

**Česká zemědělská univerzita v Praze**

**Provozně ekonomická fakulta**

**Katedra ekonomických teorií**



## **Bakalářská práce**

**Kryptoměny: porovnání výkonu a faktory úspěchu**

**Pavel Hodan**

© 2022 ČZU v Praze

## ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Pavel Hodan

Ekonomika a management

Název práce

**Kryptoměny: porovnání výkonu a faktory úspěchu**

Název anglicky

**Cryptocurrencies: comparison of performance and success factors**

---

### Cíle práce

Hlavním cílem práce bude poměření výkonnosti klasických fiat vůči Bitcoinu a Ethereum, jakožto nejrozšířenějším kryptoměnám, od jejich vzniku až do dnešní doby. Jako další cíl bude zjištění výkonnosti mladších kryptoměn, mezi které se řadí Cardano a Polkadot, a jejich rozšířenost a použitelnost oproti Bitcoinu a Ethereum. Jako poslední bude zjištěna decentralizace jednotlivých kryptoměn k následnému určení potenciální manipulace s cenou.

### Metodika

Teoretická část se bude zabývat vývojem klasických měn a kryptoměn. Dále se bude zjišťovat potenciální využitelnost kryptoměn v budoucích letech a až do jaké míry jsou schopny nahradit klasické měny. Praktická část se bude zabývat fundamentální a technickou analýzou daných měn a kryptoměn pomocí ukazatelů, mezi které patří klouzavý průměr, RSI index a Fibonnaciho posloupnost. Tyto ukazatele budou určovat další vývoj těchto měn a jejich cenové hladiny v budoucnosti. Nakonec se bude určovat jaké množství jednotlivých kryptoměn je v rukou drobných a investorů a jaké množství vlastní velké společnosti k určení potenciálního ovlivňování cen jednotlivých kryptoměn.

## Doporučený rozsah práce

30 – 40 stran

## Klíčová slova

analýza, Bitcoin, blockchain, Cardano, digitální měna, kryptoměna, Polkadot,

---

## Doporučené zdroje informací

- ANTONOPOULOS, A. M. *Mastering bitcoin: unlocking digital cryptocurrencies*. Sebastopol, CA: O'Reilly, 2015. ISBN 978-1-449-37404-4
- ASHWORTH, Will, 2021. *Cardano Is Worth Considering for Its Utility and Strong Leadership* [online]. 7.4.2021 [cit. 2021-5-6]. Dostupné z: <https://investorplace.com/2021/04/cardano-is-worth-considering-for-its-utility-and-strong-leadership/>
- GRAHAM, B. – ZWEIG, J. *Intelligentní investor*. Praha: Grada, 2007. ISBN 978-80-247-1792-0.
- LÁNSKÝ, J. *Kryptoměny*. V Praze: C.H. Beck, 2018. ISBN 978-80-7400-722-4.
- Polkadot — An Early In-Depth Analysis — Part One — Overview and Benefits. [Cryptoseq.medium.com](https://cryptoseq.medium.com/polkadot-an-early-in-depth-analysis-part-one-overview-and-benefits-ea16de17c05c) [online]. 9.9.2020 [cit. 2021-5-6]. Dostupné z: [/cryptoseq.medium.com/polkadot-an-early-in-depth-analysis-part-one-overview-and-benefits-ea16de17c05c](https://cryptoseq.medium.com/polkadot-an-early-in-depth-analysis-part-one-overview-and-benefits-ea16de17c05c)
- STROUKAL, D. – SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti : historie, ekonomie a technologie kryptoměn, stručná příručka pro úplné začátečníky*. Praha: Grada Publishing, 2018. ISBN 978-80-271-0742-1.
- VERMAAK, Werner, 2021. *A Deep Dive Into Cardano*. [Coinmarketcap.com](https://coinmarketcap.com/alexandria/article/a-deep-dive-into-cardano) [online]. 18.1.2021 [cit. 2021-5-6]. Dostupné z: <https://coinmarketcap.com/alexandria/article/a-deep-dive-into-cardano>

---

## Předběžný termín obhajoby

2021/22 LS – PEF

## Vedoucí práce

Ing. David Křížek

## Garantující pracoviště

Katedra ekonomických teorií

Elektronicky schváleno dne 29. 12. 2021

**doc. PhDr. Ing. Lucie Severová, Ph.D.**

Vedoucí katedry

Elektronicky schváleno dne 8. 2. 2022

**doc. Ing. Tomáš Šubrt, Ph.D.**

Děkan

V Praze dne 01. 02. 2023

## **Čestné prohlášení**

Prohlašuji, že svou bakalářskou práci "Kryptoměny: Porovnání výkonu a faktory úspěchu" jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 31. 3. 2023



## **Poděkování**

Rád bych touto cestou poděkoval vedoucímu své práce, panu Ing. Davidu Křížkovi za pomoc, ochotu a rady při zpracování této práce. Dále bych chtěl poděkovat rodině a přátelům za podporu během studia.

# Kryptoměny: Porovnání výkonu a faktory úspěchu

## Abstrakt

Bakalářská práce pojednává o výkonu a úspěchu Bitcoinu, Etheru, Cardana a Polkadotu v porovnání s klasickými měnami. Cílem práce zjištění faktorů pro úspěch jednotlivých kryptoměn technickou a fundamentální analýzou. Teoretická část se zabývá důvody vzniku monetárního systému a digitálních měn. Jsou zde vysvětleny základní pojmy a odlišení jednotlivých kryptoměn od sebe. Dále jsou uvedeny pojmy týkající se technické a fundamentální analýzy a jednotlivé typy ukazatelů ke zjištění potenciálního vývoje. V praktické části dochází k analýze vybraných kryptoměn z technického hlediska analýzy ke zjištění budoucího vývoje ceny. Fundamentální část se zabývá využitím a obecným přijetím daných kryptoměn ze strany investorů s následným zjištěním decentralizace jednotlivých projektů. Poslední část analýzy určuje jednotlivé výhody a nevýhody zkoumaných kryptoměn. Na základě provedené technické analýzy je Ether určený jako nejlepší aktuální investice z vybraných kryptoměn. Po stránce fundamentální analýzy vychází dobře Ether a Cardano, které nabízí velké množství uplatnění v reálném světě. Decentralizaci vládne Cardano, protože se velké množství mincí nabízí v rukou drobných investorů a nadšenců této technologie.

**Klíčová slova:** Bitcoin, Ethereum, Cardano, Polkadot, Blockchain, peněženka, analýza, decentralizace

# **Cryptocurrencies: comparison of performance and success factors**

## **Abstract**

The bachelor's thesis discusses the performance and success of Bitcoin, Ether, Cardano and Polkadot compared to traditional currencies. The aim of the thesis is to find out the factors for the success of individual cryptocurrencies through technical and fundamental analysis. The theoretical part deals with the reasons for the creation of the monetary system and digital currencies. Basic terms and the differences between individual cryptocurrencies are explained here. Terms related to technical and fundamental analysis and individual types of indicators to determine potential development are also presented. In the practical part, there is an analysis of selected cryptocurrencies from the technical point of view of the analysis to determine the future development of the price. The fundamental part deals with the use and general acceptance of these cryptocurrencies by investors, with the subsequent determination of the decentralization of individual projects. The last part of the analysis determines the individual advantages and disadvantages of the investigated cryptocurrencies. Based on the technical analysis carried out, Ether is determined to be the best current investment from the selected cryptocurrencies. In terms of fundamental analysis, Ether and Cardano do well, offering a large number of real-world applications. Decentralization is ruled by Cardano, as a large number of coins are offered in the hands of small investors and enthusiasts of this technology.

**Keywords:** Bitcoin, Ethereum, Cardano, Polkadot, Blockchain, wallet, analysis, decentralization

# Obsah

<b>1 Úvod</b> .....	<b>9</b>
<b>2 Cíl práce a metodika</b> .....	<b>10</b>
2.1 Cíl práce.....	10
2.2 Metodika.....	10
<b>3 Teoretická východiska</b> .....	<b>12</b>
3.1 Vytvoření měnového systému .....	12
3.2 První pokusy o zavedení alternativních měn .....	13
3.3 Kryptoměny .....	13
3.3.1 Blockchain a jeho vývoj .....	17
3.3.2 Typy konsensu u kryptoměn .....	19
3.3.3 Whitepaper .....	21
3.3.4 Bitcoin .....	22
3.3.5 Ethereum .....	23
3.3.6 Ada Cardano.....	24
3.3.7 Polkadot.....	28
3.4 Technická analýza .....	29
3.4.1 Svíčky grafu .....	30
3.4.2 Klouzavý průměr .....	32
3.4.3 Index relativní síly.....	33
3.4.4 Fibonnaciho retracement .....	33
3.5 Teorie Fundamentální analýzy kryptoměn .....	35
3.5.1 Faktory fundamentální analýza kryptoměn.....	35
<b>5 Vlastní práce</b> .....	<b>39</b>

5.1	Technická analýza vybraných kryptoměn .....	39
5.1.1	Technická analýza bitcoinu .....	39
5.1.2	Technická analýza Etheru .....	42
5.1.3	Technická analýza Cardana.....	43
5.1.4	Technická analýza Polkadotu.....	46
5.2	Fundamentální analýza vybraných kryptoměn.....	48
5.2.1	Fundamentální analýza Bitcoinu .....	48
5.2.2	Fundamentální analýza Etheru .....	50
5.2.3	Fundamentální analýza Cardana .....	51
5.2.4	Fundamentální analýza Polkadotu .....	52
5.3	Decentralizace jednotlivých kryptoměn .....	52
5.4	Poměření výhod a nevýhod jednotlivých kryptoměn .....	54
<b>5</b>	<b>Závěr .....</b>	<b>55</b>
	<b>Seznam použitých zdrojů.....</b>	<b>57</b>
	<b>Knížní zdroje .....</b>	<b>57</b>
	<b>Elektronické zdroje .....</b>	<b>57</b>

## **Seznam Obrázků**

Obrázek 1	Vysvětlení svíček grafu.....	31
Obrázek 2	Graf ceny Bitcoinu – denní graf .....	40
Obrázek 3	Graf ceny Bitcoinu – čtyřhodinový graf.....	41
Obrázek 4	Graf ceny Etheru – denní graf.....	42
Obrázek 5	Graf ceny Etheru – čtyřhodinový graf.....	43

Obrázek 6 Graf ceny Cardana – denní graf.....	44
Obrázek 7 Graf ceny Cardana – čtyřhodinový graf .....	45
Obrázek 8 Graf ceny polkadotu – denní graf .....	46
Obrázek 9 Graf ceny Polkadotu – čtyřhodinový graf .....	47
Obrázek 10 Vývoj těžebního výkonu Bitcoinu v grafu .....	49
Obrázek 11 Vývoj těžebního výkonu Etheru v grafu.....	50

# 1 Úvod

Po velké finanční krizi v roce 2008 nastala ve světě velká finanční nejistota. To vedlo spoustu lidí k hledání alternativ klasických měn, které by tyto měny mohly po stránce směny nahradit. Možná náhrada se objevila v podání Bitcoinu. Jeho tvůrce, Satoshi Nakamoto, představil možnost, jak bezpečně provádět téměř instantní transakce po celém světě. Systém byl naprosto transparentní a bez centrální jednotky, která by o systému rozhodovala.

V roce 2015 byl spuštěn podobný koncept, který také umožňoval provádět transakce. Tento projekt jménem Ethereum měl na svědomí mladý programátor Vitalik Buterin. Ten však viděl potenciál v posunutí celého systému na novou úroveň.

Poslední roky přinesly spoustu nových projektů podobného typu s tím, že každá z nich má snahu řešit jiné problémy. Populární jsou především u mladých lidí, kdežto starší generace je vnímá skepticky. Velké množství investorů se jim raději vyhýbá z důvodu vysoké volatility.

První část práce bude věnována historii měn až po vybrané digitální měny, které budou popsány a rozvedeny od jejich vzniku až po jejich aktuální fáze. Poté bude popsána funkce technické a fundamentální analýzy.

## **2 Cíl práce a metodika**

### **2.1 Cíl práce**

Hlavním cílem práce je poměření výkonnosti klasických měn vůči kryptoměnám, které jsou součástí nové generace platebních metod a poskytují i mnoho dalších využití. Konkrétně se bude práce věnovat čtyřem významným zástupcům jenž jsou Bitcoin, Ethereum, Cardano a Polkadot. Tyto kryptoměny se řadí mezi nejvíce populární z investorské perspektivy. Výkonnost daných kryptoměn je posouzena na základě technické analýzy, která se provádí pomocí orientace v grafech finančního vývoje za rok 2022. Pomůckou k vytváření předpokládaných budoucích cenových hladin jsou finanční ukazatele. Konkrétně se bude jednat klouzavý průměr, RSI index a Fibonnaciho posloupnost. Dále se určuje fundamentální analýza pomocí zjištění kapitalizace jednotlivých kryptoměn ke zjištění jejich vnitřní hodnoty, která určuje přidanou hodnotu jednotlivých projektů. Další část se věnuje zjišťování decentralizaci těchto kryptoměn, pro možné ovlivňování cen.

### **2.2 Metodika**

Bakalářská práce je rozdělena do dvou částí. První část se věnuje teoretickým východiskům a druhá část analyzuje vybrané kryptoměny z pohledu technické analýzy, fundamentální analýzy a decentralizace. Strukturu první části utváří pět kapitol a několik dílčích kapitol.

První kapitola se věnuje shrnutí historii a vzniku monetárního systému, až aktuální situaci. Dále popisuje roli drahých kovů, které sehráli důležitou roli v utváření měn.

Druhá kapitola pojednává o prvních pokusech vytvoření alternativních měn, které vytvořili myšlenku pro státem neřízenou měnu.

Třetí kapitola popisuje vytvoření kryptoměn, jak je dnes známe. Jsou zde popsány základní informace o jejich fungování a náležitost. Dále jsou zde popsány čtyři vybrané kryptoměny (Bitcoin, Ethereum, Cardano a Polkadot), které jsou popsány ze strany jejich fungování a využití.



Čtvrtá kapitola teoretické části se věnuje technické analýze kryptoměn pro určení potenciálního směru aktiva na základě analýzy grafu. Používá se hodně mezi investory, kteří chtějí v daný moment zjistit možný vývoj ceny. V této oblasti se využívá mnoho ukazatelů a indexů. První podkapitolu je věnovaná svíčkám grafu, které jsou základní věc u technické analýzy. Jsou zde také popsáni tři ukazatele, kteří jsou nejvíce využívány právě k určení technické analýzy u kryptoměn. Jedná se o klouzavý průměr, RSI index a Fibonnaciho retracement.

