

**Česká zemědělská univerzita v Praze**

**Provozně ekonomická fakulta**

**Katedra ekonomických teorií**



## **Bakalářská práce**

**Predikce vývoje a posouzení investičního potenciálu  
kryptoměny Bitcoin**

**Denis Kuzmyk**

**© 2024 ČZU v Praze**

## ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Denis Kuzmyk

Podnikání a administrativa

Název práce

**Predikce vývoje a posouzení investičního potenciálu kryptoměny Bitcoin**

Název anglicky

**Prediction of development and investment potential of Bitcoin**

---

### Cíle práce

Hlavním cílem této práce je určit, zda kryptoměna Bitcoin spíše vykazuje předpoklady aktiva s investičním růstovým potenciálem nebo efektivního prostředku vhodného pro směnu hodnot.

Dílním cílem je vytvoření návrhu pro uskutečňování směn, uchovávání a manipulaci s Bitcoinem, se zaměřením na praktické aspekty jeho užívání. Dalším dílním cílem je zhodnocení investičních strategií do kryptoměny Bitcoin, které reflektují individuální přístup investora vzhledem k časovému horizontu a očekávaných výnosů. Důraz je kladen na potřeby českých uživatelů, investorů a institucí, zohledňující možnosti a specifika českého trhu, poskytující relevantní informace v místním kontextu.

### Metodika

Teoretická část práce bude zpracována pomocí studia odborné literatury a dalších českých i zahraničních zdrojů věnujícím se dané problematice. Budou vysvětleny klíčové pojmy a souvislosti, které jsou důležité pro pochopení prostředků směny, investování a kryptoměn, zejména Bitcoinu, tak aby došlo k porozumění vývoje a role v oblasti investic a směny hodnot.

Na základě zpracování dostupných dat bude vypracována vlastní část práce. Využitím popisné metody s prvky komparace budou porovnány investiční strategie, které zohlední investora z hlediska přístupu vůči času. K určení, zda-li kryptoměna Bitcoin naplňuje předpoklady prostředku směn, bude využita komparace s tradičními fiat měnami nebo jinými formami majetku.

## Doporučený rozsah práce

30 – 40

## Klíčová slova

Aktiva, Bitcoin, Decentralizace, Digitální zlato, Investice, Krypto, Kryptoměny, Model, Spekulace

---

## Doporučené zdroje informací

- ANTONOPOULOS, Andreas M. Mastering Bitcoin [online]. 2nd EDITION. O'Reilly Media, 2017 [cit. 2022-05-02]. ISBN 978-1-4919-5438-6. Dostupné z: <https://github.com/bitcoinbook/bitcoinbook>
- NAKAMOTO, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System [online]. 2009 [cit. 2022-05-02]. Dostupné z: <https://bitcoin.org/en/>
- PRITZKER, Yan. Vynález jménem Bitcoin: Vznik a fungování prvních skutečně vzácných a decentralizovaných peněz [online]. Praha: Braiins Publishing, 2019 [cit. 2022-05-02]. ISBN 978-1-4919-5438-6. Dostupné z: [inventingbitcoin.com](https://inventingbitcoin.com)
- STROUKAL, Dominik a Jan SKALICKÝ. Bitcoin – Peníze budoucnosti: Historie a ekonomie kryptoměn, stručná příručka pro úplné začátečníky [online]. Praha: Ludwig von Mises Institut CZ&SK, 2015 [cit. 2022-05-02]. ISBN 978-80-87733-26-4. Dostupné z: <https://www.penizebudoucnosti.cz/>
- STROUKAL, D. – SKALICKÝ, J. Bitcoin a jiné kryptopeníze budoucnosti: historie, ekonomie a technologie kryptoměn. Praha: Grada Publishing, 2021. ISBN 978-80-271-1043-8
- TĚTEK, Josef. Bitcoin: Odluka peněz od státu [online]. Praha: Braiins Systems, 2021 [cit. 2022-05-02]. ISBN 978-80-907975-5-0. Dostupné z: <https://cs.braiins.com/blog/odluka-penez-od-statu-kniha-josef-tetek>

---

## Předběžný termín obhajoby

2023/24 LS – PEF

## Vedoucí práce

Ing. David Křížek, Ph.D.

## Garantující pracoviště

Katedra ekonomických teorií

Elektronicky schváleno dne 3. 2. 2024

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

Vedoucí katedry

Elektronicky schváleno dne 9. 2. 2024

**doc. Ing. Tomáš Šubrt, Ph.D.**

Děkan

V Praze dne 15. 03. 2024

## **Čestné prohlášení**

Prohlašuji, že svou bakalářskou práci "Predikce vývoje a posouzení investičního potenciálu kryptoměny Bitcoin" 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 15.3.2024

---

## **Poděkování**

Rád bych touto cestou poděkoval vedoucímu mé bakalářské práce Ing. Davidovi Křížkovi, PhD. za veškerou ochotu, vstřícnost a nesmírnou trpělivost během průběhu vypracování práce.

# **Predikce vývoje a posouzení investičního potenciálu kryptoměny Bitcoin**

## **Abstrakt**

Tato bakalářská práce se zabývá predikcí vývoje a posouzením investičního potenciálu kryptoměny Bitcoin. Nejprve je navrženo, jak postupovat pro uskutečnění směny, uchování a manipulování s Bitcoinem. Jsou uvedeny fáze vývoje Bitcoinu a jeho vlastnosti jako dobrého uchovatele hodnoty, které se poté komparují s tradičními fiat měnami a jinými formami majetku. V druhé části se posuzuje Bitcoin, jakožto investiční aktivum, podle strategií dlouhodobého investování. Vyhodnoceny jsou jednotlivé strategie z hlediska času, frekvence investování a zhodnocení. Na základě obou částí vlastní práce je dosaženo závěru, že Bitcoin je původní podstatou digitální měnou, která cílí k naplnění podstaty prostředku směn (peněz). Vývoj Bitcoinu z pohledu peněz se momentálně nachází ve druhé fázi ze čtyř. Nicméně, jako investiční aktivum je tato podstata naplňována, protože investorům pomáhá dosáhnout různých investičních cílů, jako je zhodnocení vloženého kapitálu, ochrana před inflací, diverzifikace portfolia a zajištění likvidity.

**Klíčová slova:** Aktiva, Bitcoin, Decentralizace, Digitální zlato, Investice, Krypto, Kryptoměny, Model, Spekulace

# **Prediction of development and investment potential of Bitcoin**

## **Abstract**

This bachelor thesis examines the development and investment potential of Bitcoin. Firstly, the exchange, storage and manipulation of Bitcoin is proposed. The phases of Bitcoin's development and its characteristics as a good store of value are presented and then compared with traditional fiat currencies and other forms of assets. In the second part, Bitcoin as an investment asset is evaluated according to long-term investment strategies. Each strategy is evaluated in terms of time, frequency of investment and performance. Based on both parts of the work, it is concluded that Bitcoin is at its core a digital currency that aims to fulfil the essence of a medium of exchange (money). Bitcoin's development from a monetary perspective is currently in the second of four phases. However, as an investment asset, it is fulfilling this essence by helping investors to achieve various investment objectives such as capital appreciation, inflation protection, portfolio diversification and the provision of liquidity.

**Keywords:** Assets, Bitcoin, Decentralization, Digital Gold, Investment, Crypto, Cryptocurrency, Model, Speculation

# Obsah

<b>1 Úvod</b> .....	<b>8</b>
<b>2 Cíl práce a metodika</b> .....	<b>9</b>
2.1 Cíl práce .....	9
2.2 Metodika.....	9
<b>3 Teoretická východiska</b> .....	<b>10</b>
3.1 Peníze .....	10
3.1.1 Definice .....	10
3.1.2 Vlastnosti a funkce.....	10
3.1.3 Historie.....	11
3.2 Kryptoměny .....	17
3.2.1 Definice .....	17
3.2.2 Historie.....	18
3.2.3 Útoky a pády burz.....	20
3.2.4 Významné kryptoměny .....	21
3.3 Bitcoin .....	24
3.3.1 Historie.....	25
3.3.2 Charakteristika.....	28
3.3.3 Klíčové inovativní řešení .....	30
3.3.4 Těženi bitcoinů .....	32
3.4 Investování .....	34
3.4.1 Investiční strategie .....	34
3.4.2 Hodnocení efektivity investice.....	34
<b>4 Vlastní práce</b> .....	<b>36</b>
4.1 Bitcoin jako prostředek směn .....	36
4.1.1 Návrh pro uskutečňování směn, uchovávání a manipulaci .....	36
4.1.2 Naplnění podstaty prostředku směn.....	50
4.1.3 Komparace bitcoinu s tradičními fiat měnami a jinými formami majetku.....	52
4.2 Bitcoin jako investiční aktivum .....	55
4.2.1 Krátkodobá investiční strategie .....	57
4.2.2 Dlouhodobá investiční strategie .....	59
4.2.3 Komparace investičních strategií.....	61
4.2.4 Zhodnocení dlouhodobých investičních strategií .....	66
<b>5 Zhodnocení výsledků</b> .....	<b>68</b>
<b>6 Závěr</b> .....	<b>69</b>
<b>7 Seznam použitých zdrojů</b> .....	<b>71</b>



