech. Zemi trápí velká nezaměstnanost i inflace. *iDNES.cz* [online] [vid. 2022-05-18]. Dostupné z: [https://www.idnes.cz/ekonomika/zahranicni/nigerie-ekonomicke-problemy-chudoba-kriminality-pandemie.A210617\\_121620\\_eko-zahranicni\\_jla](https://www.idnes.cz/ekonomika/zahranicni/nigerie-ekonomicke-problemy-chudoba-kriminality-pandemie.A210617_121620_eko-zahranicni_jla)

MACHÁČEK, Štěpán, 2021. Libanon v krizi: Kdo měl možnost, už zemi opustil, popisuje zpravodaj Radiožurnálu. *iROZHLAS* [online] [vid. 2022-05-18]. Dostupné z: [https://www.irozhlas.cz/zpravy-svet/podcast-vinohradska12-libanon-machacek\\_2112130600\\_cen](https://www.irozhlas.cz/zpravy-svet/podcast-vinohradska12-libanon-machacek_2112130600_cen)

MITCHELL, Cory, 2021. Average Directional Index (ADX) Definition and Uses. *Investopedia* [online] [vid. 2022-05-18]. Dostupné z: <https://www.investopedia.com/terms/a/adx.asp>

MITCHELL, Cory, 2022. Accumulation/Distribution Indicator (A/D) Definition and Uses. *Investopedia* [online] [vid. 2022-05-18]. Dostupné z: <https://www.investopedia.com/terms/a/accumulationdistribution.asp>

MÜHLFEIT, František, 2022. NFT token přehledně: co to je, jak vytvořit a kde ho koupit. *E15.cz* [online] [vid. 2022-05-18]. Dostupné z: <https://www.e15.cz/kryptomeny/nft-prehledne-kde-koupit-a-jak-vytvorit-token-jenz-hybe-kryptosvetem-1383564>

PLANB, 2019. Bitcoin Stock to Flow Model - S2F Live Chart (PlanB). *Buy Bitcoin Worldwide* [online] [vid. 2022-05-18]. Dostupné z: <https://stats.buybitcoinworldwide.com/stock-to-flow/>

ROONEY, Kate, 2020. Bitcoin loses half of its value in two-day plunge. *CNBC* [online] [vid. 2022-05-18]. Dostupné z: <https://www.cnb.com/2020/03/13/bitcoin-loses-half-of-its-value-in-two-day-plunge.html>

SHARMA, Rakesh, 2022a. Non-Fungible Token (NFT): What It Means and How It Works. *Investopedia* [online] [vid. 2022-09-27]. Dostupné z: <https://www.investopedia.com/non-fungible-tokens-nft-5115211>

SHARMA, Rakesh, 2022b. What Is Decentralized Finance (DeFi) and How Does It Work? *Investopedia* [online] [vid. 2022-09-27]. Dostupné z: <https://www.investopedia.com/decentralized-finance-defi-5113835>

STROUKAL, Dominik a Jan SKALICKÝ, 2021. *Bitcoin a jiné kryptopeníze budoucnosti: historie, ekonomie a technologie kryptoměn, stručná příručka pro úplné začátečníky*. Třetí rozšířené vydání. Praha: Grada Publishing. ISBN 978-80-271-1043-8.

TAN, Tan, 2021. Joe Biden oficiálně podepsal schválení záchranného balíčku v hodnotě 1,900 XNUMX miliard USD. *Blog Tiền Áo* [online]. [vid. 2022-05-18]. Dostupné

z: <https://cs.blogtienao.com/joe-biden-vyhr%C3%A11-prvn%C3%AD-v%C3%BDzvu-v-hodnot%C4%9B-1900-miliard-USD/>

TĚTEK, Josef, 2020. Bitcoinový halving a model Stock to flow | Alza.cz. *Alza* [online] [vid. 2022-05-18]. Dostupné z: <https://www.alza.cz/bitcoinovy-halving-a-model-stock-to-flow>

TĚTEK, Josef, 2021. *Bitcoin: Odluka peněz od státu*. Praha: Braiins Systems. ISBN 978-80-907975-5-0.

THE INVESTOPEDIA TEAM, 2022a. Coronavirus Aid, Relief, and Economic Security (CARES) Act. *Investopedia* [online] [vid. 2022-05-18]. Dostupné z: <https://www.investopedia.com/coronavirus-aid-relief-and-economic-security-cares-act-4800707>

THE INVESTOPEDIA TEAM, 2022b. Top 7 Technical Analysis Tools. *Investopedia* [online] [vid. 2022-05-18]. Dostupné z: <https://www.investopedia.com/top-7-technical-analysis-tools-4773275>

WEISINGER, Corey, 2022. Codeless Time Series Analysis with KNIME: A Practical Guide to Implementing Forecasting Models for Time Series Analysis Applications. *ProQuest Ebook Central* [online]. Dostupné z: <https://www.proquest.com/legacydocview/EBC/7072635?accountid=17116>

WILLIAMS, Ward, 2022. Timeline of U.S. Stock Market Crashes. *Investopedia* [online] [vid. 2022-09-27]. Dostupné z: <https://www.investopedia.com/timeline-of-stock-market-crashes-5217820>