Pátá, a také poslední kapitola teoretické části popisuje teorii fundamentální analýzy aktiv, která se používá pro lepší ohodnocení vybraného aktiva, v tomto případě kryptoměn. Popisuje způsoby, kterými se může určit cena kryptoměny. Tato metoda je široce využívána mezi investory, kteří chtějí reálně ohodnotit vybrané aktivum.

Praktická část je rozdělena do čtyř částí, která se věnují podrobné analýzy Bitcoinu, Etheru, Cardana a Polkadotu.

První část se zaměřuje na technickou analýzu vybraných kryptoměn za použití klouzavého průměru, RSI indexu a Fibonnaciho posloupnosti. Jednotlivé kryptoměny jsou zkoumány z delšího a kratšího časového úseku. Delší představuje denní graf a kratší představuje čtyřhodinový graf. U každé kryptoměny se popisuje jejich další možný cenový vývoj.

Druhá část se věnuje fundamentální analýze zkoumaných kryptoměn, pro určení jejich přidané hodnoty ze strany reálného i potenciálního využití.

Třetí část zkoumá decentralizaci kryptoměn pomocí analýzy největších kryptopeněženek vybraných kryptoměn.

Poslední část popisuje výhody a nevýhody vybraných kryptoměn.

### 3 Teoretická východiska

Část teoretická východiska se věnuje vývoj měn od směnného obchodu až po kryptoměny. Popisuje čtyři konkrétní kryptoměny a jejich způsob fungování. Dále je v této části vypsán význam a způsob fundamentální technické analýzy, které se používají k přesnějšímu ohodnocení všech aktiv, tedy i kryptoměn.

#### 3.1 Vytvoření měnového systému

V prvopočátku zde existoval pouze směnný obchod neboli Barter, který se využíval velice dlouhou dobu. Bohužel narážel na různá úskalí, ale největší z nich byl ten, že pokud chtěl někdo dostat ku příkladu vlnu a nabízel za něj například vajíčka, tak tato osoba musela najít někoho, kdo bude vlnu nabízet a zároveň bude potřebovat vajíčka. Z tohoto důvodu se jako prostředek směny začali používat vzácnější předměty, které měly dlouhou životnost a zároveň byly dobře skladné. V různých kulturách napříč světem se tento problém řešil všemi možnými způsoby. V přímořských oblastech byl tento problém řešen například mušlemi. Postupně se však ve většině zemí přešlo k drahým kovům díky jejich vzácnosti. Díky svému objemu se staly prvním univerzálním prostředkem směny. Další výhodou bylo jejich odvažování a jednoduché dělení. Mince od té doby byly různě upravovány ale k jejich největšímu vývoji došlo až v poměrně nedávné době. Ve spoustě zemí byly zavedeny bankovky, které měly pevnou hodnotu, ale největší změna přišla až ve 20. století, kdy byla jejich hodnota oddělena od drahých kovů. Vedlo to k tomu, že již nebyly kryty zlatem nebo stříbrem ale jejich hodnota byla určena jednotlivými státy. V dnešní době drahé kovy mají význam pouze jako předmět obchodu a udržitel ceny. Z toho důvodu se jejich cena určuje převážně spekulacemi na komoditních trzích. Díky tomu jsou peníze vydávány a pouze státem a ten také jediným ručitelem dané měny. Dalším vývojem peněz je jejich elektronizace. Jde hlavně o to, že v dnešní době je většina peněz, zhruba 90 %, pouze v elektronické podobě na bankovních účtech. <sup>1</sup>

---

<sup>1</sup> DAVIES, Glyn, 2002. *A history of money: From Ancient Times to the Present Day*. 3. Cardiff: UNIVERSITY OF WALES PRESS. ISBN 0-7083-1773-1.

## 3.2 První pokusy o zavedení alternativních měn

Po vzniku internetu se ve světě začaly tvořit myšlenky na to, jak by bylo možné přesouvat peníze z účtu na účet, aniž by tato transakce netrvala řadu dní, mnohdy i týdnů. Dalšími problémy posílání peněz tkvěly v tom, že platby stály vysoké poplatky, byly netransparentní a také v mnoha případech nebezpečné. Mezi první pokusy zavedení alternativních plateb můžeme řadit Ecash nebo Cybercash. Ecash byl vytvořen společností Digicash a byl považován za průkopníka v kryptoměnach. Jednalo se o systém, jenž sloužil k posílání drobných částek (méně než jeden dollar). Šlo o to, že celá tato digitální měna fungovala na způsob slepého podpisu. Tím pádem, dokud není tento digitální dopis podepsán příjemcem, tak je obsah zprávy zakryt. Díky inovativní vlastnosti šlo o velice zabezpečený typ plateb. Za tímto projektem stojí Dr. David Chaum, který s touto myšlenkou přišel již v roce 1983, přitom přístup veřejnosti k internetu byl až v roce 1990. Tento nápad se zamlouval i spoustě bank, které chtěli tuto platformu využívat a rozšířit jí do vědomí společnosti. Mezi bankami, jež o tuto platformu měli zájem, patřila například Deutsche Bank, Credit Suisse a mnoha dalších. Zájem byl dokonce i od Microsoftu, který jí chtěl využít v operačním systému Windows 95, jenže se tyto společnosti nemohly dohodnout a z akvizice nakonec sešlo. Téměř všechny banky, které chtěli využívat platformu, nakonec zůstali pouze u testování platformy a nikdy jí nevypustily jako skutečný produkt pro klienty. Jedinou bankou, která platformu spustila byla banka Mark Twain.<sup>2</sup>

## 3.3 Kryptoměny

Kryptoměnu můžeme definovat jako digitální aktivum, které, na rozdíl od klasických měn, nemá žádnou fyzickou podobu. Tím pádem veškerý nákup a prodej těchto měn probíhá

---

<sup>2</sup> KAGAN, Julia. Ecash. <https://www.investopedia.com/> [online]. 31.3.2021 [cit. 2023-01-31]. Dostupné z: <https://www.investopedia.com/terms/e/ecash.asp#:~:text=pioneer%20in%20cryptocurrency,-eCash%20was%20created%20by%20Dr.,link%20withdrawal%20and%20spend%20transactions>.

elektronicky. Tyto měny nejsou regulovány žádným centrálním systémem, jako u klasických měn, a díky tomu veškeré obchody mezi klienty probíhají bez jakéhokoliv prostředníka.<sup>3</sup>

V dnešní době je přesná definice kryptoměn poměrně složitá, jelikož je aktuálně v oběhu něco přes 20000 různých kryptoměn, které mají spoustu různých druhů využití a je čistě na jejich vývojářích, jaké množství dané kryptoměny bude v oběhu.

Kryptoměny obecně však musí splňovat určité vlastnosti, aby byla určena obecná definice, např.:

- Decentralizace – neexistuje žádná centrální autorita nebo banka, která může danou kryptoměnu ovlivňovat a kontrolovat.
- Absence třetí strany – využívá se zde peer-to-peer systém, takže zde nenalezneme žádného prostředníka, který by se staral o přenos transakcí mezi uživateli.
- Mezinárodní systém – transakce lze posílat instantně po celém světě, což bankovní systém neumožňuje. Jsou zde z pravidla i mnohonásobně menší poplatky za transakce.
- Zabezpečení – Díky využití asymetrické kryptografie mají kryptoměny vysokou bezpečnost a lze je velmi těžko prolomit. K šifrování a následnému dešifrování jsou použity dva různé klíče.
- Anonymita – U transakcí nelze vidět údaje o odesílateli ani příjemci. Transakce je ale možné dohledat.
- Transparentnost sítě – Jedná se o fundamentální myšlenku kryptoměn. V Blockchainu lze každou transakci dohledat.
- Platby nelze stornovat – v případě, že uživatel již transakci provedl, tak není jí následně zrušit.<sup>4</sup>

#### a) Mince a token

Pro označování prostředku směny u kryptoměn se používá mince a token. Mince, na rozdíl od tokenu, je u kryptoměn, které mají svůj vlastní blockchain. Jedná se tedy například o

---

<sup>3</sup> STROUKAL, D. -- SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti: historie, ekonomie a technologie kryptoměn, stručná příručka pro úplné začátečníky*. Praha: Grada Publishing, 2018. ISBN 978-80-271-0742-

<sup>4</sup> HARTINGEROVÁ, Emma. Kryptoměny-Definice a vlastnosti. <https://www.itnetwork.cz> [online]. [cit. 2023-01-30]. Dostupné z: <https://www.itnetwork.cz/kryptomeny/zaklady-kryptomen/>

Bitcoin, Ether, Cardano a Polkadot. U těchto mincí se také používá označení nativní token. Jedná se tedy přímé aktivum blockchainu dané kryptoměny.

Token však potřebuje pro vznik být na blockchainu jiné kryptoměny, protože vlastní blockchain nemá. Nejčastěji tokeny vznikají na blockchainu Etheru. Tokeny mají mnoho typů využití v různých oblastech. Mezi zástupce se řadí bezpečnostní tokeny, majetkové tokeny, stabilní mince a nenahraditelné tokeny.

Bezpečnostní tokeny představují akcie určité firmy, která tyto tokeny emituje. Mají tedy veškeré vlastnosti akcií, ale jsou zde přidány výhody blockchainu v podobě vysoké rychlosti přenosů, nízkým poplatkům a možnosti hlasovat o budoucnosti firmy pomocí Proof of stake.

U majetkových tokenů je hodnota podložena na základě reálných aktiv, mezi které lze zařadit zlato, stříbro nebo třeba nemovitosti.

Stabilní mince neboli stablecoin představují mnohem stabilnější hodnotu uchování ceny než kryptoměny. Cena stablecoinů je podložena cenou klasických fiat měn jako je americký dolar anebo euro. Jejich hodnota je navázaná a vybranou měnu 1:1.

Nenahraditelné token neboli také NFT představují digitální předměty, které jsou unikátní v celém blockchainu. To z nich dělá lákavé aktivum pro investice. Může představovat různá umělecká díla nebo sběratelské předměty v počítačových hrách.<sup>5</sup>

## b) Kryptopeněženka

Způsobů, kterými si uživatel může pořídit kryptoměny, je v dnešní době opravdu mnoho. Mezi ty nejznámější se řadí softwarové peněženky. Zde nalezneme velké množství zástupců, z nichž jsou nejvíce rozšířené coinbase wallet, exodus a mycelium. Hlavní funkcí těchto peněženek je přesouvat tokeny z jedné adresy na jinou pomocí kryptografie. Tyto peněženky představují program nebo aplikaci v mobilu, ve kterém má uživatel jednoduchou správu svých financí. Peněženka musí obsahovat celou kopii blockchainu, aby v ní provedené transakce mohly být ověřeny.

---

<sup>5</sup> WON, Daniel. Token vs. Coin – Simple Explanation. <https://www.exodus.com/> [online]. 2020 [cit. 2023-01-25]. Dostupné z: <https://www.exodus.com/news/token-vs-coin/>

Další možnost držet kryptoměny je pomocí kryptoburz. Burzy jsou uživatelsky velmi přívětivé, jelikož je velmi jednoduché účet vytvořit a následně jedním kliknutím uživatelem vybranou kryptoměnu nakoupit. V tomto případě jsou nakoupené kryptoměny uloženy v síti dané burzy a uživateli stačí znát jen své přihlašovací údaje. Uživatel tedy ukládá prostředky u třetí strany. Na základě tohoto faktu mají kryptoburzy snahu co nejvíce eliminovat možnost zcizení kryptoměn. Nejčastěji ke zcizení v tomto případě dochází v případě, že si uživatel vytvořil slabé heslo, které lze jednoduše prolomit. Proto burzy doporučují uživateli při vytváření účtu kombinaci velkých a malých písmen, a také přidání čísel a symbolů k zabezpečení. Popřípadě se také používá autentizace přihlašování a plateb pomocí SMS kódu nebo zasláním potvrzovacího kódu na e-mail.

Posledním zástupcem jsou hardwarové peněženky. Ty mají podobu zařízení, které je podobné externímu disku a připojí se USB portem k počítači. Jsou vybaveny úložištěm a zabezpečovacím čipem, který snižuje riziko vykradení peněženky hackerem, který by se k ní dostal. Prodávají se různé typy, u kterých může záležet na tom, kolik kryptoměn mohou uložit a na typu zabezpečovacího čipu. To vše záleží na tom, kolik uživatel za peněženku zaplatí. Schopnější peněženky umí uložit více typů kryptoměn.

Nevýhody jsou v tom, že peněženku může uživatel lehce ztratit, což se v minulosti stalo již mnohokrát. Uživatelé také mohou mít problémy, pokud chtějí nakoupit peněženku za co nejnižší cenu, a to může vést k nakoupení peněženky z neautorizovaných stránek. Zde se mohou nacházet peněženky, které mají předem nahráný virus, který se aktivuje vložením prostředků na ní. Následně dojde ke zcizení obsahu peněženky přesunutím prostředků na předem určenou peněženku.<sup>6</sup>

Například kryptopeněženka Ledger Nano X dokáže uložit až 5500 mincí různých kryptoměn a dokáže se bezdrátově připojit i k mobilnímu telefonu pomocí funkce Bluetooth.<sup>7</sup>

---

<sup>6</sup> KERNER, Sean. Crypto wallet (cryptocurrency wallet). *Https://www.techtarget.com* [online]. [cit. 2023-01-30]. Dostupné z: <https://www.techtarget.com/searchsecurity/definition/crypto-wallet-cryptocurrency-wallet>

<sup>7</sup> *Ledger Nano X* [online]. [cit. 2023-01-30]. Dostupné z: <https://shop.ledger.com/pages/ledger-nano-x>

### 3.3.1 Blockchain a jeho vývoj

Pod pojmem Blockchain si můžeme představit účetní knihu, ve které se zapisují veškeré transakce kryptoměny, která se na daném Blockchainu nachází. Jeho jednotlivé části jsou bloky, jež jsou za sebou lineárně uspořádané a vzájemně na sebe navazují. Toto spojení se nazývá Hash. Jde o to, že každý má v sobě specifický kód, jenž je obsažen i v jeho předchozím bloku. Díky této funkci je systém jako celek velice bezpečný, protože pokud by někdo chtěl manipulovat s daným blokem, tak by musely být upraveny i všechny ostatní bloky. První vytěžený blok neboli tzv., Genesis Block“ je vždycky tím nejznámějším blokem a je zde 0 místo hashe jeho předka, jelikož zde žádný není. V případě Bitcoinu byl vytěžen Satoshiem Nakamurou a odstartoval tímto těžbu Bitcoinu. Bitcoin může obsahovat i určité větve o velikosti 1 až 2 bloky. Jsou brány jako výhonky celého řetězce. Tyto výhonky se vyskytují velice výjimečně a mohou nastat v případě, že je v Blockchainu vytěžen blok dvěma různými a na sobě nezávislými těžaři v podobnou dobu. Tyto bloky se následně ignorují. Schváleny jsou pouze transakce v nejdelší lineární řadě bloků. Pouze tento řetězec je pro celý blockchain relevantní.<sup>8</sup>