<b>8</b>	<b>Seznam obrázků, tabulek, grafů a zkratk .....</b>	<b>78</b>
8.1	Seznam obrázků .....	78
8.2	Seznam tabulek .....	78
8.3	Seznam grafů .....	79

# 1 Úvod

Pro navázání komunikace a umožnění směny hodnot bylo třeba více než jen barterového obchodu, který s větším rozšiřujícím se objemem už nedokázal plnit svou funkci. Předchůdci peněz a peníze samy o sobě umožnily rozvoj lidstva v různých oblastech, jako je ekonomika, technologie a kultura. Rozvojem informačních a komunikačních technologií, zejména díky internetu, se naskytlá příležitost pro vznik digitálních měn a kryptoměn, které měly za cíl usnadnit, zrychlit a zefektivnit platby. Jenže tento princip se některým vládám nezamlouval, a několikrát zasáhly proti tvůrcům těchto měn. Svým postavením v systému stále působili jako centrální autorita a tím je bylo možné spojit s daným projektem a také je kriminalizovat.

Bitcoin byl první kryptoměnou, která se snažila řešit problémy tradičního bankovního systému a zároveň odstranit potřebu třetí strany. Bitcoin svou technologií a ekosystémem oslovil zejména libertariány a lidi, kteří chtěli zachovat svou anonymitu. S přílivem zájmu uživatelů a investorů se začal Bitcoin obchodovat veřejně na burze. S rostoucí popularitou a porozuměním jeho vnitřní hodnoty se Bitcoin začal stávat běžným pojmem a častým tématem veřejné diskuse. Jako alternativní možnost investování dosáhl Bitcoin pro určité investory vysokého zhodnocení, i přes rizika spojená s jeho volatilitou.

Bitcoin nabízí možnost zefektivnit obchodování a zároveň poskytuje útočiště těm, kteří chtějí ochránit a zhodnotit své peněžní prostředky v době vysoké inflace, cenzury a omezení. Původní obavy spojené s Bitcoinem se postupně rozptýlily a vlády si začínají uvědomovat přínosy, které by mohl Bitcoin pro ně mít. Naopak pro ty, kteří chtějí potlačovat a omezovat své občany, je Bitcoin vnímán jako hrozba.

## **2 Cíl práce a metodika**

### **2.1 Cíl práce**

Hlavním cílem této bakalářské práce je určit, zda Bitcoin spíše vykazuje předpoklady aktiva s investičním růstovým potenciálem nebo efektivního prostředku vhodného pro směnu hodnot.

K dosažení hlavního cíle práce jsou stanoveny dva dílčí cíle, které spočívají ve vytvoření návrhu pro uskutečňování směn, uchovávání a manipulaci s Bitcoinem, se zaměřením na praktické aspekty jeho užívání. Dalším dílčím cílem je zhodnocení investičních strategií do kryptoměny Bitcoin, které reflektují individuální přístup investora vzhledem k časovému horizontu a očekávaných výnosů. Důraz je kladen na potřeby českých uživatelů, investorů a institucí, zohledňující možnosti a specifika českého trhu, poskytující relevantní informace v místním kontextu.

### **2.2 Metodika**

Teoretická část práce bude zpracována pomocí studia odborné literatury a dalších českých i zahraničních zdrojů věnujícím se dané problematice. Budou vysvětleny klíčové pojmy a souvislosti, které jsou důležité pro pochopení prostředků směny, investování a kryptoměn, zejména Bitcoinu, tak aby došlo k porozumění vývoje a role v oblasti investic a směny hodnot.

Na základě zpracování dostupných dat bude vypracována vlastní část práce. Využitím popisné metody s prvky komparace budou porovnány investiční strategie, které zohlední investora z hlediska přístupu vůči času. K určení, zda-li kryptoměna Bitcoin naplňuje předpoklady prostředku směn, bude využita komparace s tradičními fiat měnami nebo jinými formami majetku.

## 3 Teoretická východiska

### 3.1 Peníze

Pro navázání spolupráce mezi ranými moderními lidmi a její efektivní využití bylo třeba více než jen jazyka (Szabo, 2002). Vývojem předchůdců peněz procházelo něco, co mělo jiný význam, než jen nositel symbolické nebo dekorativní hodnoty, což je dle Boyapatiho (2023) jen první fáze, kterou si musí projít něco, co má potenciál se stát skutečnými penězi. Drahé kovy, zejména pak zlato, tuto roli v historii zastávaly celá tisíciletí.

A jestliže škeble mohou být penězi, kožešiny mohou být penězi, zlato může být penězi, jestliže peníze nejsou jen mince nebo bankovky vydané vládou na základě zákonů o zákonném platidle, ale mohou to být nejrůznější předměty, pak co to vlastně jsou peníze (Szabo, 2002), k čemu jsou a jaký byl jejich význam při modelování současné společnosti? Peníze jsou jedním z nejdůležitějších statků, pokud se chceme bavit o rozvinuté ekonomice, protože umožňují nejenom obchodování, ale také spoření (Boyapati, 2023).

#### 3.1.1 Definice

Revenda (2012) i Boyapati (2023) uvádí, že peníze jsou takovým aktivem, které je všeobecně přijímáno všemi subjekty v dané společnosti a umožňuje vykonávat směnu za jiné statky a služby, přičemž subjekty věří, že své peníze budou moci znovu využít v budoucnosti při jiných transakcích. Pakliže je tato důvěra narušena, zejména vlivem poklesu kupní síly, tak se subjekty obrátí na naturální formu transakcí, případně na jiné zahraniční měny (Revenda et al., 2012).

#### 3.1.2 Vlastnosti a funkce

Stroukal a Skalický (2018) se zmiňují o dobrých penězích tak, že musí naplňovat určité vlastnosti a funkce, které již od dob Aristotela zůstaly téměř v neměněné podobě. Dobré peníze by měly být dobře dělitelné na menší jednotky, aby bylo možné provádět transakce při různých hodnotách. Zároveň by měly být, co nejnáze a nejrychleji ověřitelné. Mezi další vlastnosti se řadí přenositelnost, možnost skladovat a uchovávat, zaměnitelnost, a především by dobré peníze měly být vzácné. Vzácné natolik, aby jejich hodnota byla větší než nula, a

zároveň nesmí být v příliš hojném počtu. V současné době je stále více aktuální i jejich odolnost vůči ceně, tak aby nepodléhaly přílišné libovůli mocenských zájmů třetích stran.

Černohorský (2020) a Boyapati (2023) se ve své podstatě moc neliší v tom, co jeden vnímá jako dobré peníze a druhý jako vývoj peněz. Oba autoři mluví o uchovateli hodnoty, prostředku směny a zúčtovací jednotce, avšak Boyapati přidává počáteční fázi vývoje peněz – sběratelský předmět. Jednotlivé fáze nebo znaky peněz se dají chronologicky popsat následovně:

- **sběratelský předmět** – majitel předmětu jej vlastní kvůli jeho zvláštnosti, jedinečnosti a ve svých počátcích slouží jako třeba dekorace, něco, co ještě nemá povahu peněz;
- **uchovatel hodnoty** – peníze si uchovávají svou kupní sílu i do budoucna;
- **prostředek směny** – lze s nimi pořídit statky a služby či za ně uhradit dluh;
- **zúčtovací jednotka** – umožňují vyjádřit hodnotu statků a služeb a usnadňují ekonomickou kalkulaci.

### 3.1.3 Historie

Rozvoj společnosti a vývoj obchodních vztahů mezi lidmi jsou spojeny s potřebou získávat věci, které si člověk nedokázal sám vyrobit nebo obstarat. Pokud se nechtěl uchýlit ke krádeži a jinému nepoctivému obohacování na úkor jiných, musel přijít s něčím, co by mu zaručilo takovou směnu.