- Hashrate

Tento pojem se používá zejména u sítě Bitcoinu. Jedná se o výkonnost Bitcoinové sítě v jednotkách za sekundu. Můžeme ho využít pouze u kryptoměn, které jsou těženy na základě P-O-W neboli Proof of work. Díky tomuto ukazateli lze zjistit zájem o těžbu dané kryptoměny. Pokud se hashrate zvyšuje, tak lze usoudit že o kryptoměnu je veliký zájem ze strany těžařů a zároveň se zvyšuje bezpečnost celého blockchainu kryptoměny. Těžaři se také mohou díky svému osobnímu hashratu vypočítat, nakolik je jejich těžba výnosná po finanční stránce. Naopak, pokud se hashrate snižuje, tak se kryptoměna pro těžaře stává nevýnosná a následně

---

<sup>8</sup> ANTONOPOULOS, A. M. Mastering bitcoin: unlocking digital cryptocurrencies. Sebastopol, CA: O'Reilly, 2015. ISBN 978-1-449-37404-4



můžou změnit těženou kryptoměnu nebo přestat těžit úplně. Z investorského hlediska je snižující se hashrate negativní věc, jelikož ukazuje snížený zájem o kryptoměnu.<sup>9</sup>

- Blockchain 2.0

Původní blockchain, na kterém je vytvořen Bitcoin, měl pouze jednu zásadní funkci, a to sice provádění transakcí mezi uživateli této sítě. Jeho nástupce neboli Blockchain 2.0, však umožňuje i daleko více možností využití. Tento blockchain je nejvíce známý u Etheru. Funkcí v tomto novém konceptu poměrně dost, například zde můžeme najít pojem mikrotransakce. Tato funkce nezní moc zajímavě ale rozhodně se jedná o důležitou schopnost novější verze blockchainu. Výhoda oproti klasickému platebnímu systému tkví v tom, že na blockchainu lze provádět transakce pohybující se v řádech centů. Tato možnost přináší nové příležitosti k reálnému použití. Například lze platit mikrotransakce ostatním uživatelům blockchainu, aby byla vaše hlavní transakce vyřízena dříve. V tomto případě se snižuje vytíženost sítě a zvyšuje se tím efektivita celého systému. Další funkcí jsou již zmiňované chytré kontrakty. Nejjednodušší případ můžeme nalézt u nákupních automatů. Tento systém má jasně daná pravidla, podle kterých se řídí. Do automatu vložíte mince, vyberete svoji volbu a systém následně začne ověřovat, jestli vložená částka odpovídá ceně vybraného produktu. V případě že ano, automat vám vybranou volbu poskytne. Můžeme zde nalézt také tzv. chytré vlastnosti. Tato schopnost se týká obzvláště autorského práva. Toto umožňuje uživateli vlastnit určitou věc. Informace o vlastnictví je pevně zadána v blockchainu, tím pádem nelze danou věc od skutečného majitele jakýmkoliv způsobem zpronevřit.<sup>10</sup>

- Blockchain 3.0

Blockchain první i druhé generace nabízeli spoustu nových věcí, ale stále měli problémy se škálovatelností. Konkurence v podobě PayPalu a Visy dokáže provádět průměrně 1700

---

<sup>9</sup> KAVANAGH, Robin. Hash rate: A measure of the computing power on a cryptocurrency network that is a key security indicator. <https://www.businessinsider.com> [online]. 2022 [cit. 2023-01-30]. Dostupné z: <https://www.businessinsider.com/personal-finance/hash-rate>

<sup>10</sup> ALYOSHKIN, Roman. <https://polys.vote/> [online]. 2017 [cit. 2023-01-30]. Dostupné z: <https://polys.vote/blog/blockchain-2>



transakcí za minutu ale Bitcoin za stejnou dobu provede maximálně 7 transakcí a Ether zvládne provést 20. Problém je v tom, že při transakci se platba potvrzuje zpětně od odesílatele. Dochází tedy k prodlevě, díky které dochází k omezení rychlosti transakcí mezi uživateli. Došlo tedy k vytvoření nového způsobu, kdy není třeba informace o platbě zpětně potvrzovat. Tento způsob umožní pohybu informací v pouze jedním směrem a dojde k navýšení rychlosti plateb. U kryptoměn, které tento způsob využívají je schopnost provádět až 10 transakcí za minutu. Proto je tento způsob výrazně větší a počítá s větším množstvím uživatelů v budoucí době. Jako hlavní zástupce této nové generace lze zařadit Cardano, Polkadot, EOS a mnoho dalších. Vývoj technologie však ještě potřebuje přijetí všeobecné společnosti.<sup>11</sup>

### 3.3.2 Typy konsensu u kryptoměn

Konsensus se v oblasti kryptoměn využívá k tomu, aby byly všechny provedené transakce v síti ověřeny správně. Vyjadřuje souhlas všech těžařů, kteří těží stejnou blok sítě, a tím pádem mají stejnou verzi blockchainu. Zastávají tedy podobnou funkci jako centrální jednotka u klasických měn, aby nevznikaly falešné transakce, které skutečně neproběhly. Jedná se tedy o základní pilíř fungování kryptoměn, při kterém není třeba žádný prostředník, který by kontrolu prováděl.<sup>12</sup>

#### a) Proof of work

V síti Bitcoinu se k těžbě mincí používá systém Proof of work, který se týká všech uživatelů. Pokud tedy uživatel chce Bitcoin těžit, a nejen nakupovat a prodávat, tak potřebuje výkonný počítačový systém, který je využit k těžbě mincí. Každý těžařský systém obsahuje kopii účetní knihy Bitcoinu. Systémy, které obsahují stejnou verzi této účetní knihy pak následně zahájí těžbu stejného bloku sítě. Těžba probíhá tak, že těžařské systémy zpracovávají různé typy komplexních matematických úloh, které potřebují velký výpočetní výkon k následnému vyřešení. Tým, který jako první všechny úlohy na daném bloku splní, vyhrává a

---

<sup>11</sup> NAVEEN, Joshi, 2021. EVERYTHING YOU NEED TO KNOW ABOUT BLOCKCHAIN 3.0. <https://www.bbntimes.com> [online]. 2021 [cit. 2023-01-30]. Dostupné z: <https://www.bbntimes.com/technology/everything-you-need-to-know-about-blockchain-3-0>

<sup>12</sup> PRITZKER, Yan, 2020. *Výnález jménem Bitcoin*. Braiins Publishing. ISBN 978-80-907975-0-5.

následně všechny ostatní výpočetní systémy aktualizují své účetní knihy, aby se shodovaly s účetní knihou vítězného týmu. Tento tým si následně rozdělí odměnu v podobě mincí a poplatků za transakce. Tato odměna je mezi uživatele rozdělena proporcionálně na základě výpočetní síly, kterou jednotlivý uživatelé na těžbu vynaložili.<sup>13</sup>

Tento systém je velice užitečný u veřejných blockchainových sítí, ale jeho hlavní nevýhoda spočívá v množství vynaložené energie na těžbu. Další problém spočívá v tom, že čím více bloků je vytěženo, tím se náročnost na těžbu exponenciálně zvyšuje. V prvních letech těžby stačil k těžbě i obyčejný notebook, na kterém se spustil speciální počítačový program k těžbě a uživatel mohl těžit. V posledních letech se však náročnost na těžbu zvýšila z důvodu neustále rostoucího zájmu o kryptoměny. Proto tedy těžaři musí mít počítačové sestavy složené z mnoha výkonných grafických karet za statisíce korun. To se však posledním roce mění, jelikož ceny kryptoměn jsou na ročním minimu a cena elektrické energie se stále zvyšuje. To vede těžaře k ukončení těžby a následnému prodeji těchto drahých komponent.<sup>14</sup>

Výhody můžeme tedy najít v tom, že systém jako celek je velice bezpečný pro transakce. Díky potvrzování transakcí jednotlivými těžaři je systém plně decentralizovaný a riziko útoku se snižuje. Nevýhody zde nalezneme v tom, že transakce jsou poměrně pomalé oproti Proof of stake a je zde vysoká energetická náročnost sítě. Je zde také riziko tzv. 51 % útoku, který spočívá v tom, že by se skupině těžařů podařilo dosáhnout více 50 % výpočetní síly celé sítě. Těžaři by poté nemuseli záměrně potvrzovat transakce v bloku nebo v celém systému. To by následně vedlo k zadržení transakcí mezi uživateli. Dále by také byli schopni nechat vracet již provedené transakce, což by vedlo k následnému dvojitému utrácení mincí. Tento typ útoku je však v dnešní době těžko proveditelný z důvodů velkého množství těžařských společností. Proto již dlouze zavedené kryptoměny, jakožto Bitcoin a Etheru, téměř není možné ohrožit.

---

<sup>13</sup> SHEIKH, Husneara, Rahima Meer AZMATHULLAH a Faiza RIZWAN, 2018. *Proof-of-Work Vs Proof-of-Stake: A Comparative Analysis and an Approach to Blockchain Consensus Mechanism* [online]. 6. [cit. 2023-01-31]. ISBN 23219653.

<sup>14</sup> BONHEUR, Kristoffer. PoW: Advantages and Disadvantages of Proof-of-Work. <https://www.profolus.com/> [online]. 15.9.2021 [cit. 2023-01-31]. Dostupné z: <https://www.profolus.com/topics/pow-advantages-and-disadvantages-of-proof-of-work/>

Naopak je tento útok využíván spíše u altcoinů, u kterých je mnohem snazší potřebnou výpočetní sílu získat.<sup>15</sup>

#### b) Proof of stake

Mechanismus Proof of stake funguje odlišně od Proof of work a jeho hlavní výhoda spočívá v tom, že oproti Proof of work má téměř nulovou náročnost na výpočetní výkon sítě. Způsob, kterým dochází k vytváření nových bloků a ověřování transakcí tkví v tom, že uživatelé nakoupí jimi požadovaný množství mincí, které jsou jimi následně uloženy do depozitáře. Následně dochází k vytvoření nového bloku validátorem, který se vybírá na základě náhodnosti hlasování. Validátor následně ověřuje transakce a informace o bloku. Díky tomu může následně získat poplatky z provedených transakcí. Částka, kterou uživatel musí do depozitáře vložit se odlišuje podle druhu kryptoměny. Čím vyšší je depozitář uživatele, tím větší je možnost jeho zvolení jako validátora. Díky tomu je zde také nižší pravděpodobnost možnost 51 % útoku, jelikož by uživatelé s možností útoku na síť musí mít uloženo velké množství mincí, čímž by snížili i hodnotu svých mincí.<sup>16</sup>

### 3.3.3 Whitepaper

Whitepaper nebo jinak řečeno bílá kniha je dokument, který je sdílen na veřejnost prostřednictvím nějaké určité společnosti, či neziskové organizace, aby se co největší množství lidí dozvědělo o dané kryptoměně všechny nezbytné informace. Jedná se proto o nezbytný základ každé kryptoměny. Tento dokument obsahuje veškeré informace o kryptoměně, její konkurenční výhody, typy využití ale také složité výpočty a technologické problémy. Nejznámějším zástupcem je whitepaper o Bitcoinu, který vydal Satoshi Nakamoto v roce 2008

---

<sup>15</sup> FRANKENFIELD, Jake. 51 % Attack: Definition, Who Is At Risk, Example, and Cost. <https://www.investopedia.com/> [online]. 28.9.2022 [cit. 2023-01-31]. Dostupné z: <https://www.investopedia.com/terms/1/51-attack.asp>

<sup>16</sup> SMITH, Corwin, ed. PROOF-OF-STAKE (POS). <https://ethereum.org/> [online]. 12.1.2023 [cit. 2023-01-25]. Dostupné z: <https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/#:~:text=One%20validator%20is%20randomly%20selected,of%20the%20block%20being%20proposed.>

pod názvem „Bitcoin: A Peer-to-Peer Electronic Cash System“, načež dva měsíce nato byla vytvořena Bitcoinová síť neboli Blockchain.<sup>17</sup>

### 3.3.4 Bitcoin

Bitcoin můžeme považovat za úplně první kryptoměnu, která na rozdíl o klasických měn není nijak centralizovaná. To znamená, že neexistuje žádná skupina lidí, která může hodnotu této měny ovlivnit. U klasických měn vláda dané země určuje hodnotu tím, kolik dalších peněz vypustí ročně do oběhu a tím pádem určují i následnou inflaci dané měny. V případě bitcoinu je v oběhu jen určitý počet jednotek. Díky tomu zde neexistuje žádná inflace, protože nemůže být vytěženo víc jednotek, jelikož je jejich počet limitován. O to, kolik jednotek dané kryptoměny existuje, rozhodují vývojáři dané kryptoměny při jejím vzniku. První zmínky o Bitcoinu jsou z roku 2008, kdy byla založena stránka Bitcoin.org. Po zhruba dvou měsících od jejího vytvoření byl přidán na stránku metzdowd.com příspěvek od uživatele jménem Satoshi Nakamoto, ve kterém popisuje celou síť Bitcoinu. Článek nesl označení „Bitcoin: A Peer-to-Peer Electronic Cash System“. Toto je úplně první zmínka o této kryptoměně a sám Satoshi Nakamoto je pro mnoho zastánců Bitcoinu vnímám jako průkopník. O autorovi Bitcoinu toho však není moc známo, protože se za tímto jménem, nebo spíše pseudonymem nemusí nutně skrývat jedinec, ale může jít o celou skupinu lidí, jenž se snažila vytvořit něco, co by do jisté míry mohlo nahradit klasický měny. Nakamoto se následně v roce 2011 stáhl z fóra a nechal odpovědnost rozvoje kódu a celé sítě na skupině dobrovolníků. Hlavní vlastnost Bitcoinu, je to, že se jedná čistě o digitální aktivum. To znamená, že se je ukládán na krypto účtech uživatelů. Proto je populární u spíše mladší generace lidí.<sup>18</sup>

---

<sup>17</sup> What Is a Cryptocurrency Whitepaper?. <https://academy.binance.com/> [online]. 31.10.2022 [cit. 2023-01-30]. Dostupné z: <https://academy.binance.com/en/articles/what-is-a-cryptocurrency-whitepaper>

<sup>18</sup> ANTONOPOULOS, A. M., 2015. *Mastering bitcoin: unlocking digital cryptocurrencies*. Sebastopol: O'Reilly. ISBN 978-1-449-37404-4.

### 3.3.5 Ethereum

Původní koncept Etheru byl představen široké veřejnosti v roce 2013 Vitalikem Butherinem. Tento mladý programátor, jemuž bylo v tomto roce teprve 19 let, se již nějakou dobu zaobíral Bitcoinem. Za představení tohoto konceptu obdržel stipendium Petera Thiela, tzv., Thiel Fellowship“ ve výši 100000 amerických dolarů. Toto stipendium ho přimělo k tomu, aby skončil na vysoké škole a věnoval se na plný úvazek jako vývojář Etheru. Butherin však viděl blockchain, jenž je základ všech kryptoměn, jako mnohem více rozšiřitelný systém, a ne pouze jako místo k transakcím mezi jeho uživateli. Jeho vize byla v tom, že na tomto blockchainu mohou fungovat různé typy decentralizovaných aplikací a také, že Bitcoin může reprezentovat nový typ komodit. Tohohle všeho lze dosáhnout díky užití kryptografie a tím pádem zde kompletně odpadá nutnost právního systému, jenž je zbytečně pomalý a komplikovaný. Kódování celého systému je velice bezpečné a zároveň transparentní. V roce 2014 zahájil Butherin vývoj Etheru společně s týmem vývojářů, které k tomu přizval. Projekt si získal velkou přízeň široké veřejnosti. V červenci stejného roku proběhlo úvodní kolo prodeje Etheru, jenž je měna Ether, veřejnosti, aby si tento projekt zařídil financování na jeho vývoj.<sup>19</sup>

- Chytrý kontrakt

Ether má stejný základ jako Bitcoin v tom, že má vlastní blockchain, na kterém lze sledovat veškeré transakce v jeho síti. Na blockchainu Etheru je však přidána další vrstva, která umožňuje vytváření chytrých kontraktů na rozdíl od Bitcoinu. Ve své podstatě se jedná pouze o počítačový program, který je vytvořen vývojáři této sítě. Tyto chytré kontrakty lze používat ke spoustě činností, ale mezi hlavní z nich se řadí uzavírání smluv. Program je tvořen na zdrojovém kódu, ve kterém je zapsáno, za jakých podmínek bude smlouva realizovaná. Díky tomu dokáže uzavřít smlouvu mezi dvěma a více účastníky. Následně kontrolu průběh celé smlouvy a v případě, že všechny podmínky smlouvy jsou splněny, tak dojde k jejímu naplnění. Dále se na této síti mohou vytvářet různé typy aplikací, her a burz.

---

<sup>19</sup>Vitalik Buterin: The man who co-created Ethereum. <https://cointelegraph.com/> [online]. [cit. 2023-01-31]. Dostupné z: <https://cointelegraph.com/ethereum-for-beginners/who-is-vitalik-buterin>

Hlavní výhody této sítě tedy tkví v tom, že:

- Jsou naprosto nestranné vůči účastníkům smlouvy
- Mají mnohem menší náklady na provádění vyhotovení smluv, na rozdíl od právních dohod
- Mají jasnou logiku provedení a matematickou formulaci
- Vytvářejí důvěryhodné vztahy mezi účastníky smluv

Mezi nevýhody můžeme zařadit například chyby při vytváření zdrojového kódu, který by může mít dalekosáhlé následky. Také ještě neexistuje žádná legislativa, která se týká chytrých kontraktů.<sup>20</sup>

- **Ethereum 2.0**

V létě 2022 došlo u Etheru k velké změně podobě aktualizace na nový blockchain. To znamená pro Ether dvě klíčové výhody oproti původnímu konceptu. Síť přešla na způsob ověřování plateb z Proof of work na Proof of stake, což vede k radikální úspoře energie, která je podle vývojářů snížena o 99,9 %. Není to však tak, že by předchozí verze byla odstraněna ale pouze došlo k přidání nové vrstvy, která se stará o ověřování plateb. Původní vrstva má nyní význam jako platforma pro odesílání a přijímání plateb, a dále zde jsou stále k dispozici chytré kontrakty.

Dále by mělo dojít v nejbližší době k navýšení škálovatelnosti. Síť by měla být v roce 2023 schopná provádět tisíce transakcí za vteřinu, což jí dodá konkurenční výhodu oproti Bitcoinu.<sup>21</sup>

### **3.3.6 Ada Cardano**

S postupem času dochází k vytváření spousty dalších kryptoměn po boku hlavních zástupců, jako je Bitcoin a Ether. Tyto nové měny se nazývají altcoiny. Cardano se řadí mezi nejvýraznější zástupce této nové generace. Má snahu se navázat na výhody Bitcoinu a Etheru,

---

<sup>20</sup> *Smart Contracts* [online], 2023. [cit. 2023-01-31]. Dostupné z: <https://ethereum.org/en/smart-contracts/>

<sup>21</sup> MILLMAN, Rene, Stephen GRAVES a Liam KELLY. What Is Ethereum 2.0? Ethereum's Consensus Layer and Merge Explained. <https://decrypt.co/> [online]. 24.3.2022 [cit. 2023-01-31]. Dostupné z: <https://decrypt.co/resources/what-is-ethereum-2-0>



ale hlavně má za úkol tento koncept posunout na novou úroveň. Projekt byl založen jedním ze spoluzakladatelů Etheru, a to sice Charlesem Hoskinsonem. Hoskinson se odloučil od vývojářského týmu Etheru poté, co se dostal do sporu s Vitalikem Buterinem. Proto se rozhodl k vytvoření vlastní kryptoměny, která se zakládá na vlastním Blockchainu se snahou eliminovat nedostatky Etheru.<sup>22</sup>

Mince sítě Cardana neboli ADA, byl pojmenován po matematicce Adě Lovelace. Projekt byl založen v roce 2015 a oficiální spuštění blockchainu proběhlo v roce 2017. V pozadí celého projektu stojí 3 společnosti, z nichž každá hraje svoji roli. První a hlavní společností je Cardano Foundation, která dohlíží na celý vývoj ekosystému kryptoměny. Stará se rovněž všechny právní dokumenty, celkovou integraci systému do systémů jiných kryptoměn a o všeobecném povědomím projektu. Tato společnost je řízena radou, která dohlíží nad celým projektem. Další společností je Input-Output Hong Kong, jenž stará o údržbu sítě Cardano a také o celkovou implementaci blockchainu do vládních systémů, školství a soukromých firem. Dále se stará o decentralizaci a chytré kontrakty na platformě. Hlavním projektem IOHK bylo samotné spuštění celého projektu v roce 2015. Poslední společností v pozadí Cardana je Emurgo, která se podílí na vytváření aplikací a nástrojů pro vývojáře a investuje nových start-upů. Dále se stará o vzdělávání široké veřejnosti ohledně významu a schopností blockchainu. Partnerských společností je mnohem více, ale tyto tři mají úzkou vazbu na celý projekt a jeho budoucnost. Cardano je založené na Proof of stake systému, který je mnohem atraktivnější alternativou Proof of work díky nižší energetické náročnosti. Za celým blockchainem Cardana stojí protokol známý jako Ouroboros. Díky němu má celý vysokou bezpečnost a zároveň celkovou udržitelnost.<sup>23</sup>

---

<sup>22</sup> ASHWORTH, Will, 2021. *Cardano Is Worth Considering for Its Utility and Strong Leadership* [online]. 7.4.2021 [cit. 2021-05-06]. Dostupné z: <https://investorplace.com/2021/04/cardano-is-worth-considering-for-its-utility-and-strong-leadership/>

<sup>23</sup> VERMAAK, Werner, 2021. A Deep Dive Into Cardano. *Coinmarketcap.com* [online]. 18.1.2021 [cit. 2021-05-06]. Dostupné z: <https://coinmarketcap.com/alexandria/article/a-deep-dive-into-cardano>

- Fáze vývoje Cardana

Většina kryptoměn má od jejich vývojářů uvedenou mapu postupných fází vývoje, a to platí i pro Cardano. Vývojáři proto sepsali 5 nejdůležitějších fází vývoje této kryptoměny, které jsou pro její blockchain nezbytné, aby byla vytvořena budoucí hodnota pro investory, pokud ke splnění této fáze skutečně dojde.

První fáze vývoje nese kódové označení Byron. Její hlavní vlastností je, aby byla vytvořena síť Cardana pro možnost nákupů a prodeje tokenů ADA. Tato fáze byla již splněna.

Následuje další již splněná fáze s označením Shelley, ve které došlo k implementaci protokolu Ouroboros, jakožto blockchainu Cardana. Tento protokol funguje základě consensu Proof of stake, který umožňuje uživatelům vkládat nakoupené mince ADA do depozitáře sítě, aby se mohli tyto uživatelé následně podílet na rozšiřování blockchainu a získávat za to odměny.

Další fáze se stará implementaci chytrých kontraktů do sítě pomocí tokenů ADA k vytváření smluv mezi uživateli a k tvorbě decentralizovaných aplikací, které mohou na platformě vznikat. Tato fáze nese označení Goguen a k jejímu vytvoření došlo v září roku 2021.

Čtvrtou fází v pořadí je Basho. V této fázi dochází k vylepšení sítě pomocí lepší interoperability a zlepšení škálování celého systému. Interoperabilita u kryptoměn je velice důležitá věc, jelikož umožňuje, aby blockchain jedné kryptoměny byl schopný komunikovat s ostatními blockchainy jiných kryptoměn. Škálování na druhou stranu zase vyjadřuje počet transakcí, které blockchain dokáže uskutečnit během vteřiny. Blockchain Bitcoinu je v tomto ohledu problematický, jelikož dokáže během vteřiny zpracovat pouze několik desítek transakcí, což je malý počet v porovnání s platebním systémem Cardana, který je potenciálně schopen zpracovat řádově miliony transakcí za vteřinu. V tomto ohledu je systém Cardana v porovnání s ostatními kryptoměnami podstatně výhodnější.

Poslední plánovaná fáze Cardana nese název Voltaire. Cardano se v této fázi stane soběstačnou díky systému hlasování budoucích projektů v komunitě a také díky pokladnici, která bude dotovat nové projekty. Držitelé stakovaných mincí budou hlasovat o nových projektech, které mají být prospěšné pro komunitu. Pokladnice bude představovat krypto



peněženku, do které bude chodit zlomek částky poplatku z každé transakce, která na síti proběhne. To pomůže Cardanu osamostatnit se od IOHK, které aktuálně financuje vývoj.<sup>24</sup>

- **Ouroboros**

Kryptoměny trpí na několik problémů, které se tvůrci Cardana rozhodli minimalizovat vytvořením speciálního blockchainu jménem Ouroboros. V tom spočívá hlavní rozdíl mezi Cardanem a ostatními kryptoměnami. Většinou je ve světě kryptoměn zvykem, že vývojáři pustí nové funkce mezi uživatele, aniž by předem důkladně prováděli kompletní testy.

Ouroboros se zaměřuje na hlavní problém celé oblasti kryptoměn. Jsou jimi škálovatelnost, interoperabilita a udržitelnost. Ke každému z těchto problémů se Ouroboros staví jinak.

– Škálovatelnost vyjadřuje množství transakcí, které lze v průběhu jedné vteřiny provést. Jak již bylo zmíněno, tak tento protokol jich je schopný zpracovat milióny za vteřinu. V současné době je však reálné využití mnohem nižší, tudíž ještě nedošlo k plnému využití. Pro tuto oblast je také třeba velké využití paměti, aby mohly být všechny provedené transakce uloženy. To vývojáři v budoucnu chtějí řešit pomocí komprese uložených dat, ale díky aktuálním nízkým cenám cloudových úložišť je tento problém prozatím neaktuální.

– Interoperabilita pomáhá k propojení více blockchainů mezi sebou. Vývojáři Cardana si byli vědomi, že v budoucnu nebude pouze jedna kryptoměna a všechny ostatní zmizí. Proto do protokolu Ouroboros vložili způsob, který dokáže propojovat blockchainy mezi sebou napřímo. Řešení tohoto problému se nalézá v mostech blockchainu. Ten funguje díky chytrým kontraktům. Pokud tedy někdo chce převést například token ADA na Ether, tak nejprve dojde k vytvoření chytrého kontraktu v síti ADA, ve kterém se do depozitu vloží množství tokenů, které chce uživatel směnit. Poté dochází na řadu tzv. operátoři, kteří uvolní pomocí chytré smlouvy ekvivalentní množství tokenů Etheru. Je zde také odlišení mezi typy mostů, které mohou být jednosměrné nebo i obousměrné.

---

<sup>24</sup> *Cardano – Phases* [online]. [cit. 2023-01-31]. Dostupné z: <https://roadmap.cardano.org/en/>

– Udržitelnost se týká všech kryptoměn. Budoucí vývoj není možný ze strany vývojářů, pokud na to nebudou dostatečné finanční prostředky. Zde Ouroboros přichází s pokladnicí, kterou bude představovat peněženka, ze které nemůžou být vybírány prostředky. Budou se zde ukládat poplatky za transakce mezi uživateli. Prostředky se zde uvolní pouze v případě, že tým vývojářů navrhne nové rozšíření, které je následně předloženo komunitě. Ta na základě hlasování rozhodne, jestli je projekt opravdu přínosný a následně budou na jeho vývoj uvolněny prostředky. To zajišťuje, že prostředky na vývoj budou uplatňovány účelně a nedojde k jejich plýtvání, což má na udržitelnost celé sítě dobrý předpoklad.<sup>25</sup>

### 3.3.7 Polkadot

Polkadot se řadí, stejně jako Cardano, mezi kryptoměny 3. generace a k jeho spuštění došlo 26. května 2020, což ho řadí mezi nejmladší kryptoměnu oproti všem dříve jmenovaným. Vývoj této nové kryptoměny vede Gavin Wood, který se společně s Charlesem Hoskinsonem podílel na vývoji Etheru.

Jeho hlavní cíl je řešit interoperabilitu mezi jednotlivými blockchainya. Jeho základ je tvořen takzvaným relé řetězcem, který funguje na protokolu Proof of stake, stejně jako Cardano. Relé řetězec je hlavním blockchainem celé sítě, který dostává informace od jednodušších typů blockchainů zvaných para řetězců. Tyto sítě získávají informace od klasických blockchainů typu Bitcoin a Etheru. Výměna informací mezi všemi sítěmi se díky tomu velice usnadní i za nízké energetické náročnosti.<sup>26</sup>

Para řetězec získává zabezpečení od relé řetězců pomocí jeho typu konsensu. Díky tomu nevyžaduje svoje vlastní zabezpečení a posílání informací je také v bezpečí. Celý relé řetězec je veden validátory, kteří ověřují transakce v celém systému ukládáním mincí do depozitáře. Mince se zde nazývají DOT.