#### **Barterový obchod**

Szabo (2002) popisuje prvotní způsob, jak uskutečnit směnu – barterový obchod. Barter si vyžaduje souhru zájmů, nabídky, poptávky, dovednostní, preferencí, času a nízkou výši transakčních nákladů. Pakliže první i druhý účastník směny disponuje takovým zbožím, které lze směnit ihned, například výměna jablek za hrušky, kde se dá očekávat sklizeň v blízkém rozmezí, tak barter funguje celkem dobře. Avšak může nastat situace, kdy směna není možná v daném čase, ať už z jedné nebo druhé strany, například z důvodu, že první účastník směny nemá ještě daný plod dozrálý, na rozdíl od druhého účastníka směny, ale očekává daný výnos v určité kvalitě budoucnosti. Taková směna pak funguje na principu důvěry, případně zakomponováním mezičlánku, který dohlédne na uskutečnění plnění takové dohody. Související problém barteru je, že směnný obchod nefunguje ve velkém měřítku. Dobře si vede při malých objemech, ale při velkých objemech se stává příliš

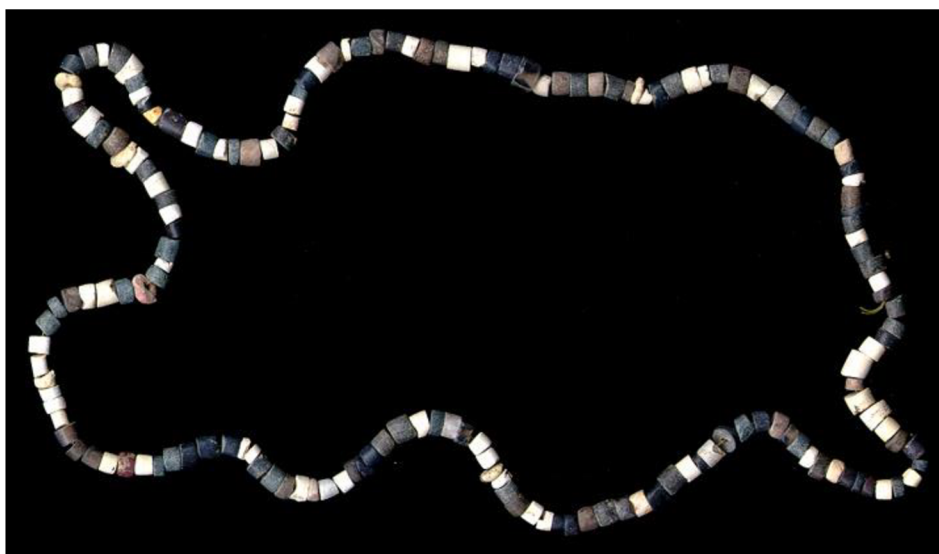
nákladným na to, aby byl efektivní. Při barterovém obchodu s  $n$  různými druhy statků a služeb je třeba sledovat  $n^2$  cen, zatímco při použití peněz je třeba sledovat pouze  $n$  cen, což je mnohem praktičtější. Barter je omezený ve srovnání s obchodem s penězi, i když stále funguje lépe než žádný obchod.

### **Komoditní (zbožové) peníze**

Szabo (2002) tvrdí, že primitivní peníze existovaly dlouho před vznikem rozsáhlých obchodních sítí. Komoditní peníze výrazně zlepšily fungování i malých barterových sítí, protože výrazně snížily potřebu úvěrů. Účastníci obchodu už nemuseli čekat a sledovat, kdo komu dluží, nebo věřit paměti či poctivosti toho druhého. Primární funkce těchto peněz spočívala v tom, že sloužily jako prostředek k ukládání a předávání bohatství.

Ke komoditním penězům Szabo (2002) uvádí, jak američtí indiáni používali peníze po tisíciletí. Místo toho, aby domorodci v Nové Anglii používali pouze kov s vyraženými tvářemi svých politických vůdců, využili toho, co se v jejich prostředí nacházelo – odolné části kosterních částí ze své kořisti. Konkrétně se jednalo o ulity škeblí *Venus mercenaria* a jejich příbuzných, které navlékali na přívěšky (viz obrázek 1). Během směny byly ulity spočítány, množstevně upraveny směrem nahoru nebo dolů, a nakonec přeskládány na nový náhrdelník. Přestože se takové ulity škeblí nacházely jen u oceánu, tak se s nimi obchodovalo hluboko ve vnitrozemí. Na jejich výrobu se specializovalo jen několik málo kmenů, zatímco stovky dalších kmenů, z nichž mnozí byly lovci a sběrači, je používali. V letech 1637 až 1661 se dokonce wampum stal zákonným platidlem v Nové Anglii. Rok 1661 předznamenal začátek konce pro wampum, když se „koruna“ rozhodla posílat své peníze do Ameriky, mince ze stříbra a zlata, kde ražbu a kontrolu prováděla „koruna“. Co započalo, jako dobře zpracované peníze skončilo jako dekorací

**Obrázek 1 Náhrdelník z wampumu**



<https://coins.nd.edu/colcoin/colcointext/wampum.html> (15.2.2024)

Szabo (2002) k mušlím uvádí, že nebyly jediným předmětem, který sloužil pro směnu, přestože se různé variace, podobným těm, které používali američtí indiáni, našly například v africké Keni, ale také v Libanonu, významném území Blízkého východu. Přesto, jak docházelo k migraci a pohybu našich předků, se objevily tyto předměty i po Evropě, ale svůj původ nachází na africkém kontinentu.

Dobytek, kůže, kožešiny, zuby a další varianty předmětů tu byly, které pro tento účel sloužily, ovšem takovéto předměty vykazovaly mnohé nedostatky a překážky, špatná dělitelnost, složitá přenosnost a například takový čaj, kakaové boby, olivový olej, nebo sůl jistě podléhaly zkáze kvůli své omezené době životnosti (Revenda et al., 2012).

### **Drahé kovy**

Do určité míry dělitelné, přenosné a hlavně trvanlivé, takové jsou drahé kovy zastoupeny jako prostředek směn zejména zlatem a stříbrem, obzvláště pak díky zlatu zažilo lidstvo největší rozmach obchodu (Boyapati, 2023). U zlata a stříbra došlo k přetavení jejich podoby na podobu mincí.

Dle Revendy et al. (2012) o takových mincích z drahých kovů se dá říct, že se skutečně jedná o první „opravdové“ peníze. Jsou totiž vzácné, v omezeném množství a v brzké době jich více nebude, hlavně co se týče zlata, které vzniká při výbuchu supernovy nebo srážce dvou neutronových hvězd. Drahé kovy a mince z nich skutečně začínají usnadňovat, zlevňovat a výrazně zpřehledňovat směnu po statcích a službách. Výsadní právo k vydávání peněz do oběhu si přivlastnili tehdejší vládcí či panovníci. Ražbu a určení obsahu zlata či

stříbra v mincích připadala na jejich libovůli, což se historicky projevovalo zlehčováním mincí.

### **Papírové peníze (bankovky, státovky a fiat)**

Revenda et al. (2012) uvádí, že historický vývoj a rozvoj bankovního systému vedl k vývoji papírových peněz, které nahrazovaly mince z běžných kovů, kterým svým zlehčováním skončily s nižší a nižší nominální hodnotou. Úschovou mincí v bance jedinec získá doklad, který stvrzuje hodnotu uloženého jmění, a tak vzniká první forma bankovek, které při směně začínají suplovat fyzické mince. Vedle historických bankovek panovník nebo vláda emitovali státovky. Státovky sloužily jako slib, který měl zaručit, že v budoucnu dojde k jejich zpětné výměně za mince z drahých kovů. Jejich využití bylo nejčastěji během období války, které značně „vyčerpávalo“ státní kasu. Samotný slib však nestačil k tomu, aby se subjekty dobrovolně rozhodli k jejich používání, takové rozhodnutí bylo často vynuceno panovníkem nebo vládou pod hrozbou přísného trestu. Emise státovek a jejich krytí na vrub státnímu rozpočtu u drtivé většiny zemí došlo konce poté, co docházelo k zvyšování cenové hladiny a ztrátě důvěry v domácí měnu. Řadu zemí dokonce přivedly k bankrotům.

Jak zmiňuje Revenda (2012), tak mezi „první peníze podnikatelského světa“ patří obchodní směnky, které se závazkem k jejich uhrazení vydávali podnikatelé, kteří dočasně v danou dobu neměli prostředky k zaplacení za zboží. Díky oblibě a právnímu postavení těchto směnek mohli jednotliví podnikatele platit mezi sebou, za předpokladu splnění určitých podmínek. Mimo jiné, takovéto směnky skýtaly výhodu v tom, že je banky odkupovaly za „hotové“. Banky vlastními bankovkami pokryly jejich výši a podnikatelé nemuseli tak čekat na dobu dospělosti (den proplacení) směnky. Zároveň směna byla výhodnou i pro samotné banky, které z každé takto realizované transakce realizovali určitý zisk ve formě diskontu. Souběžně s výkupem směnek banky vykupovaly zlato a stříbro a na základě jejich hodnoty emitovaly klasické bankovky, které byly kryty jak směnkami, tak i drahými kovy. Zlaté krytí a obchodní krytí tak zaručovalo rovnováhu mezi poptávkou a nabídkou, co se množství peněz týče. Co dobře fungovalo v období ekonomického rozkvětu, kdy byla vysoká důvěra v banky a v podnikatele, že uhradí své závazky, nefungovalo již tak dobře v období poklesu. Banky byly schopny vydat ze zásob drahých kovů jen určité množství, aniž by narušily povinnost udržovat jejich určitou minimální výši. Zároveň podnikatelé během poklesu ztráceli schopnost dostát svých závazků a krachovali.