---

<sup>25</sup> Why use cardano. <https://docs.cardano.org> [online]. [cit. 2023-01-31]. Dostupné z: <https://docs.cardano.org/new-to-cardano/why-use-cardano>

<sup>26</sup> Polkadot — An Early In-Depth Analysis — Part One — Overview and Benefits, 2020. [Cryptoseq.medium.com](https://cryptoseq.medium.com) [online]. 9.9.2020 [cit. 2021-05-06]. Dostupné z: [/cryptoseq.medium.com/polkadot-an-early-in-depth-analysis-part-one-overview-and-benefits-ea16de17c05c](https://cryptoseq.medium.com/polkadot-an-early-in-depth-analysis-part-one-overview-and-benefits-ea16de17c05c)

Relé řetězec má tedy jednoduchou funkci koordinace dat mezi jednotlivými blockchainya. Je zde dokonce absence chytrých kontraktů, jelikož cíl tohoto blockchainu do takové oblasti nezasahuje. Jeho zaměření je na vytvoření spojení mezi všemi ostatními blockchainya. Cílem vývojářů je tedy vytvoření blockchainu, který by se stal středem celého systému všech blockchainů, kde by docházelo k bezpečné výměně informací napříč celým kryptoměnovým sektorem.<sup>27</sup>

### 3.4 Technická analýza

Technická analýza nepracuje s daty o společnosti, komoditě nebo měně ale přímo využívá geometrických čísel převedených do grafů vývoje zkoumaného objektu k následnému určení vývoje v blízké budoucnosti. Předpokladem celé této analýzy je tedy zjišťování určitých tržních vzorců z dosavadního vývoje. Na základě těchto poznatků může investor s vysokou pravděpodobností zjistit následný vývoj. Na rozdíl od fundamentální analýzy tedy zkoumá čistě vývoj grafů. Tento technický vývoj zkoumaného grafu pomáhá lépe určit celkový trend trhu neboli to, jakým směrem se trh ubírá.

V dnešní době se tento typ analýzy stává více a více běžným, jelikož nástroje na tvorbu technické analýzy jsou k dostání na internetu zcela zdarma. Společnosti, které zprostředkovávají prodej akcií, komodit, měn a kryptoměn tyto nástroje přímo vkládají do svých aplikací. Tímto způsobem může investor přímo tyto nástroje využít a následně na stejném portálu obchod uzavřít. To výrazně zjednodušuje situaci pro investora.

Technickou analýzu můžeme využít pro všechny finanční trhy, ale u konkrétních trhů jsou doporučovány různé typy ukazatelů a indikátorů, jelikož ne každý je vhodný pro všechny trhy zároveň.

Další důležitá věc u využití technické analýzy je v tom, v jakém časovém horizontu chce investor obchodovat. Pro investory, kteří obchodují z krátkodobého hlediska, tedy v řádech dnů anebo hodin, je fundamentální analýza naprosto zbytečná.

---

<sup>27</sup> WOOD, Gavin. POLKADOT: VISION FOR A HETEROGENEOUS MULTI-CHAIN FRAMEWORK. <https://polkadot.network> [online]. [cit. 2023-01-25]. Dostupné z: <https://polkadot.network/PolkaDotPaper.pdf>

Jako první se u technické analýzy zjišťuje aktuální trend, který se ubírá třemi směry. V prvním případě je trend rostoucí, dále také nazývaný býčí trh nebo uptrend. V něm investoři nakupují dané aktivum, a to žene cenu aktiva vzhůru. Dochází k němu v době, kdy se růst ekonomiky zvyšuje a nastává ideální čas k investování.

Druhý typ trendu je klesající. Mezi investory se nazývá medvědí trh nebo downtrend. U něho dochází k poklesu ceny, což vede investory k prodávání aktiva. Vyvolává ho snížený zájem po daném aktivu anebo zhoršující se ekonomická situace ve světě.

Třetím typem je horizontální trend, také nazývaným neutrální trend. Při něm je pro investory mnohem více obtížné zjistit potenciaální směr ceny aktiva a je tedy nutný hlubší průzkum. Zjištění trendu je tedy pro investory první nezbytná věc, kterou musí zjistit. Následně lze uplatňovat jednotlivé indikátory a ukazatele zvýšení úspěchu investice.<sup>28</sup>

### 3.4.1 Svíčky grafu

Při zkoumání grafu je hlavní rozumět tomu, jak vůbec jeho jednotlivé svíčky fungují. Pokud investor chce z grafu vyčíst co nejvíce, tak se doporučují právě svíčkové grafy pro jejich přehlednost. Jednotlivé svíčky nám určují, jaký pohyb cenové hladiny nastal za určitý časový rámec. Tento časový rámec si uživatel sám vybírá podle toho, jestli svojí investici vidí krátkodobě nebo dlouhodobě. Například si může zvolit denní graf, u kterého každá svíce představuje jeden den. Pro investicích v kryptoměnách se spíše používají nižší časové úseky. Ideálně se používá čtyřhodinový graf, ve kterém jedna svíce odpovídá posunu za čtyři hodiny.

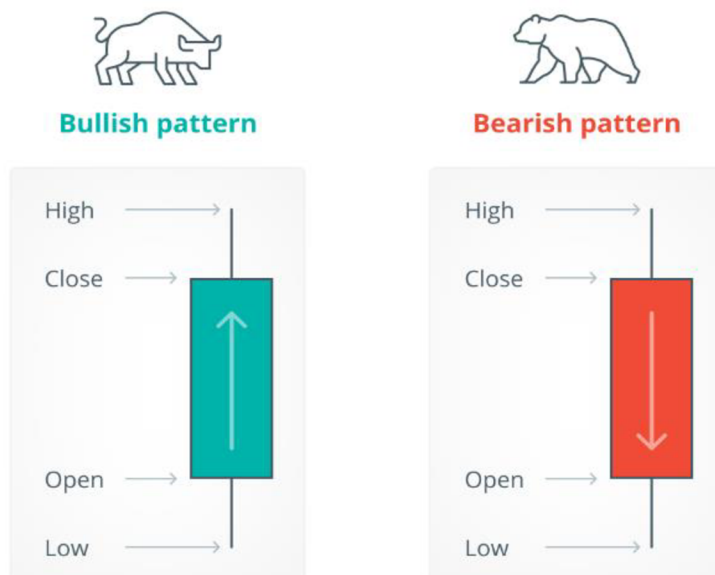
Dále je pro investora ideální sledovat i nižší časové posuvy například desetiminutový graf anebo pětiminutový graf. Tyto grafy pomáhají pro zjištění ideálního vstupu do obchodu a následnému výstupu, aby byl potenciaální zisk co největší.

---

<sup>28</sup> MCALLEN, Fred, 2012. *Charting and Technical Analysis*. Createspace Independent Publishing Platform. ISBN 1456468693.

## Understanding candlestick charts:

Bullish pattern v/s Bearish Pattern



 | cointelegraph.com

Zdroj: cointelegraph.com (2022)

Obrázek č. 1 nám ukazuje, jak tyto svíčky fungují. Zelená nám znázorňuje, že se cena pohybuje směrem vzhůru a červená nám ukazuje pohyb na nižší cenu. V místě „Open“ se svíce otevírá, tedy začíná její časový rámec, který máme předem zvolený. V místě „Close“ naopak dochází k zavření svíce a od této cenové hladiny je tvořena následující svíce. Vrchol svíce neboli místo „High“ nám určuje nejvyšší cenovou hladinu, které svíce za časový úsek dosáhla a „Low“ zase představuje nejnižší cenovou hladinu v utvořené svíci.<sup>29</sup>

---

<sup>29</sup> HOMMA, Munehisa, 2022. *The Candlestick Bible* [online]. Lulu [cit. 2023-01-31]. ISBN 9781458313843.

### 3.4.2 Klouzavý průměr

Když se při technické analýze zjišťuje aktuální trend, tak právě klouzavý průměr je pro to nejvhodnější nástroj. Díky němu může investor s vysokou pravděpodobností zjistit změnu aktuálního trendu. Dále se také může uplatnit ke zjištění supportů a rezistencí ve zkoumaném grafu. Klouzavý průměr je linie vypočítaná jako průměr ceny určitého počtu cenových hladin za uplynulou dobu. Tato linie se zobrazí přímo v grafu sledovaného aktiva. K jeho určení se používají různé časové periody, například 50 nebo 200 dní. Při jejich protnutí dochází k signálu pro investora, jakým trendem se bude aktivum ubírat. Pokud se klouzavý průměr zvyšuje, tak to vypovídá o růstovém trendu. Naopak v případě snižování klouzavého průměru lze předpokládat klesající trend. Můžeme ho dále dělit na více typů klouzavého průměru. Základním typem je jednoduchý klouzavý průměr, který je nazýván SMA (simple moving average). Ten je počítán jako součet uzavřených cenových hladin v zadané periodě vydělený množstvím těchto hladin. Dalším významným ukazatelem je exponenciální vážený průměr neboli EMA (exponencial moving average). Ten funguje na stejném principu, ale na rozdíl od SMA přikládá větší význam novějším hodnotám periody. Takže hodnotám, které jsou nejbližší od aktuální ceny je přikládám větší důraz než těm, které jsou vzdálené. Tyto výpočty ale není nutné provádět, jelikož v dnešní době má každá platforma tyto ukazatele v nabídce grafů, což investorovi podstatně zjednodušuje práci. Tento klouzavého průměru je v praxi mnohem efektivnější, jelikož křivku grafu kopíruje mnohem lépe než SMA.

V praxi se používají ideálně dva klouzavé průměry s jinak dlouhou periodou. Pokud použijeme periodu 50, tak určujeme krátkodobější trend než při použití periody 200. To mnohem lépe naznačuje konec nebo začátek trendu. Tento indikátor je na trhu vysoce používaný a to znamená, že na něj trh rychle reaguje.<sup>30</sup>

---

<sup>30</sup> FERNANDO, Jason. Moving Average (MA): Purpose, Uses, Formula, and Examples. <https://www.investopedia.com> [online]. 2023 [cit. 2023-01-30]. Dostupné z: <https://www.investopedia.com/terms/m/movingaverage.asp>



### 3.4.3 Index relativní síly

Index relativní síly neboli RSI nám udává informace o tom, jestli je trh přeceněný nebo podceněný. Jeho výpočet se provádí na základě cen trhu za posledních 14 dní. Je také zakreslen do grafu a jeho hodnoty jsou vždy mezi 0 a 100 body. V praxi je třeba určit hranice této stupnice ideálně na rozmezí 30 až 70 bodů, abychom byli schopni usoudit kdy do obchodu vstoupit. Pokud se aktuální cena nalézá v hodnotách od 0 do 30, tak je to znamení, že trh je podhodnocený a je ideální čas aktivum nakoupit. Když se cena pohybuje mezi 30 a 70 body, tak je třeba počkat až trh provede posun nad nebo pod danou hladinu, jelikož je trh v neutrální pozici. V momentě, kdy trh pohybuje v rozmezí 70 a 100 bodů, tak se jedná o přesycení trhu je vhodný čas na prodej.<sup>31</sup>

V případě kryptoměn je tento ukazatel vhodné kombinovat s ostatními ukazateli technické analýzy pro přesnější určení následného vývoje. V kombinaci s klouzavým průměrem a fibonnaciho retracementem máme k dispozici skvělé nástroje technické analýzy.

### 3.4.4 Fibonnaciho retracement

Tato metoda je jedna z nejpoužívanějších metod ve světě tradingu k určení cen a u nás nazývá Fibonnaciho úroveň zpětných pohybů. Využívána je zejména ve Forexu neboli měnovém trhu, tudíž je vhodná i pro kryptoměny. Základ má v řadě čísel Fibonnaciho posloupnost a je jednou z pěti metod Fibonnaci, které se v tradingu využívají. Tato metoda se tedy moc nepoužívá při investování na dlouhodobý horizont a spíše pomáhá určovat cenové hladiny v řádu hodin či dní. Klíčové pro tuto metodu jsou určitá čísla, která pomáhají k určení supportů a rezistencí. Support je označení pro místo, ve kterém je předpokládán odraz cenové hladiny vzhůru. Při dotyku grafu této cenové hladiny lze předpokládat odraz ceny vzhůru a tím pádem i vhodný čas na provedení obchodu. Rezistence funguje přesně naopak od supportu, tedy při dotyku aktuální ceny s rezistencí je předpokládána změna vývoje grafu směrem dolů. Cenové hladiny u fibonnaciho retracementu jsou hodnoty 38,2 %, 50 % a 61,8 %. V každé investiční platformě lze tento indikátor používat bez složitých výpočtů uživatele. Jednoduše se

---

<sup>31</sup> HAYDEN, John, 2004. *RSI: The Complete Guide*. Wasendorf & Associates. ISBN 0934380880.

vybere indikátor a následně dojde ve vyznačení nejnižší a nejvyšší cenová hladina grafu v případě, že graf má růstový trend. V případě klesajícího trendu nejdříve dochází k označení nejvyššího bodu a následně bodu nejnižšího. Kromě zjištění supportů a resistencí grafů může být užitečný také pro nalezení cílové ceny anebo stop-loss bodu. Toto je používání spíše u tradingu než u investování na delší dobu. K nastavení těchto bodů dochází při vytvoření obchodu přímo uživatelem. Při dosažení cílové ceny dojde k uzavření ceny, což je pro uživatele výhodný, jelikož nemusí graf neustále sledovat. To samé platí u stop-lossu, kterého je dosaženo, pokud se směr grafu obrátí opačným směrem, než uživatel předpokládal. Je využít primárně k tomu, aby uživatel při špatném odhadnutí směru nepřišel o celou investici.<sup>32</sup>

---

<sup>32</sup> BORODEN, Carolyn, 2008. *Fibonacci Trading: How to Master the Time and Price Advantage*. ISBN 9780071498159.



### 3.5 Teorie Fundamentální analýzy kryptoměn

Tato analýza se považuje za nejvíce komplexní přístup k hodnotě firmy, v našem případě kryptoměny, k určení budoucího pohybu kurzu. Určuje cenu z několika různých faktorů, např.:

1. Vnitřní hodnota podniku
2. Globální faktory
3. Politické faktory
4. Historické faktory
5. Odvětvové faktory

Vnitřní hodnota podniku zjišťuje nejrůznější aspekty firmy, a hlavně její tržní potencial v budoucnosti. K tomu je třeba zjistit aktuální stav firmy a její nastávající projekty.

Zjištění této hodnoty je třeba hlavně ve střednědobém a dlouhodobém investičním horizontu. Pokud investora zajímá krátkodobý finanční horizont, tak toto zjištění bráno jako málo relevantní.

Po analýze všech těchto faktorů investor srovnává odvozenou cenu s aktuální cenou na burze ke zjištění následného vývoje akcií.<sup>33</sup>

#### 3.5.1 Faktory fundamentální analýza kryptoměn

Narozdíl od fundamentální analýzy podniku se u kryptoměn neseťkám s vnitřní hodnotou podniku. Podniky ve většině případů vydávají čtvrtletní reporty o tom, jak se podniku dařilo. Z nich lze pak vypočítat, jestli tržby podniku odpovídají ceně akcií. U kryptoměn žádné takové účetní standardy nejsou, nicméně je možné veřejně vyčíst data o tom, jak často jsou prováděny transakce, a hlavně v jakém objemu. K takovému účelu je možné využít blockchain dané kryptoměny, který je naprosto veřejně přístupný. I přesto si však investoři musí získat náhled na daný projekt, jelikož jsou konkrétní výpočty naprosto odlišné od těch, které se používají ke zjištění fundamentální hodnoty podniku.