K problému klasických bankovek a centrálních bank Revenda et al. (2012) dodává, že klasické bankovky doprovázely ještě další dva problémy, kterým bylo časové omezení a územní omezení. To mělo za příčinu určitou nepřehlednost systému, z kterého těžili padělatelé, kteří měli „žně“. Aby se systém zpřehlednil, tak emise bankovek byla svěřena jediné centrální instituci – centrální bance, která disponovala emisním monopolem. S centrální bankou přišla i centralizaci moci, moci státu, který si nyní mohl půjčovat od své vlastní banky, dle svých vlastních podmínek. Směna za drahé kovy byla významně omezena a v oběhu bylo více peněz, než bylo poptáváno, což vedlo ke zvýšení cenové hladiny a snížení kupní síly. Již značně omezená směnitelnost zaniká poté, co se americká vláda v roce 1971 jednostranně rozhodla, že dolar již nebude fyzicky krytý zlatem a tím zanikl zlatý standard.

V současnosti již nejsou státní měny, například česká koruna, dolar, euro, kryté zlatem nebo jiným drahým kovem. Jedná se o tzv. fiat měny, který mají svůj oběh vynucený vládou.

### **Bezhotovostní peníze**

Revenda et al. (2012) uvádí, že bezhotovostní peníze jsou úzce provázány s hotovostními penězi v podobě bankovek a mincí. Prvně se začínají objevovat ke konci 19. století a svou podstatou umožňují konvertovat hotovost do bezhotovostní podoby tím, že jsou uloženy v bance, která tuto směnu umožňuje jedním, tak i druhým směrem při výběru a vkladu. Emise bankovek a případně mincí spadá pořád výhradně do rukou centrální banky, avšak takové bezhotovostní peníze nejsou emitovány jen a pouze centrální bankou, ale i ostatními bankami, které je poskytují skrze své finanční instrumenty, jako jsou úvěry.

### **Digitální měny**

NTT DATA Payment Services India (2024) uvádí k digitálním měnám, že digitální měnou se myslí peníze, které své podoby nabývají jen a pouze v digitální nebo elektronické podobě na rozdíl od fiat měn, které si zachovávají svou podobu v oběživech. Rozdíl mezi digitální měnou a online bankovníctvím, přestože se oba vyskytují v digitálním prostředí, je ten, že online bankovníctví pořád využívá fiat měnu, která podléhá dohledu ze strany vlády a centrální banky, což se nedá říct u digitální měny, která je na těchto institucích nezávislá a nepodléhá restrikcím z jejich strany. Nemají tedy fyzické atributy (oběživo) a transakce se tak uskutečňují skrze počítače nebo elektronické peněženky, které jsou připojeny

k internetové síti. Stejně tak jako fiat měny, tak i digitální měny umožňují nákup statků a služeb. Existuje několik typů digitálních měn, o nichž může být hovořeno, jako je například:

- **kryptoměny** (viz Kryptoměny);
- **digitální peníze centrálních bank (CBDC)** – regulované, ve své podstatě by umožnily dalším subjektům přístup k bezhotovostním penězům centrální banky. Tento přístup mají zatím výhradně obchodní banky (Digitální peníze centrálních bank (CBDC), 2022);
- **virtuální měny** – neregulované, pod kontrolou vývojářů nebo emitující společností (například virtuální měny mezi online komunitami hráčů);
- **stablecoins** – digitální měny, jenž mají udržovat konstantní hodnotu vůči tradiční měně (například americký dolar). Každý takový token je zajištěn odpovídajícím množstvím fiat měny, případně i předzajištěn, pakliže se jedná o stablecoins kryté kryptoměnami (Bouška, 2023).

Klíčové aspekty u jednotlivých typů digitálních měn jsou zobrazeny v tabulce 1.

**Tabulka 1 Typy digitálních měn a jejich klíčové aspekty**

Kritéria	Kryptoměny	CBDC	Virtuální měny	Stablecoins
Řízení/ovládání	Decentralizované	Centralizované	Centralizované	Centralizované nebo hybridní
Regulace	Mírná až žádná	Regulováno	Mírná až žádná	Určitý regulativní dohled
Cenová stabilita	Vysoká volatilita	Stabilní	Různí se	Navrhnutá jako stabilní
Krytí aktivem	Žádné	Zajištěno vládou	Různí se	Spojené s aktivem krytí
Anonymita	Vysoká	Omezená	Různí se	Různí se
Rychlost transakcí	Může být pomalá	Rychlá	Rychlá	Rychlá
Poplatky	Různí se	Mírné až žádné	Mírné až střední	Různí se
Adaptace	Rostoucí	Vznikající trh	Zavedené	Rostoucí

Zdroj: převzato z NTT DATA Payment Services (2024)

## 3.2 Kryptoměny

Masivní rozšíření internetu s sebou přineslo i první projekty, které chtěly řešit problémy tradičního bankovníctví, a přestože se zprvu jednalo spíše o digitální peníze než o digitální měny, tak svou existencí, se všemi svými nedokonalostmi, vydláždili cestu Bitcoinu (Stroukal & Skalický, 2018).

Cyberpunkeri a kryptoanarchisti se snažili přijít s něčím, co by jim poskytlo imunitu vůči donucování ze strany státní a moci a zároveň jim poskytlo anonymitu, anonymitu v možnosti provádět platby (Boyapati, 2023).

### 3.2.1 Definice

Manjula et al. (2022) ke kryptoměnám zmiňuje, že kryptoměny jsou jedním ze čtyř typů digitálních měn, které poskytují velmi silnou míru zabezpečení a anonymity. Výměna kryptoměny probíhá mezi souhlasícími stranami bez účasti zprostředkovatelů nebo

regulačních orgánů. Jejich hodnota se odvíjí od základního principu cenové poptávky a nabídky a lze s nimi obchodovat proti mnoha fyzickým měnám. Kryptoměny mohou být velmi emotivní záležitostí pro někoho, kdo je na trhu kryptoměn nováčkem. Vysoká volatilita už je takovým denním chlebem pro ty, kteří déle věnují pozornost tomu, jak se odvíjí cena na kryptoměnových burzách, protože tak jako je tomu u všeho, tak i kryptoměny a jejich cena je dána jejich vnitřní hodnotou, kterou jí lidé přisuzují, a pakliže dojde k emotivním veřejným prohlášením, které mají tendenci ovlivňovat názory investorů, stává se, že jim lidé podlehnou a naslouchající dav tak s sebou přináší lavinu, která do značné míry má schopnost hýbat s cenou. Kryptoměny tak mají tendenci vykazovat vyšší míru volatility, než je tomu u fiat měn právě z výše zmíněných důvodů.

### 3.2.2 Historie

Stroukal a Skalický (2018) se k historii kryptoměn zmiňují, že ještě před příchodem kryptoměn, které tu jsou ještě jen velmi krátce, zde dříve byly digitální měny. Za otce digitálních měn se často označuje David Chaum, který přišel s první digitální měnou ecash. Společnost Digicash, založena roku 1989, neměla nahradit celý peněžní systém, ale svou technologií měla přinést alternativu, která by zefektivnila drobné finanční mikrotransakce a pomocí kryptografie poskytla svým uživatelům anonymitu, avšak projekt, přestože byl výjimečným vynálezem, zanikl s bankrotem, který o necelých 10 let později společnost vyhlásila, a provoz systému tím tak byl ukončen. Na rozdíl od Bitcoinu, Digicash pracovala na principu klient-server, tudíž zde pořád figurovala nadřazená centrální autorita, která svým privátním klíčem generovala a ověřovala mince, které uživatele mohli směnili za peníze. Takový požadavek vytvoří uživatel vůči serveru, který daný požadavek respektuje a podepíše jej svým privátním klíčem, aniž by dokázal určit, kdo je původním žadatelem, protože takováto mince je skryta pomocí šifrovacího schématu. Výhody tkvěly hlavně v naprosté anonymitě a schopnosti být nevysledovatelným, pakliže nedojde ke dvojí útratě (viz Problém dvojí útraty). Chaum byl a je skvělým matematikem, kterému však chyběly manažerské dovednosti k využití potenciálních obchodních příležitostí s jinými společnostmi (Abrar, 2014).

Později na úspěch/neúspěch Digicash navázaly další podobné projekty s vlastními měnami, například HashCash, CyberCoin, milicent, Visa Cash, Mondex, ePassport, Liberty Reserve, Liberty Dollar, E-gold a další. HashCash byl systémem vynalezeným britským kryptografem Adamem Backem, stalo se tak v roce 1997 (Stroukal, & Skalický, 2018). HashCash s sebou přinesl zásadní a nezbytnou inovaci, kterou bylo proof-of-work (viz Klíčové inovativní řešení), sice na trhu neuspěl, ale i přesto s touto inovací ovlivní budoucnost kryptoměn (Boyapati, 2023).

E-gold byla digitální měna, která svou hodnotu kryla skutečným zlatem, jenž nakupovala a skladovala, stejně tak jako to kdysi byla fiat měna kryta zlatem tzv. zlatý standard (Stroukal & Skalický, 2018). Jednalo se o měrnou jednotku vyjádřenou v uncích. E-gold se používalo k obchodování s ostatními uživateli, vyplácení ve formě fyzického zlata nebo směny za americké dolary, avšak její úspěch byl zároveň i její zkázou, která na sebe nenechala dlouho čekat (Stroukal & Skalický, 2018). V roce 2001 ji postihl první útok na uživatele a v roce 2009 dokonce došlo k jejímu zániku v podobě uzavření, které bylo vyvoláno podezřením úřadů z praní špinavých peněz, legálnosti a na podezření z malého Ponziho schématu (Thakur, Banik, 2018). Zaniknutí, ale také i uvěznění jeho vynálezce Bernarda von NotHause, čekalo i na projekt Liberty Dollar, který přišel s úmyslem vytvořit dobré peníze (viz Naplnění podstaty prostředku směn), který však byl později u soudu označen za terorismus (Stroukal & Skalický, 2018). Obdobný konec čekal na autora digitální měny Arthura Duvoskyho, který přišel s projektem digitální měny Liberty Reserve, která umožňovala provádět směnu z tradičních měn na Liberty Reserve dolary nebo Liberty Reserve eura, aniž by bylo zapotřebí více než jména, datumu narození, které nemusely být ověřovány, a emailové adresy (Chen, 2020). Obdobně, s pokusem krýt svou digitální měnu zlatem, skončil e-Bullion, který v rukou manželů Jima a Pamelý Fayedových nashromáždil přes 50 tisíc uncí zlata a přes milion uživatelů, kteří po pádu projektu nedostali ani dolar nazpět (Stroukal & Skalický, 2018). Za obět krátkozrakosti počítačových vývojářů padla digitální měna CyberCoin, která se nevypořádala s problémem dvojí útraty poté, co počátkem roku 2000 počítače nedokázaly nastavit správné datum a přelomem tisíciletí se chybně vrátily do roku 1900 (Stroukal & Skalický, 2018).

### 3.2.3 Útoky a pády burz

Kryptoměny se útokům nevyhnuly. Jen v roce 2022 bylo odcizeno uživatelům přes 3,8 miliardy dolarů v kryptoměnách, které „ležely“ na účtech burz a jiných platformách (George, 2023).

Mezi nejzrozsáhlejší útoky se řadí ten z března roku 2022 na Ronin Network, který si vyžádal ztrátu na hodnotě majetku v kryptoměnách ve výši 624 milionů dolarů poté, co útočník prvně vysál ze sítě 173 600 ETH (Ethereum – druhá nejvýznamnější kryptoměna po bitcoinu) a v druhém kroku 25,5 milionů USDC (USD Coin – stablecoin vázaný na hodnotu amerického dolaru v ekvivalentu jednoho dolaru) (George, 2023).

Ještě v téže roce padla možná jedna z nejvýznamnějších kryptoburz vůbec – FTX. FTX se stala insolventní poté, co majetek burzy v hodnotě 600 milionů dolarů byl odcizen z kryptoměnových peněženek společnosti, ačkoliv to společnost prezentovala jako hackerský útok na ní a její uživatele, tak s ohledem na běžící vyšetřování, tak se dá odvodit, že svou zásluhu na tom měl i její zakladatel Sam Bankman-Fried, který přijal špatná rozhodnutí mísit aktiva uživatelů s aktivy společnosti Alameda Research, což ke konci vedle ke krizi likvidity obou společností (George, 2023).

Stroukal a Skalický (2018) se zmiňují o prvních útocích a pádech na kryptoměnové scéně. Mezi první útok na soukromou peněženku uživatele se řadí ten, který se odehrál během června roku 2011, kdy uživateli s přezdívkou allianvain bylo odcizeno 25 tisíc bitcoinů. A jen o pár dní později se odehrálo něco, co významně otřásl s důvěryhodností kryptoměn a Bitcoinu konkrétně – pád burzy Mt.Gox. Z burzy byly ukradeny soukromé informace o jejích uživatelích a zároveň bylo příkazem uvolněno do nabídky obrovské množství bitcoinů, které z hodnoty 18 dolarů za bitcoin srazily cenu až skoro k nule.

Ať už je zájem útočníků jakýkoliv, tak jednoduché pravidlo pro uživatele říká, že své kryptoměny je nejlépe držet mimo online platformy a předejít tak riziku neoprávněného přístupu k nim a potenciální ztrátě majetku (viz Peněženky).

V tabulce 2 je sestupně, podle výše škody, znázorněno, na co útoky mířily v rozpětí třinácti let a jaké škody přitom na majetku způsobily.

**Tabulka 2 Žebříček nejzrozsáhlejších útoků na krypto sítě a burzy (2011-2023)**











Pořadí	Cíl	Ztráty (mil. \$)	Datum
1.	Ronin Network	624	23/3/2022
2.	Polly Network	611	10/8/2021
3.	FTX	600	12/11/2022
4.	Binance	586	6/10/2022
5.	Mt.Gox	480	19/6/2011
6.	Solana	326	2/2/2022
7.	Mixin Network	200	23/9/2023
8.	Euler Finance	197	13/3/2023
9.	Bitmart	196	4/12/2021
10.	Nomad Bridge	190	1/8/2022

Zdroj: převzato z Rekt News (2024)

#### 3.2.4 Významné kryptoměny

Mezi významné kryptoměny se řadí ty, které mají vysokou tržní kapitalizaci (viz obrázek 2 a 3), širokou uznávanost a použitelnost, vysokou likviditu a stabilitu. Mezi jednoznačně nejvýznamnější kryptoměny je Bitcoin, který má většinový podíl na tržní kapitalizaci, což je ukazatel, který měří relativní váhu Bitcoinu ve srovnání s ostatními kryptoměnami na trhu. Když je podíl vysoký, tak se dá říct, že vykazuje důvěru u uživatelů a investorů, zatímco nižší podíl signalizuje rostoucí zájem o jiné kryptoměny.

Obrázek 2 Nejvýznamnější kryptoměny podle tržní kapitalizace a dominance na trhu kryptoměn

#	Name	Price	Market Cap	Dominance
1	 Bitcoin BTC	\$62,737.06	\$1,232,213,121,630	52.9439%
2	 Ethereum ETH	\$3,464.37	\$416,234,330,988	17.879%
3	 Tether USDt USDT	\$1.00	\$98,755,165,126	4.2351%
4	 BNB BNB	\$407.65	\$60,961,331,949	2.6169%
5	 Solana SOL	\$132.44	\$58,612,594,459	2.5142%
6	 XRP XRP	\$0.6065	\$33,109,636,094	1.4187%
7	 USDC USDC	\$0.9999	\$28,636,162,560	1.228%
8	 Cardano ADA	\$0.6945	\$24,640,240,664	1.056%
9	 Dogecoin DOGE	\$0.1335	\$19,124,671,391	0.8235%
10	 Avalanche AVAX	\$43.58	\$16,437,235,134	0.7064%

<https://coinmarketcap.com> (29.2.2024)

Obrázek 3 Bitcoinová dominance na trhu kryptoměn (2014-2024)



<https://www.tradingview.com> (29.2.2024)

O ostatních kryptoměnách, vyjímaje Bitcoin, se mluví jako o altcoinech. Altcoiny představují alternativní kryptoměny, které nabízejí jiné funkcionality a řešení. Altcoiny, které se svou tržní kapitalizací následují Bitcoin jsou:

- **Ethereum (ETH)** – liší se v podpoře decentralizovaných aplikací a inteligentních kontraktů (Smart Contracts) a tím umožňují vyšší škálovatelnost a uplatnění;
- **Tether USDt (USDT)** – stablecoin, který je navázán na hodnotu dolaru v poměru 1:1. Jeho hodnota je konstantní a nevykazuje oproti Bitcoinu známky volatility a slouží hlavně k převodu mezi kryptoměnami bez nutnosti převodu na fiat měny;



- **BNB Coin (BNB)** je tokenem emitovaným kryptoburzou Binance a slouží primárně k obchodování na burze samotné, což zajišťuje určitou slevu pro její uživatele při používání. Zároveň BNB Coin je silně provázaný s Binance, a tak žije a padá s úspěchem burzy;
- **Solana (SOL)** je stejně jako Bitcoin blockchainová platforma, která se specifikuje vysokou rychlostí a nízkými transakčními poplatky;
- **Ripple (XRP)** se zaměřuje na institucionální hráče, jako jsou banky a jiné finanční instituce s cílem zjednodušení jejich plateb.