---

<sup>33</sup> GRAHAM, B. -- ZWEIG, J. *Inteligentní investor*. Praha: Grada, 2007. ISBN 978-80-247-1792-0.

Hlavním cílem analýzy kryptoměny je snížení rizika pro investora a vyhodnocení ziskového potenciálu kryptoměny.

Jsou zde 3 různé kategorie, ze kterých lze fundamentální analýzu vytvořit.

#### c) Blockchain

Blockchain je velice dobrý zdroj, ze kterého můžeme vyextrahovat data, ale jedná se o velice pracný úkon. Naštěstí je zde spousta programů, které poskytují nástroje na následnou extrakci dat. Jedná se především o kryptoburzy, které jsou v tomto ohledu velmi výhodné. Dokážou uživateli poskytnout spoustu užitečných informací jako je například množství aktivních uživatelů, celkový počet transakcí a výše jednotlivých transakcí. Tyto údaje řadíme k těm nejdůležitějším, co se týče tvoření fundamentální analýzy. Dále zde můžeme zjišťovat i poplatky za transakce.

#### d) Finanční ukazatele

Hlavní cílem fundamentální je zjištění skutečné kvantitativní hodnoty ze strany investora. Investor musí být seznámen s obchodními podmínkami daného aktiva včetně likvidity kryptoměny, okolních faktorů a odezvy celého trhu. Toto vše ukazuje důležitost fundamentální analýzy, obzvláště před vytvořením investičního plánu.

##### – Tržní kapitalizace

Tento ukazatel vyjadřuje celkovou hodnotu sítě. Vypočítat jí lze vynásobením hodnoty jedné mince s celkovým množstvím mincí v oběhu. U tohoto ukazatele je také nutné zjišťovat další faktory, a to hlavně likviditu. Investoři se často obecně domnívají, že kryptoměny s nižší tržní hodnotou mají vyšší potenciál růstu, ale ve většině případů tomu tak není, jelikož daná kryptoměna nemá žádné výhody oproti konkurenci. Vyšší tržní kapitalizace naopak poukazují na lepší infrastrukturu sítě a její celkovou sílu. Výpočet tržní kapitalizace nelze však přesně určit, jelikož se neberou v potaz všechny faktory, které jí mohou ovlivnit, například zapomenuté peněženky nebo ztracené klíče k nim.

##### – Likvidita

Likvidita nám určuje rychlost nákupu a prodeje aktiva. Pokud tedy můžeme kryptoměnu rychle nakoupit a následně rychle prodat, tak to poukazuje a na silnou likviditu. Likvidní kryptoměna má spoustu kupujících a prodávajících, kteří čekají, než se jejich obchod uskuteční.

Toto snižuje rozdíly mezi nákupní a prodejní cenou nabídek, které jsou zadané v takzvané Bid-Ask-Spread tabulce.

- Objem obchodů

Tento termín určuje množství obchodů uzavřených v daném časovém okně. Indikátor tohoto typu nám může být přínosný ke zjištění toho, jakou má daná kryptoměna schopnost držet setrvačnost neboli momentum. Konkrétně zjišťujeme, kolik jednotek je obchodováno na burze za určitý časový úsek. Pokud máme aktiva trend, který žene cenu nahoru, a objem obchodů je také na vysoké úrovni, tak se předpokládá, že cena poroste stále vzhůru. V případě, že cena aktiva má vysokou fluktuaci a objem obchodů je na nízké úrovni, tak se nedoporučuje investici provést, jelikož není dostatečně určený směr ceny aktiva.

- Obíhající zásoba mincí

Obíhající zásoba mincí nám určuje celkové množství mincí v oběhu, které v aktivní nabídce přistupné obecné veřejnosti. Tato zásoba je rozdílná od celkové zásoby mincí zejména díky tomu, že počet cirkulujících mincí se může v průběhu času zvyšovat nebo snižovat. Zvyšování může nastat v případě, že je vývojáři počet mincí navýšen centralizovaným přidáním. Pokud se kryptoměna dá těžit, tak také znamená, že se následně zvyšuje celková nabídka. Snižování počtu mincí může nastat v případě, že se mince spálí. Tento proces probíhá tak, že uživatelé posílají mince do speciální peněženky, která může mince pouze přijímat a nelze jí používat pro transakce. Koncept tohoto typu můžeme naleznout i u klasických akcií společností. V tomto případě k tomuto procesu dochází tak, že společnost, jenž akcie emituje, zpětně akcie vykoupí od akcionářů.

#### e) Projekční ukazatele

Pokud chceme výhledově zjistit potenciál kryptoměny, tak je k tomuto účelu ideální použít následující ukazatele. Zjišťujeme s nimi zejména vnitřní a vnější faktory pro úspěch u kryptoměny. Jedná se zejména o účel kryptoměny a jak její projekt funguje.

- Analýza pozadí projektu

Při této analýze zjišťujeme co nejvíce informací o lidech, kteří za projektem stojí. Spousta kryptoměn má oficiální stránky, na kterých mají uvedený jednotlivé členy projektu. Jednotlivé úspěchy a předešlé zkušenosti členů týmu dokážou pomoci v tom, nakolik moc má kryptoměna potenciál k úspěchu. Na stránkách kryptoměny lze také naleznout mapy budoucích

aktualizací, které naznačují směr, kterým se kryptoměna bude v následujících měsících i letech ubírat. Také je vhodné si najít rané podporovatele a poradce projektu, abychom byla zjištěna následná důvěryhodnost projektu.

– Porovnání konkurence

Konkurence je ve světě kryptoměn velice vysoká a je tedy třeba hledat konkrétní konkurenty dané kryptoměny ke zjištění výhod a nevýhod.<sup>34</sup>

---

<sup>34</sup> How to Analyze a Cryptocurrency Using Fundamental Analysis. <https://learn.bybit.com/> [online]. 2021 [cit. 2023-01-25]. Dostupné z: <https://learn.bybit.com/investing/how-to-analyze-a-cryptocurrency-using-fundamental-analysis/>

## **5 Vlastní práce**

V praktické části bude provedena fundamentální a technická vybraných kryptoměn. Fundamentální analýza se bude zabývat vizí jednotlivých projektů, konkrétním uplatněním a obliby ze strany široké komunity.

Při vytvoření technické analýzy bude vytvořen graf určující poslední rok jednotlivých kryptoměn, jelikož vytváření delší časové řady by bylo složité kvůli volatilitě kryptoměn a následné zavedení do grafu by bylo komplikované. Dojde tedy ke zjištění potencionálního vývoje v příštích měsících pomocí RSI, SMI a Fibonnaciho retracementu. Zpracování grafů technické analýze bude probíhat v platformě Etoro, která je uživatelsky velice přívětivá a vytváření jednotlivých ukazatelů je intuitivní a jednoduché.

V poslední řadě dojde k porovnání diverzifikace tokenů kryptoměn zjištěním množství peněženek.

### **5.1 Technická analýza vybraných kryptoměn**

#### **5.1.1 Technická analýza bitcoinu**

V posledním roce zažil trh kryptoměn úpadek vyvolaný různými společenskými faktory. Mezi hlavní podněty recese v oblasti kryptoměn patří válka na Ukrajině a stále se zvyšující ceny elektřiny, které mají obzvlášť negativní dopad na kryptoměny, jež jsou postavené na systému Proof of work. V listopadu roku 2021 došlo u Bitcoin k dosažení historického maxima, které činilo 68,789.63 dolarů za jednu minci, což v přepočtu bylo 1,694,219.80 korun. Aktuálně se hodnota mince Bitcoinu pohybuje okolo 20,000 dolarů za minci To znamená propad na méně než třetinu hodnoty z loňského listopadu.

Obrázek 2 Graf ceny Bitcoinu – denní graf



Zdroj: etoro.com (2022)

Dle obrázku č. 2 se trh aktuálně nachází v klesajícím směru, jelikož SMA 50 i 200 se nachází nad aktuální cenou. Trh si nyní hledá dno, díky kterému se následně vytvoří support Bitcoinu. Z grafu můžeme vyčíst, že support se nachází v oblasti 20,000 dolarů, což by odpovídalo nejvyšším hodnotám Bitcoinu z konce roku 2018, kdy došlo k velkému zvýšení povědomí o kryptoměnách. V roce 2018 byly tedy kryptoměny na historickém maximu díky investicím široké veřejnosti, která se kryptoměny viděla jako investice bez hlubšího pochopení. Pro investora je nyní ideální počkat na konkrétní pohyb trhu který upřesní následující směr. Prozatím se cena Bitcoinu příliš nemění, a proto lze zjišťovat následující cenové hladiny pouze krátkodobě. Delší investiční výhled není rozhodnut. Podle sledování SMA 50 a 200 lze očekávat, že v případě protnutí těchto ukazatelů dojde ke změnu směru a Bitcoin by se následně měl ocitnout v býčím trhu. Přidáním RSI a Fibonnaciho retracementu nám graf určuje další možné cenové hladiny, které by Bitcoin v dalším potencionálním býčím trhu mohl dosáhnout. V Případě protnutí SMA 50 a 200 lze očekávat dlouhodobý posun k hodnotám 38,000 dolarů, které určují 38,2 % Fibonnaciho retracementu. V těchto hodnotách by pak následně došlo k otestování rezistencí z února a března roku 2022, kdy se cena Bitcoinu pohybovala v těchto hladinách. Podle RSI ukazatele, který vyobrazen pod grafem, se cena aktuálně pohybuje okolo

60 bodů. Z toho lze usoudit že v případě překročení 70 bodů dojde k pře nakoupenému trhu. Může tedy nastat to, že cena po překročení klesne. Pokud však RSI bude nad 70 body a cena Bitcoinu poroste, tak to bude znamení silného býčího trhu.

Obrázek 3 Graf ceny Bitcoinu – čtyřhodinový graf



Zdroj: etoro.com (2022)

Následný obrázek č. 3 Bitcoinu je zobrazen v kratším časovém úseku, a to konkrétně na čtyřhodinovém úseku, kde každá svíce představuje průběh čtyř hodin. Na základě Fibonnaciho retracementu je vidět, že trh na procentuální hladiny ukazatele reaguje. Na konci října došlo již dvakrát k otestování resistance v procentuální hladině 38,2 % a v obou případech došlo k odmítnutí průniku na vyšší cenové hladiny. To vypovídá o nejistotě trhu, který vůči Bitcoinu stále pesimistický. SMA 50 a 200 také neindikují směr, jelikož jsou obě křivky v podobných hodnotách, a to jen více podporuje nejistotu v investici. RSI se sice nachází v hodnotách, kdy je Bitcoin brán jako přeprodán, ale tento ukazatel je poměrně nepřesný, když trh nemá rozhodnutý směr a nelze to tedy brát jako signál pro nákup.

Shrnutí technické analýzy Bitcoinu tedy naznačuje, že není vhodné aktuálně provádět investice do této kryptoměny z důvodu nepřesného směru.

## 5.1.2 Technická analýza Etheru

Obrázek 4 Graf ceny Etheru – denní graf



Zdroj: etoro.com (2022)

Při pohledu na obrázek č.4 Etheru lze vidět, že směr grafu je velice podobný jako u Bitcoinu. Je to dáno tím, že ceny kryptoměn jsou silně korelované. Jsou zde však rozdíly, které se týkají posledních pár měsíců. Ether se dostal na svoje maximum v listopadu 2021, kdy se jeho cena zastavila na 4891.7 dolarech. Aktuálně se obchoduje v rozmezí 1,500 až 1,600 dolarů. Minimum roku 2022 bylo dosaženo 18. července, kdy hodnota byla 896.11 dolarů. Je tedy nutné podotknout, že Ether má mnohem větší volatilitu než Bitcoin. Vývoj SMA 50 a 200 naznačuje, že se u této kryptoměny nastává pravděpodobnější scénář na býčí trh, než je tomu u Bitcoinu. SMA 50 již protнула cenový graf a nyní se čeká, jestli to samé provede i SMA 200. Pokud se však cena pouze odrazí od křivky SMA 200, tak nastane korekce ceny v podobě vrácení ceny zpět k hranici 1000 dolarů, kde si Ether vytvořilo support. Fibonacciho retracement nám určuje nejbližší resistenci býčího trhu, která se nachází v hodnotě 2,500 dolarů.



Obrázek 5 Graf ceny Etheru – čtyřhodinový graf



Zdroj: etoro.com (2022)

Závěrem technické analýzy podotknout, že Ether prochází velmi podobnými cykly jako Bitcoin ale za cenu větší volatility. To z něho dělá rizikovější aktivum a je třeba vykonat podrobnější technickou analýzu. Ether však získává větší impuls pro býčí trh než Bitcoin.

### 5.1.3 Technická analýza Cardana

Cardano je mnohem mladší kryptoměna než Bitcoin a Ether, a proto je v jeho případě volatility na mnohem větší úrovni. Vlastnění Cardana tedy může být pro mnohé investory více lákavé, protože možný zisk je vyšší ale stejně je tomu i u možné ztráty.

Obrázek 6 Graf ceny Cardana – denní graf



Zdroj: etoro.com (2022)

Po shlédnutí obrázku č. 6 lze pozorovat, že je mezi nejvyšší cenou Cardana, které kryptoměna dosáhla v září 2021, a cenou aktuální téměř rozdíl desetinásobné hodnoty. To vypovídá o silném medvědímu trhu, což vede trh k tlačení cen kryptoměn na dvouleté minimum. Při využití SMA 50 a 200 lze však pozorovat, že se oba ukazatele stále přibližují, což může vést ke změně trendu. Toho by mělo dosaženo při protnutí ukazatelů. Nadále by se cena měla ustalovat, ale rozhodně to není automaticky bráno jako předpoklad pro začátek býčího trhu. RSI se aktuálně udržuje na 50 bodech, což taky vyjadřuje nepřesný pohyb trhu. Pokud by však RSI byl aktuálně na nižších hodnotách, tak by to mohlo být bráno jako dobrý signál pro nákup po protnutí SMA 50 a 200. Fibonacci zde aktuálně nemá výrazné využití, jelikož nejbližší hodnota 38,2 % se nachází velmi vysoko a Cardano se k této hodnotě může přiblížit až bude směr vývoje možně jasně určit.