Hlavní rozdíly mezi Bitcoinem a altcoiny jsou popsány v tabulce 3, která rozlišuje Bitcoin a altcoiny podle určitých vlastností, a v tabulce 4, která popisuje rozdíl mezi Bitcoinem a konkrétními altcoiny. Kryptoměny jsou seřazeny sestupně podle tržní kapitalizace a dominance na trhu kryptoměn. Rozdíly popisované v tabulce jsou v rychlosti transakce a celkové zásobě.

**Tabulka 3 Rozdíl mezi Bitcoinem a altcoiny**

Vlastnost	Bitcoin	Altcoiny
<b>Inovace</b>	Původní kryptoměna s omezenými nadstavbami	Často zahrnují nové a inovativní funkce
<b>Specializace</b>	Zaměřen na být digitální zlato a uchovatel hodnoty	Specializované na různé použití, jako jsou smart kontrakty, decentralizované finance (DeFi) a další
<b>Adaptace</b>	Nejvíce rozšířená a uznávaná kryptoměna	Různé úrovně adopce, některé mohou být velmi nové nebo málo známé
<b>Riziko</b>	Považován za méně rizikový díky své historii a stabilitě	Může být vyšší riziko kvůli menší historii a volatilitě

Zdroj: převzato z Velká kniha o Bitcoinu a kryptoměnách, aneb, Finanční gramotnost pro každého (Bouška, 2023)

**Tabulka 4 Rozdíl mezi Bitcoinem a altcoiny (rychlost transakcí, výše poplatků a jejich celkové zásoby)**

Kryptoměna	Rychlost transakce	Celková zásoba
Bitcoin (BTC)	Pomalé	21 milionů
Ethereum (ETH)	Střední až rychlé	∞
Tether USDt (USDT)	Rychlé	Dynamická
BNB Coin (BNB)	Velmi rychlé	200 milionů
Solana (SOL)	Téměř instantní	∞
Ripple (XRP)	Téměř instantní	100 miliard

Zdroj: převzato z <https://www.statista.com> (2024)

### 3.3 Bitcoin

Bitcoin je nepřehlédnutelným lídrem kryptotrhu. Jeho dominance je zřejmá, ať už se jedná o hodnotu, popularitu nebo technologickou sílu. Bitcoin je považován za lídra trhu z několika důvodů:

- **první kryptoměna** – Bitcoin byl první kryptoměnou, která byla úspěšně implementována a získala širokou adopci;
- **nejvyšší tržní kapitalizace** – díky svému prvenství a adopci má Bitcoin nejvyšší tržní kapitalizaci mezi všemi kryptoměnami;
- **široce uznávaný** – je vnímán jako „digitální zlato“ a forma uchování hodnoty.

V tabulce 5 jsou popsány hlavní výhody a nevýhody Bitcoinu.

**Tabulka 5 Výhody a nevýhody Bitcoinu**

Výhody	Nevýhody
Decentralizace – Bitcoin je decentralizovaný, což znamená, že není ovládán jedinou entitou	Volatilita – jeho cena může výrazně kolísat, což může být riziko pro investory
Omezená nabídka – Bitcoin má pevně stanovený počet mincí (21 milionů), což mu dodává hodnotu	Omezená škálovatelnost – s narůstajícím počtem uživatelů může být obtížné udržet rychlost transakcí
Uznávaný jako uchovatel hodnoty – investoři hledají Bitcoin jako bezpečnou investici v době ekonomické nejistoty	Vysoká energetická náročnost – těžba Bitcoinu vyžaduje velké množství energie.
Široká adopce a uznání – Bitcoin je přijímán obchodníky a institucemi po celém světě.	Asociace s nelegálními aktivitami – v minulosti byl spojován s nelegálními transakcemi.

Zdroj: převzato z Velká kniha o Bitcoinu a kryptoměnach, aneb, Finanční gramotnost pro každého (Bouška, 2023)

### 3.3.1 Historie

Za toho, kdo vydláždil cestu pro vznik Bitcoinu, je považován vývojář Satoshi Nakamoto, který vystupuje anonymně pod pseudonymem. Satoshi v roce 2008 sdílel s ostatními členy kryptografické komunity, že pracuje na novém elektronickém systému peněz, který funguje čistě na principu peer-to-peer a nevyžaduje tak třetí strany a zároveň popsal ve zprávě hlavní klíčové aspekty (viz Klíčové inovativní řešení) (Nakamoto, 2008). Prvotní dokument (Bitcoin whitepaper) s názvem „Bitcoin: A Peer-to-Peer Electronic Cash System“ popisuje originální plán a protokol pro Bitcoin (Nakamoto, 2009).

Stroukal a Skalický (2018) objasňují, kdo by mohl být Satoshi Nakamoto. Satoshi Nakamoto – není známo, zda se jedná o osobu nebo skupinu, která by za tímto projektem stála. Nicméně existují spekulace, které naznačují, kdo by to mohl být. Za nejpravděpodobnějšího Satoshi Nakamota je označován Nick Szabo – americký programátor, původem z Maďarska. O decentralizované digitální měně o „bit gold“ již dříve mluvil v článku. Často také využíval pseudonymy, jejichž iniciály se shodovaly s těmi, které jsou obsaženy ve jméně Satoshi Nakamoto. Navzdory těmto spekulacím však svou asociaci

odmítl. Objevila se další jména jako Shinichi Mochizuki, který byl geniálním matematikem, pak například trojice Neal King, Vladimir Oksman a Charles Bry, kteří se ale vůči tomu ohradili a nařčení z autorství odmítli. Spekulace o autorství dopadly i na vývojáře, kteří projekt později převzali – Hal Finney, Gavin Andresen a Jed McCaleb. Nevyhnuly se ani zakladateli ilegálního tržiště Silk Road, kterým byl Ross Ulbricht. Avšako málo kdo vzbudil takový zájem médií o určení toho, kdo by mohl stát za Bitcoinem, tak jako Dorian Nakamoto, Japonec, narozený pod jménem Satoshi, žijící v Kalifornii, Spojených státech amerických. Absolutní shoda ve jménu, které vzbuzuje tolik emocí ve veřejném prostoru, jako málokteré jiné, avšak brzy se ukázalo, že asociovat ho k anonymnímu vývojáři, vystupujícím pod pseudonymem, které se shodou okolností shoduje s rodilým jménem Dorian Nakamota, nikam nevede. Co ale tento mediální hon přinesl je vyjádření skutečného otce zakladatele, ten se na svém internetovém profilu vyjádřil takto: „nejsem Dorian Nakamoto.“ (viz obrázek 4)

Obrázek 4 „nejsem Dorian Nakamoto.“

The screenshot shows the P2P Foundation website interface. At the top, it says 'P2P foundation' and 'The Foundation for Peer to Peer Alternatives'. Below that are navigation links: 'Main My Page Members Videos Forum Groups Blogs Chat'. There are also links for 'All Discussions' and 'My Discussions', and a '+ Add' button. The main content area is titled 'Satoshi Nakamoto's Discussions (5)'. Below this is a search bar 'Search by This Author' and a 'View' dropdown menu set to 'Discussions Replied To'. The main content is a table with four rows, each representing a discussion. Each row has a profile icon, a title, a 'Replies' count of 46, and a 'Latest Activity' date of Oct 28, 2022. The second row, with the title 'I am not Dorian Nakamoto.', is highlighted in yellow. Below each title is a small text snippet: 'Satoshi Nakamoto replied Dec 24, 2021 to Bitcoin open source implementation of P2P currency' for the first, 'Satoshi Nakamoto replied Mar 7, 2014 to Bitcoin open source implementation of P2P currency' for the second, 'Satoshi Nakamoto replied Feb 18, 2009 to Bitcoin open source implementation of P2P currency' for the third, and 'Satoshi Nakamoto replied Feb 15, 2009 to Bitcoin open source implementation of P2P currency' for the fourth.