Obrázek 7 Graf ceny Cardana – čtyřhodinový graf



Zdroj: etoro.com (2022)

Po využití čtyřhodinového grafu u obrázku č. 7 lze mnohem lépe rozpoznat aktuální směr trhu. Dlouhodobý směr je stále medvědí, a ještě nedošlo k vytvoření silného supportu, od kterého by se cena mohla odrazit. U ukazatele SMA 50 a 200 došlo sice k protnutí, což většinou naznačuje změnu trendu, a to lze označit jen za krátkodobou změnu směru. RSI je stejně jako u denního grafu nerozhodný a rozhodně nedává podnět k možné investici. Fibonnaci nám však dává mnohem víc informací. Dle tohoto ukazatele došlo v druhé části října již dvakrát k otestování resistance v hodnotě 38,2 %. Lze tedy očekávat další otestování resistance této hodnoty. Pokud dojde posunu směrem vzhůru, tak se bude testovat další resistance na hodnotě 50 %. Může ale i nastat scénář, že bude hodnota 38,2 % znovu odmítnuta, a to povede k opětovnému posunu dolů, kde se bude testovat support 0 %.

Shrnutím technické analýzy Cardana nelze určit přesný směr pohybu, a proto není vhodná investice.

### 5.1.4 Technická analýza Polkadotu

Polkadot je brán jako více riziková kryptoměna, protože se stále ještě dostává do povědomí investorů, stejně jako je tomu u Cardana. Z tohoto důvodu je jeho volatilita také na vyšší úrovni, a to činí u potenciálního investora větší zájem o investici ale zároveň větší strach z možné ztráty.

Obrázek 8 Graf ceny polkadotu – denní graf



Zdroj: etoro.com (2022)

Graf Polkadotu u obrázku č. 8 je velice podobný jako u Cardana. Obě tyto kryptoměny jsou v dlouhodobém medvědí trendu. Polkadot se však pohyboval v rekordních hodnotách průběhem listopadu, stejně tomu bylo u Bitcoinu. Všechny kryptoměny na náladu trhu odpovídají podobnými průběhy.

SMA 50 a 200 vypovídá o nepřetržitém medvědí trhu celým průběhem letošního roku. Tyto hodnoty se však vzájemně přibližují, což může značit brzkou změnu trendu. RSI je na úrovni 53 bodů, a to také nijak neurčuje překoupení nebo přeprodání trhu. Fibonnaci zde je

nevýznamný ukazatel, jelikož z důvodu volatility Polkadotu by nejbližší dlouhodobá resistance vznikla až v hodnotě 38,2 %, která byla dosažena v dubnu 2022.

Obrázek 9 Graf ceny Polkadotu – čtyřhodinový graf



Zdroj: etoro.com (2022)

Za pomoci čtyřhodinového časového průběhu vývoje ceny Polkadotu u obrázku č. 9 lze lépe vidět aktuální směr. Polkadot byl poslední dva měsíce v medvědím trhu ale došlo v říjnu k většímu ustálení ceny. U SMA 50 a 200 došlo začátkem listopadu k protnutí. To může značit změnu směru, ale také může jít jen o krátkodobý posun vzhůru. RSI je opět neutrální, a tedy nelze na jeho aktuální pozici určit směr. Fibonnaci nám udává nejbližší výrazný bod resistance v hodnotě 38,2 %. Polkadot však aktuálně nemá dostatečný momentum aby se v blízké době této hodnoty posunul.

Shrnutím technické analýzy Polkadotu pomocí denního grafu nelze předpokládat obrácení trendu v nejbližší době. Čtyřhodinový graf však vypadá nadějněji a pokud dojde k opětovnému odrazu od supportu na Fibonnaciho úrovni 0 %, tak se je možné investici provést ale kryptoměna si musí získat silné momentum směrem vzhůru.

## 5.2 Fundamentální analýza vybraných kryptoměn

### 5.2.1 Fundamentální analýza Bitcoinu

Bitcoin sdílí většinu fundamentálních věcí s ostatními kryptoměnami, a to vede k tomu, že pohyb cen u kryptoměn probíhá velice podobně. Hlavní rozdíl tkví v typu konsensu, objemu obchodů a poplatcích za transakce na síti kryptoměny. V případě Bitcoinu je konsensu dosaženo pomocí Proof of work. Tím se odlišuje od Etheru, Cardana a Polkadotu. U Bitcoinu je hashrate aktuálně 237,42 eh/s. Eh nese označení pro exahashe. Jeden exahash představuje 10000000000000000000 hashů.<sup>35</sup>

---

<sup>35</sup> *Bitcoin Hashrate Chart* [online]. [cit. 2023-02-01]. Dostupné z: <https://www.coinwarz.com/mining/bitcoin/hashrate-chart>

Obrázek 10 Vývoj těžebního výkonu Bitcoinu v grafu



Zdroj: coinwarz.com (2022)

U obrázku č.10 lze pozorovat vývoj výpočetního výkonu blockchainu Bitcoinu. Největší výkyv ve výkonu nastal v květnu roku 2021. Tento významný pokles těžby nastal z důvodu zakázání těžby kryptoměn v Číně. Nicméně i přes toto omezení se ve zbytku hashrate zvyšoval a v na konci roku 2021 byl opět na květnových hodnotách. Nadále dochází k jeho zvyšování, a to i přes rostoucí ceny energií s tím spjaté. Tento vývoj je pro Bitcoin příznivá zpráva, ale pro společnost je to spíše nežádoucí.<sup>36</sup>

Kapitalizace Bitcoinu je aktuálně 318 miliard dolarů. Z celkové zásoby 21 miliónů mincí je v oběhu 19 218 381 mincí. Z toho 1 milión mincí vlastní zakladatel Satoshi Nakamoto.

---

<sup>36</sup> WOLF, Karel. Kolikrát ještě Čína zakáže bitcoin? A co si z toho vzít? <https://forbes.cz/> [online]. 2021 [cit. 2023-01-25]. Dostupné z: <https://forbes.cz/kolikrat-jeste-cina-zakaze-bitcoin-a-co-si-z-toho-vzit/>

Z toho tedy vychází, že zbývá vytěžit necelých 750 000 Bitcoinů, než dojde k zastavení těžby. Průměrná doba držení Bitcoinu uživateli je 142 dní.<sup>37</sup>

Z fundamentální analýzy Bitcoin nenabízí tedy nic jiného než alternativu k aktuálním platbám.

## 5.2.2 Fundamentální analýza Etheru

Ether má pro svůj potencionální růst větší předpoklad než Bitcoin, jenž je tak rozšířený a veřejně známý z důvodu, že se jedná o první kryptoměnu. Ether má však velkou výhodu v přidané vrstvě chytrých kontraktů.

Po stránce výkonu celé sítě je hashrate na zlomku hodnoty z důvodu přechodu na Proof of stake systém.

Obrázek 11 Vývoj těžebního výkonu Etheru v grafu



Zdroj: coinwarz.com (2022)

<sup>37</sup> Bitcoin market cap [online]. [cit. 2023-02-01]. Dostupné z: <https://coinmarketcap.com/currencies/bitcoin/>



Z obrázku č. 11 je zřejmé, že celý přechod významně ovlivnil těžbu. Ta však není na nulových hodnotách, jelikož má Ether ještě další vrstvu, která se nazývá Ether classic. Ten stále využívá systém Proof of work. Aktuální hashrate Etheru je 390 MH/s. Před přechodem na Proof of stake hashrate Etheru dosáhl 1,25 PH/s, což je více než tři milion násobek aktuálního výkonu sítě.

Kapitalizace Etheru je 143,4 miliardy dolarů při aktuální ceně 1215 dolarů. V oběhu je 122,4 miliónů mincí, ale celkový počet mincí není daný, takže v budoucnosti mohou další mince do oběhu přibýt. To, kolik jich následně bude přidáno záleží čistě na vývojářích. Průměrná doba držení Etheru v krypto peněžence je 118 dní.<sup>38</sup>

Využití Etheru má v budoucnu velký potenciál za předpokladu, že dojde k širšímu přijetí veřejností.

### 5.2.3 Fundamentální analýza Cardana

Kapitalizace Cardana je 10,8 miliardy dolarů při ceně 0,31 dolarů za mince, a to z ní dělá sedmou nejhodnotnější kryptoměnu. Celkově je v oběhu 34,4 miliardy mincí. Z pohledu investorů je ale více důvěryhodná, jelikož průměrná doba držení této kryptoměny je 181 dní.<sup>39</sup>

Cardano je po stránce reálného využití stále v rané fázi, avšak již probíhá implementace do školních systémů v Etiopii. Díky Cardanu by celý systém školství v této zemi měl přejít na identifikační systém studentů a učitelů pomocí blockchainu Ouroboros. Cíl projektu je poskytnout identifikační karty pro 5 miliónů studentů a 750 000 profesorů v celé zemi. Ouroboros pomůže ověřovat udělované známky a podle toho budou vyhodnocovány studijní výsledky.<sup>40</sup>

Dále Cardano našlo využití i v ověřování originálního původu obuvi, a to sice u značky New Balance. Vše funguje tak, že zákazník načte QR kód na obuvi a tím dojde k zařazení

---

<sup>38</sup> *Ethereum market cap* [online]. [cit. 2023-02-01]. Dostupné z: <https://coinmarketcap.com/currencies/ethereum/>

<sup>39</sup> *Cardano market cap* [online]. [cit. 2023-02-01]. Dostupné z: <https://coinmarketcap.com/currencies/cardano/>

<sup>40</sup> SIROIS, Alex. Cardano Is Already Demonstrating Real-World Utility. *Https://www.nasdaq.com/* [online]. 2021 [cit. 2023-01-25]. Dostupné z: <https://www.nasdaq.com/articles/cardano-is-already-demonstrating-real-world-utility-2021-05-05>

konkrétního páru bot do blockchainu. Tento systém snižuje šíření padělků, jelikož i při nákupu od třetí strany si konečný zákazník může ověřit, že daný pár bot je opravdu originální. To činí velký krok pro globální značky, maloobchodní prodejny i finální zákazníky a zvyšuje důvěryhodnost produktu.<sup>41</sup>

#### 5.2.4 Fundamentální analýza Polkadotu

Polkadot má povědomí u menšího množství než Cardano, Ether anebo Bitcoin. To má vliv na jeho kapitalizaci, která činí 6,3 miliardy dolarů při aktuální hodnotě 5,55 dolarů za minci. To ho řadí až na deváté místo v krypto světě. Celkově je tedy v oběhu 1,1 miliardy mincí. Denní objem obchodů je aktuálně 197,3 miliónu dolarů a typická doba držení uživateli dosahuje 131 dní.<sup>42</sup>

Budoucnost tohoto projektu bude zajímavá. Polkadot je dnes pro klasického uživatele, který dopodrobna nemá síť nastudovanou, velice komplikovaná kryptoměna. V budoucnu by měl Polkadot získat větší přízeň veřejnosti, protože se nemá snahu být nejlepší kryptoměnou ale systémem, který umožní všem blockchainům ostatních kryptoměn mezi sebou spolupracovat. Po stránce vývojářů a komunity celého projektu je na tom Polkadot velice dobře. V komunitě se už mluví nástupci v podobě Polkadot 2.0, ale to zatím vyvolává více otázek než odpovědí. Až tento projekt dojde do fáze, kdy uživatel bude využívat benefitů blockchainu, bez toho, aniž by si uvědomoval, že ho využívá, tak bude jeho popularita značně zvýšená.

### 5.3 Decentralizace jednotlivých kryptoměn

Decentralizace bude určena množstvím peněženek Bitcoinu, Etheru, Cardana a Polkadotu. Samotná decentralizace však nemůže být určena přesně, jelikož jeden subjekt může vlastnit neomezené množství peněženek. Dále také dochází k nákupů mincí prostřednictvím burz, kde však uživatel danou kryptoměnu nepřímo vlastní ale mince nejsou obsaženy přímo

---

<sup>41</sup> PHILLIPS, Daniel. New Balance to Use Cardano Technology to Fight Counterfeits. <https://beincrypto.com/> [online]. 2019 [cit. 2023-01-31]. Dostupné z: <https://beincrypto.com/new-balance-to-use-cardano-technology-to-fight-counterfeits/>

<sup>42</sup> Polkadot market cap [online]. [cit. 2023-02-01]. Dostupné z: <https://coinmarketcap.com/currencies/polkadot-new/>

v peněžence uživatele. Množství těchto uživatelů také nelze zjistit, jelikož existuje nespočet burz na prodej kryptoměn.

Bitcoin má vysokou míru decentralizace. Počet adres, které obsahují bitcoiny aspoň za 1 dolar je zhruba 55 000 000. Z toho je 2045 adres, které obsahují minimálně 1000 bitcoinů.

Právě těchto 2045 adres vlastní dohromady téměř 40 % Bitcoinu. Prvních 100 největších adres obsahuje dohromady 15,3 % celkové objemu mincí. Adresa s největším množstvím mincí ukrývá celkově 250 597 mincí, a to představuje 1,3 % celkového množství mincí. Jedná se o jedinou peněženku, ve které je uloženo více než 1 % bitcoinů.<sup>43</sup>

U Etheru existuje okolo 66 000 000 peněženek s mincemi za aspoň 1 dolar. Prvních 100 největších peněženek vlastní dohromady 38,8 % mincí z celkové zásoby etheru. Ether peněženek, které obsahují aspoň 1 % celkového obsahu mincí, je 6. Z toho však ani jedna není vlastněna konkrétním majitelem, jelikož se jedná o peněženky různých kryptoburz, hlavně tedy Binance. Největší soukromě vlastněná peněženka obsahuje 347 300 mincí etheru, což představuje 0,228 % celkového obsahu. Podle toho lze říct, že ether je více vlastněn obchodními a investičními společnostmi, které mají na jeho cenu větší vliv.<sup>44</sup>

V případě Cardana má decentralizace nejvyšší míru z uvedených kryptoměn. Držitelů Cardano je v poměru k Bitcoinu a Etheru mnohem méně, a to sice 3 500 000. Deset nejbohatších peněženek přitom vlastní pouze 6,7 % celkové zásoby kryptoměny. Prvních 100 největších peněženek vlastní pouze 19 % Cardana. To vypovídá o tom, že naprostá většina mincí je držena komunitou uživatelů, a ne velkými společnostmi.<sup>45</sup>

Polkadot je na tom po stránce decentralizace nejhůře. Dohromady je zde 1 052 857 držitelů. Prvních 10 největších držitelů vlastní 28,09 % celkového obsahu mincí. Prvních 100 peněženek dokonce obsahuje 76,23 % mincí v oběhu.<sup>46</sup>

---

<sup>43</sup> *Bitcoin rich list* [online]. [cit. 2023-02-01]. Dostupné z: <https://bitinfocharts.com/top-100-richest-bitcoin-addresses.html>

<sup>44</sup> *Ethereum rich list* [online]. [cit. 2023-02-01]. Dostupné z: <https://bitinfocharts.com/top-100-richest-ethereum-addresses.html>

<sup>45</sup> *Cardano rich list* [online]. [cit. 2023-02-01]. Dostupné z: <https://www.coinarp.com/currencies/cardano/richlist/>

<sup>46</sup> *Polkadot rich list* [online]. [cit. 2023-02-01]. Dostupné z: <https://www.coinarp.com/currencies/polkadot100/richlist/>

To z něho dělá možný cíl na pump and dump metodu, která je ve světě kryptoměn poměrně normální a týká se především kryptoměn, které jsou majoritně vlastněny malou skupinou lidí. Při ní velcí investoři nakoupí velké množství dané mince. Následně vydají zprávu veřejnosti, která pozitivně mluví o daném aktivu. To vede ke zvýšení pozornosti a ostatní drobní investoři mají domněnku, že cena poroste. Po vyhnání ceny nahoru velcí investoři své mince prodají se ziskem, a to vede k propadu ceny směrem dolů. Velcí investoři vydělají ale drobní investoři na tom prodělají.