Discussions Replied To (4)	Replies	Latest Activity
"After 13 years of decentralized payment systems evolution we came where we are now,..." Satoshi Nakamoto replied Dec 24, 2021 to Bitcoin open source implementation of P2P currency	46	Oct 28, 2022 Reply by Greg Matthews
"I am not Dorian Nakamoto." Satoshi Nakamoto replied Mar 7, 2014 to Bitcoin open source implementation of P2P currency	46	Oct 28, 2022 Reply by Greg Matthews
"It is a global distributed database, with additions to the database by consent of th..." Satoshi Nakamoto replied Feb 18, 2009 to Bitcoin open source implementation of P2P currency	46	Oct 28, 2022 Reply by Greg Matthews
"Could be. They're talking about the old Chaumian central mint stuff, but maybe only..." Satoshi Nakamoto replied Feb 15, 2009 to Bitcoin open source implementation of P2P currency	46	Oct 28, 2022 Reply by Greg Matthews

<https://p2pfoundation.ning.com> (1.3.2024)

První bitcoiny nevytěžil nikdo jiný než samotný Satoshi, který 3. ledna 2009 spustil první proces těžení a vytěžil si tím pro sebe 50 bitcoinů. Prvnímu bloku na blockchainu,

kterým vše začalo, se říká „genesis blok“ nebo je také označován za „blok 0“ (viz Blockchain) (Stroukal & Skalický, 2018).

Jak uvádí Stroukal a Skalický (2018): „*první člověk vlastnil první bitcoiny.*“

S prvními bitcoiny přišla i první transakce mezi. Stejně jako první těžbu provedl i první transakci Satoshi, který v lednu téhož roku poslal 10 bitcoinů vývojáři Halu Finneyemu (Stroukal & Skalický, 2018). Avšak první směna za statek nebo službu se udála o více než rok později poté, co floridský programátor Laszlo Hanyecz poptával na Bitcoinovém fóru dvě velké pizzy, které byl ochotný směnit za 10 000 bitcoinů a už o čtyři dny později potvrdil, že mu skutečně poptávané pizzy byly doručeny tím, že jako důkaz poskytl fotografie s pizzami (viz obrázek 5) (Hanyecz, 2010).

Obrázek 5 Záznam transakce na Blockchainu

TX USD

## Bitcoin Pizza

Broadcasted on 22 May 2010 08:16:31 GMT+2

**Notable**

**Hash ID**  
a1075db55d416d3ca199f55b6084e2115b9345e16  
c5cf302fc80e9d5fbf5d48d

This transaction was made by Laszlo Hanyecz in 2009 where he paid Jeremy Sturdivant 10,000 bitcoin for two pizzas. It was worth ~\$41 at the time and was arranged on the bitcointalk forums.

<b>Amount</b>	10000.00000000 BTC • \$621,385,000
<b>Fee</b>	99,000,000 SATS • \$61,517.12
<b>From</b>	1XPTg-trvH4
<b>To</b>	Jeremy Sturdivant

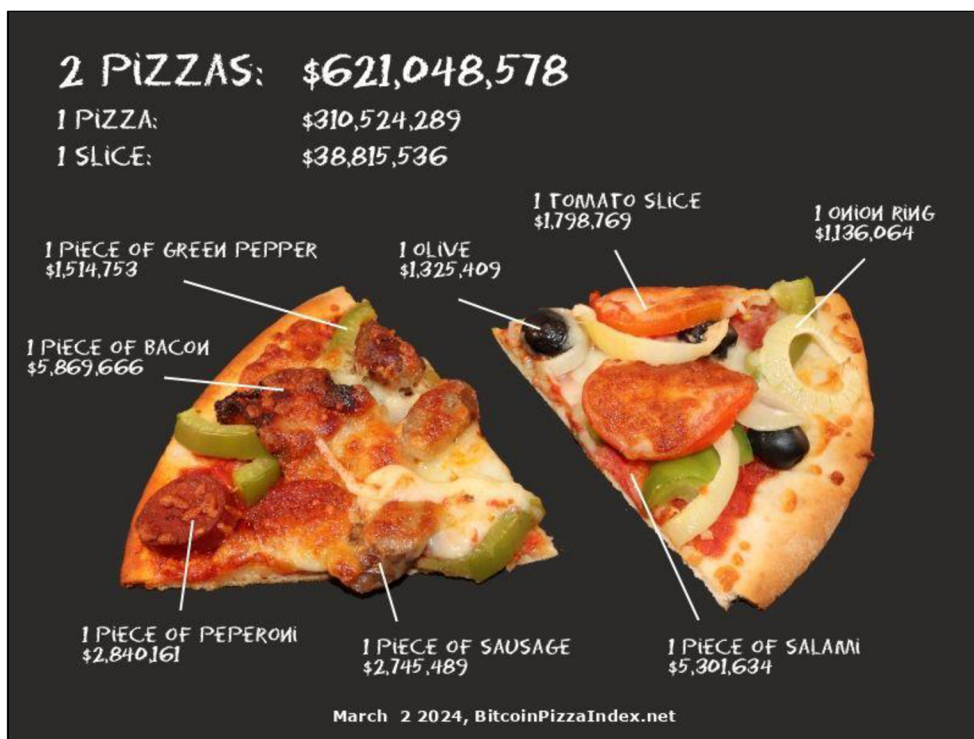
**Confirmed**

<https://www.blockchain.com> (2.3.2024)

V tu dobu měla hodnota bitcoinu zhruba dvojnásobek ceny na burze, co měly doručené pizzy, které stály 25 dolarů. Citováno jako „nejdražší pizza dějin“, kterou reflektuje tzv. Bitcoin Pizza Index, jenž ukazuje hodnotu vynaloženou na pořízení těchto pizz vůči ceně

bitcoinu na burze. Co začalo jako pizza za 41 dolarová pizza má dnes hodnotu přesahující 620 milionů dolarů (viz obrázek 6).

Obrázek 6 Bitcoin Pizza Index



<https://bitcoinpizzaindex.net> (2.3.2024)

### 3.3.2 Charakteristika

Antonopoulos a Harding (2023) uvádí, že Bitcoin je kolekce konceptů a technologií, která utváří ucelený základ pro ekosystém digitálních peněz, spravuje historii platebních transakcí mezi svými uzly, aniž by bylo zapotřebí třetí strany, která by tyto transakce spravovala a figurovala zde, jako nadřazená centrální autorita v superiorní roli. Jedná se tudíž o P2P (peer-to-peer; viz Klíčové inovativní řešení) síti, kde komunikace probíhá pouze na principu klient-klient, a tak spolu uživatelé, využívající Bitcoin protokolu, komunikují převážně skrze internetovou síť. Neexistuje zde centrální server, a tak jednotlivé uzly komunikují spolu přímo (Nakamoto, 2009). V bankovním sektoru tato komunikace probíhá na principu klient-server, kde komunikaci zprostředkovává server, na který je zadán dotaz, ten se akceptuje, zpracuje a vrátí se klientovi ve formě požadované informace. Celá síť v tomto případě stojí a padá na serveru, což u Bitcoinu nelze považovat za hrozbu.

Rozlišuje se Bitcoin s velkou iniciálkou a bitcoin s malou iniciálkou. Bitcoin je síť a bitcoin (BTC) je základní jednotkou transakce, tak jako česká koruna je měnovou jednotkou České republiky (mezinárodně CZK). Českou měnu, v její podobě bankovek a mincí, má

právo vydávat pouze a výhradně Česká národní banka, tak jako i správu zásob a ražbu (Česká republika, 1993), zatímco bitcoin je oproti české koruně a jiným tradičním měnám zcela virtuální, neexistují žádné její podoby, ať už v mincích, či bankovkách (Antonopoulos & Harding, 2023). Bitcoin se distribuuje skrze Bitcoinovou síť těžařům, kteří silou své výpočetní techniky ověřují transakce a řeší složité matematické úkoly, které umožňují přidávat nové bloky transakcí do blockchainu (viz Těžení bitcoinů a Blockchain).

Svou výhodu si bitcoin uchovává v tom, že je rychlý, zabezpečený (viz Kryptografie a Komparace bitcoinu s tradičními fiat měnami a jinými formami majetku) a neohraničený státními hranicemi (Antonopoulos & Harding, 2023). Umožňuje tak přenášení hodnoty na velkou vzdálenost, kterou lze provádět s minimálním požadavkem na důvěru (Boyapati, 2023).

K přístupu do zabezpečené sítě Bitcoin je zapotřebí klíče, kterým se uživatelé prokazují k vlastnictví svých bitcoinů. S těmito klíči autorizují platby, kterými uvolňují množství a hodnotu ze své peněženky na vrub peněženky příjemce. Takové autorizační klíče jsou uloženy na digitálních peněženkách, případně i v hardwarové formě (viz Peněženky) (Antonopoulos & Harding, 2023).

Boyapati (2023) uvádí, že Bitcoin není krytý a nelze stanovit jeho vnitřní hodnotu obvyklými metodami, například metodou stanovení hodnoty na základě poptávky po statku, který slouží k výrobě statku vyššího řádu. To proto, že bitcoin patří do peněžních statků, a ty jsou oceňovány na základě metod teorie her. Každý účastník trhu přiřazuje Bitcoinu hodnotu podle svého uvážení a odhadu, s ohledem na užitek a vzácnost. Čím dříve si někdo uvědomil, že v budoucnu bude poptávka po bitcoinu, tím levněji si ho mohl pořídit, protože cena s rostoucí poptávkou stoupá.