## 5.4 Poměření výhod a nevýhod jednotlivých kryptoměn

Když dojde na srovnání těchto 4 kryptoměn, tak všechny jsou velice zajímavé projekty, které je díky tomu řadí mezi nejvíce populární kryptoměny na trhu.

Bitcoin má nejširší povědomí veřejnosti, a to z něho dělá nejvíce konzervativní kryptoměnu. Bohužel však nenabízí žádnou přidanou hodnotu pro investora. Technická analýza naznačuje, že Bitcoin stále hledá svůj silný support, od kterého by se mohl odrazit. Hodnotu pro uživatele má pouze z hlediska decentralizace. V budoucnu lze předpokládat, že Bitcoin předběhnou mladší kryptoměny, které nabízí i spoustu využití v reálném světě, a nejen jako uchovatel hodnoty proti inflaci a centrálním orgánům.

Ether má v budoucnosti vysoký potenciál úspěchu, o čemž vypovídá také dobrá technická analýza, která je pro Ether nejlépe vypadající ze všech zkoumaných kryptoměn. Po stránce decentralizace je na tom však Ether hůře, protože je vysoký počet mincí koncentrován ve velkých institucích.

Cardano má také vysoký potenciál úspěchu, díky výtečným vlastnostem a velké množství je koncentrováno v komunitě uživatelů a vývojářů. Bohužel technická analýza nenaznačuje růst v nejbližší době. Další nevýhoda také stojí na tom, že vývojáři mají u Cardana často zpoždění s novými aktualizacemi, a to snižuje důvěryhodnost mezi uživateli.

Polkadot, jakožto nejmladší ze zkoumaných kryptoměn, má skutečné vysoké cíle, ale zatím jen čas rozhodne, jestli dojde k využití v reálném světě. Tato kryptoměna může mít větší tendence k cenovým výchýlkám z důvodu nízké decentralizace.

## 5 Závěr

Tématem bakalářské práce bylo poměření výkonnosti kryptoměn pomocí technické a fundamentální analýzy. V teoretické části byl uveden vývoj měn od vzniku měnového systému po vytvoření alternativ pro klasický monetární systém. Následně byly vysvětleny základní pojmy týkající se kryptoměn a jejich fungování. Dále byla vysvětlena technická a fundamentální analýza kryptoměn pro lepší určení reálné hodnoty jednotlivých kryptoměn a jejich potencionální růst. Praktická část se zabývala technickou a fundamentální analýzou vybraných kryptoměn. Technická analýza byla provedena v časovém rozmezí od 30. 11. 2021 do 30. 11. 2022 pomocí ukazatelů SMA, RSI a Fibonnaciho retracementu. Fundamentální analýza se zabývala výhodami a nevýhodami jednotlivých kryptoměn a jejich potencionálního využití v budoucnu.

Hlavním cílem práce bylo poměření vybraných kryptoměn ze strany jejich výkonnosti. Bitcoin má ze všech kryptoměn největší kapitalizace díky tomu, že je nejvíce znám širokým publikem a má nejdelší působnost. Ze strany potencionálního využití v budoucnu ale na ostatní kryptoměny ztrácí, jelikož ho lze použít pouze k transakcím na jeho blockchainu. Ether má lepší předpoklady, protože má spoustu možností využití, a navíc díky přechodu na Proof of stake má minimální náročnost na těžbu. To z něj dělá mnohem více environmentálně a ekonomicky příhodnější alternativu. Je zde však zvýšená volatilita, která by mohla odradit konzervativnější investory. Cardano má v budoucnu největší potenciál na úspěch díky silné komunitě a připravenosti celé sítě na budoucí využití. Polkadot má také vysoké předpoklady úspěchu, ale jedná se o nejvíce volatilní kryptoměnu, což z investorské perspektivy není moc vhodná věc.

Kryptoměny jsou oproti klasickým fiat měnám velice mladá technologie. Díky digitalizace celého bankovního systému zaznamenaly za deset let své existence velký příliv investic v podání drobných investorů ale i velkých institucí. Volatilita je u nich na vysoké úrovni, protože panuje neustála nejistota o jejich vývoji. Jen samotný Bitcoin ztratil za rok 2022 okolo 60 % hodnoty, a to je jedná kryptoměnu, která ztratila za daný rok nejmenší množství hodnoty. Cyklus kryptoměn se však neustále opakuje, jelikož Bitcoin zaznamenal za celou svoji životnost již několikrát takovou roční ztrátu. I přesto však Bitcoin zaznamenal zhodnocení více než 30 000 % za dobu své existence. Největším překážkou v budoucnu i v současné pro

kryptoměny jsou regulace ze stran státních orgánů. Potenciál využití kryptoměn ve světě je široký ale i přes to panuje obecný názor, že klasické měny jimi nikdy plně nahrazeny nebudou.

## Seznam použitých zdrojů

### Knižní zdroje

DAVIES, Glyn, 2002. *A history of money: From Ancient Times to the Present Day*. 3. Cardiff: UNIVERSITY OF WALES PRESS. ISBN 0-7083-1773-1.

STROUKAL, D. -- SKALICKÝ, J. *Bitcoin a jiné kryptopenize budoucnosti: historie, ekonomie a technologie kryptoměn, stručná příručka pro úplné začátečníky*. Praha: Grada Publishing, 2018. ISBN 978-80-271-0742

ANTONOPOULOS, A. M. *Mastering bitcoin: unlocking digital cryptocurrencies*. Sebastopol, CA: O'Reilly, 2015. ISBN 978-1-449-37404-4

GRAHAM, B. -- ZWEIG, J. *Inteligentní investor*. Praha: Grada, 2007. ISBN 978-80-247-1792-0.

SHEIKH, Husneara, Rahima Meer AZMATHULLAH a Faiza RIZWAN, 2018. *Proof-of-Work Vs Proof-of-Stake: A Comparative Analysis and an Approach to Blockchain Consensus Mechanism* [online]. 6. [cit. 2023-01-31]. ISBN 23219653.

HOMMA, Munehisa, 2022. *The Candlestick Bible* [online]. Lulu [cit. 2023-01-31]. ISBN 9781458313843.

HAYDEN, John, 2004. *RSI: The Complete Guide*. Wasendorf & Associates. ISBN 0934380880.

BORODEN, Carolyn, 2008. *Fibonacci Trading: How to Master the Time and Price Advantage*. ISBN 9780071498159.

PRITZKER, Yan, 2020. *Vynález jménem Bitcoin*. Braiins Publishing. ISBN 978-80-907975-0-5.

### Elektronické zdroje

KAGAN, Julia. Ecash. <https://www.investopedia.com/> [online]. 31.3.2021 [cit. 2023-01-31]. Dostupné z: <https://www.investopedia.com/terms/e/ecash.asp#:~:text=pioneer%20in%20cryptocurrency,-eCash%20was%20created%20by%20Dr.,link%20withdrawal%20and%20spend%20transacti> ons.

HARTINGEROVÁ, Emma. Kryptoměny-Definice a vlastnosti. *Https://www.itnetwork.cz* [online]. [cit. 2023-01-30]. Dostupné z: <https://www.itnetwork.cz/kryptomeny/zaklady-kryptomen/>

WON, Daniel. Token vs. Coin – Simple Explanation. *Https://www.exodus.com/* [online]. 2020 [cit. 2023-01-25]. Dostupné z: <https://www.exodus.com/news/token-vs-coin/>

KERNER, Sean. Crypto wallet (cryptocurrency wallet). *Https://www.techtarget.com* [online]. [cit. 2023-01-30]. Dostupné z: <https://www.techtarget.com/searchsecurity/definition/crypto-wallet-cryptocurrency-wallet>

*Ledger Nano X* [online]. [cit. 2023-01-30]. Dostupné z: <https://shop.ledger.com/pages/ledger-nano-x>

KAVANAGH, Robin. Hash rate: A measure of the computing power on a cryptocurrency network that is a key security indicator. *Https://www.businessinsider.com* [online]. 2022 [cit. 2023-01-30]. Dostupné z: <https://www.businessinsider.com/personal-finance/hash-rate>

ALYOSHKIN, Roman. *Https://polys.vote/* [online]. 2017 [cit. 2023-01-30]. Dostupné z: <https://polys.vote/blog/blockchain-2>

NAVEEN, Joshi, 2021. EVERYTHING YOU NEED TO KNOW ABOUT BLOCKCHAIN 3.0. *Https://www.bbntimes.com* [online]. 2021 [cit. 2023-01-30]. Dostupné z: <https://www.bbntimes.com/technology/everything-you-need-to-know-about-blockchain-3-0>

BONHEUR, Kristoffer. PoW: Advantages and Disadvantages of Proof-of-Work. *Https://www.profolus.com/* [online]. 15.9.2021 [cit. 2023-01-31]. Dostupné z: <https://www.profolus.com/topics/pow-advantages-and-disadvantages-of-proof-of-work/>

RANKENFIELD, Jake. 51 % Attack: Definition, Who Is At Risk, Example, and Cost. *Https://www.investopedia.com/* [online]. 28.9.2022 [cit. 2023-01-31]. Dostupné z: <https://www.investopedia.com/terms/1/51-attack.asp>

SMITH, Corwin, ed. PROOF-OF-STAKE (POS). *Https://ethereum.org/* [online]. 12.1.2023 [cit. 2023-01-25]. Dostupné z: <https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/#:-:text=One%20validator%20is%20randomly%20selected,of%20the%20block%20being%20proposed.>

*Smart Contracts* [online], 2023. [cit. 2023-01-31]. Dostupné z: <https://ethereum.org/en/smart-contracts/>



What Is a Cryptocurrency Whitepaper?. <https://academy.binance.com/> [online]. 31.10.2022 [cit. 2023-01-30]. Dostupné z: <https://academy.binance.com/en/articles/what-is-a-cryptocurrency-whitepaper>

Vitalik Buterin: The man who co-created Ethereum. <https://cointelegraph.com/> [online]. [cit. 2023-01-31]. Dostupné z: <https://cointelegraph.com/ethereum-for-beginners/who-is-vitalik-buterin>

MILLMAN, Rene, Stephen GRAVES a Liam KELLY. What Is Ethereum 2.0? Ethereum's Consensus Layer and Merge Explained. <https://decrypt.co/> [online]. 24.3.2022 [cit. 2023-01-31]. Dostupné z: <https://decrypt.co/resources/what-is-ethereum-2-0>

Polkadot — An Early In-Depth Analysis — Part One — Overview and Benefits, 2020. *Cryptoseq.medium.com* [online]. 9.9.2020 [cit. 2021-05-06]. Dostupné z: [/cryptoseq.medium.com/polkadot-an-early-in-depth-analysis-part-one-overview-and-benefits-ea16de17c05c](https://cryptoseq.medium.com/polkadot-an-early-in-depth-analysis-part-one-overview-and-benefits-ea16de17c05c)

*Cardano – Phases* [online]. [cit. 2023-01-31]. Dostupné z: <https://roadmap.cardano.org/en>

WORTH, Will, 2021. *Cardano Is Worth Considering for Its Utility and Strong Leadership* [online]. 7.4.2021 [cit. 2021-05-06]. Dostupné z: <https://investorplace.com/2021/04/cardano-is-worth-considering-for-its-utility-and-strong-leadership/>

VERMAAK, Werner, 2021. A Deep Dive Into Cardano. *Coinmarketcap.com* [online]. 18.1.2021 [cit. 2021-05-06]. Dostupné z: <https://coinmarketcap.com/alexandria/article/a-deep-dive-into-cardano>

Why use cardano. <https://docs.cardano.org> [online]. [cit. 2023-01-31]. Dostupné z: <https://docs.cardano.org/new-to-cardano/why-use-cardano>

WOOD, Gavin. POLKADOT: VISION FOR A HETEROGENEOUS MULTI-CHAIN FRAMEWORK. <https://polkadot.network> [online]. [cit. 2023-01-25]. Dostupné z: <https://polkadot.network/PolkaDotPaper.pdf>

How to Analyze a Cryptocurrency Using Fundamental Analysis. <https://learn.bybit.com/> [online]. 2021 [cit. 2023-01-25]. Dostupné z: <https://learn.bybit.com/investing/how-to-analyze-a-cryptocurrency-using-fundamental-analysis/>

FERNANDO, Jason. Moving Average (MA): Purpose, Uses, Formula, and Examples. *Https://www.investopedia.com* [online]. 2023 [cit. 2023-01-30]. Dostupné z: <https://www.investopedia.com/terms/m/movingaverage.asp>

*Bitcoin Hashrate Chart* [online]. [cit. 2023-02-01]. Dostupné z: <https://www.coinwarz.com/mining/bitcoin/hashrate-chart>

*Ethereum market cap* [online]. [cit. 2023-02-01]. Dostupné z: <https://coinmarketcap.com/currencies/ethereum/>

*Bitcoin market cap* [online]. [cit. 2023-02-01]. Dostupné z: <https://coinmarketcap.com/currencies/bitcoin/>

*Cardano market cap* [online]. [cit. 2023-02-01]. Dostupné z: <https://coinmarketcap.com/currencies/cardano/>

*Polkadot market cap* [online]. [cit. 2023-02-01]. Dostupné z: <https://coinmarketcap.com/currencies/polkadot-new/>

*Polkadot rich list* [online]. [cit. 2023-02-01]. Dostupné z: <https://www.coinarp.com/currencies/polkadot100/richlist/>

*Cardano rich list* [online]. [cit. 2023-02-01]. Dostupné z: <https://www.coinarp.com/currencies/cardano/richlist/>

*Ethereum rich list* [online]. [cit. 2023-02-01]. Dostupné z: <https://bitinfocharts.com/top-100-richest-ethereum-addresses.html>

*Bitcoin rich list* [online]. [cit. 2023-02-01]. Dostupné z: <https://bitinfocharts.com/top-100-richest-bitcoin-addresses.html>