Bouška (2023) zmiňuje, že Bitcoin má své zaryté příznivce, kterým se v kryptoměnových komunitách říká „bitcoinoví maximalisté“ – jedinci, kteří věří, že Bitcoin je jedinou opravdovou kryptoměnou a ostatní alternativy jsou jen zbytečným balastem. Svou víru (Bitcoinový maximalismus) zakládají na absolutní oddanosti Bitcoinu, kterou šíří dál v rámci komunity. Z principu mohou zastávat zdravý přístup, který respektuje hodnotu Bitcoinu a zároveň nezavrhují potenciál ostatních kryptoměn, nebo toxický přístup, který často pramení ze zklamání nad neúspěšnými investicemi do altcoinů.

### 3.3.3 Klíčové inovativní řešení

Bitcoin přinesl do světa financí a technologií několik klíčových inovativních řešení, která ovlivňují způsob, jakým lidé vnímají peníze, platby, bezpečí a anonymitu při provádění transakcí a zároveň řeší problémy svých předchůdců.

#### **Problém dvojí útraty**

Hlavním problémem, se kterým se kryptoměny potýkaly, byla možnost dvojí útraty, což by umožňovalo provést platbu dvakrát duplikací digitálních peněz (Stroukal & Skalický, 2018). K předejetí takové možnosti se využívalo centrální autority v superiorním postavení, která platby verifikovala a tím předcházela tomuto problému za cenu důvěry uživatelů, nicméně, tato autorita, která fungovala jako datové centrum, byla a stále je ohrožena hackerskými útoky, které jí mohou způsobit škody nebo případné zničení.

Stroukal a Skalický (2018) k problému dvojité útraty (double spend) uvádí, že dvojitá útrata je: *„typ útoku na bitcoinovou síť, kdy se útočník snaží použít stejné bitcoiny (přesněji též výstup nějaké existující transakce) vícekrát (přesněji na vstupech více než jedné nové transakce). Tento útok se realizuje mnohem snadněji, pokud příjemce platby nepožaduje potvrzení příslušné transakce – stačí každému příjemci anoncovat pouze jemu určenou transakci. Čím větší počet potvrzení příjemce platby požaduje, než ji uzná za provedenou, tím hůře se útok realizuje. Útočník je nucen rychle vytěžit alternativní bloky a tím obětovat svůj výpočetní výkon k útoku, jehož nejistota úspěchu roste s počtem potvrzení, která musí svoji alternativní větví blockchainu „obejít“.“*

Problém byl odstraněn vytvořením „veřejné účetní knihy“ – Blockchain (viz Blockchain).

#### **Kryptografie**

Stroukal a Skalický (2018) uvádí, že kryptografie je: *„matematická disciplína zabývající se šifrováním – převodem zpráv do/z utajené podoby, která je čitelná jen se znalostí šifrovacího klíče. Pokud klíč k dešifrování zprávy není stejný jako klíč k jejímu zašifrování (resp. Pokud jsou tyto dvě informace oddělitelné), hovoříme o kryptografii asymetrické. Bitcoin využívá poznatku kryptografie ke svému bezpečnému fungování, a to zejm. hashovací funkce a digitální podpis.“*



## Blockchain

Stroukal a Skalický (2018) k blockchainu zmiňují, že je decentralizovaný účetní systém, který zaznamenává a udržuje digitální účetnictví transakcí provedených v bitcoinové síti. Tento systém využívá kryptografické metody a spojuje záznamy do lineárního seznamu bloků, nazývaného blockchain. Každý blok obsahuje data o provedených transakcích a odkaz na předchozí blok (kromě prvního bloku, tzv. „genesis blok“, který je označen „0“; viz obrázek 6) v řetězci (hash – funkce, která přijímá vstupní data libovolné délky a vrací řetězec pevné délky). Neustále se tak aktualizuje nejdelší řetězec, který svědčí jako důkaz o vykonané práci (viz Proof-of-work). Blockchain tak vytváří stromovou strukturu, která se rozvětňuje, ale nevytváří cykly. K rozvětvení blockchainu dochází jen zřídka a síť pracuje pouze s nejdelším řetězcem bloků, který je považován za nejvíce relevantní.

Tímto způsobem blockchain slouží jako veřejný, transparentní a nezměnitelný ledger (účetní kniha), který umožňuje každému sledovat historii transakcí a ověřit jejich platnost.

Obrázek 7 „Genesis blok“

00000000	01 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....
00000010	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....
00000020	00 00 00 00 3B A3 ED FD	7A 7B 12 B2 7A C7 2C 3E	....;fíýz{.²zÇ,>
00000030	67 76 8F 61 7F C8 1B C3	88 8A 51 32 3A 9F B8 AA	gv.a.È.Ã^ŠQ2:Ÿ_ª
00000040	4B 1E 5E 4A 29 AB 5F 49	FF FF 00 1D 1D AC 2B 7C	K.^J)«_IŸŸ...~+
00000050	01 01 00 00 00 01 00 00	00 00 00 00 00 00 00 00	.....
00000060	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....
00000070	00 00 00 00 00 00 FF FF	FF FF 4D 04 FF FF 00 1D	.....ŸŸŸŸM.ŸŸ..
00000080	01 04 45 54 68 65 20 54	69 6D 65 73 20 30 33 2F	..The Times 03/
00000090	4A 61 6E 2F 32 30 30 39	20 43 68 61 6E 63 65 6C	Jan/2009 Chancel
000000A0	6C 6F 72 20 6F 6E 20 62	72 69 6E 6B 20 6F 66 20	lor on brink of
000000B0	73 65 63 6F 6E 64 20 62	61 69 6C 6F 75 74 20 66	second bailout f
000000C0	6F 72 20 62 61 6E 6B 73	FF FF FF FF 01 00 F2 05	or banksŸŸŸŸ..ò.
000000D0	2A 01 00 00 00 43 41 04	67 8A FD B0 FE 55 48 27	*....CA.gŠŸ°pUH'
000000E0	19 67 F1 A6 71 30 B7 10	5C D6 A8 28 E0 39 09 A6	.gñ q0·.\Ö''(à9.!
000000F0	79 62 E0 EA 1F 61 DE B6	49 F6 BC 3F 4C EF 38 C4	ybâè.ap¶IÖ¿?Lİ8Ä
00000100	F3 55 04 E5 1E C1 12 DE	5C 38 4D F7 BA 0B 8D 57	óU.â.â.Đ\8M+ø..W
00000110	8A 4C 70 2B 6B F1 1D 5F	AC 00 00 00 00	ŠLp+kñ._~....

[https://wiki.bitcoinsv.io/index.php/Genesis\\_block](https://wiki.bitcoinsv.io/index.php/Genesis_block) (1.3.2024)

## **Proof-of-work**

Důkaz práce (Proof-of-Work) je mechanismus, který slouží jako důkaz vykonané práce. Tuto inovaci představil kryptograf Adam Back, jehož jméno je již zmíněno v historii kryptoměn. Původně tento inovativní prvek řešil problém emailového spamu, který trápil jeho autora. Kryptografický důkaz ověřoval, kolik energie bylo vynaloženo a jaké náklady byly na ni spojeny, přičemž každý email byl při tomto procesu opatřen jedinečným otiskem (hashem), který sám o sobě nebyl nákladný, avšak při masovém rozesílání spamu by se pro rozesílatele značně prodražil (Stroukal & Skalický, 2018).

## **Peer-to-peer**

Peer-to-peer (P2P) je typ počítačové sítě, kde jednotliví uživatelé komunikují přímo mezi sebou bez centrální autority v superiorním postavení (centrální server), což znamená, že síť funguje na principu rovnocennosti mezi všemi účastníky. Výhodou P2P sítě je vyšší přenosová rychlost při zapojení většího množství uživatelů, zatímco nevýhodou je počáteční obtížnost navázání komunikace (Stroukal & Skalický, 2018).

### **3.3.4 Těžení bitcoinů**

Jak uvádí Dimitri (2017), jedním z nejcharakterističtějších rysů Bitcoinu je, že registrace transakcí se provádí prostřednictvím těžby, kterou provádí určité subjekty (těžaři). Tato činnost spočívá v řešení hádanky (složitých matematických výpočtů, respektive pomocí inverzní hashovací funkce) vyžadující vysoký výpočetní výkon, protože k registraci bloku transakcí může dojít až po vyřešení hádanky. Po registraci transakcí v ledgeru je velmi důležité poskytnout správné ekonomické pobídky k vyřešení hádanky. Proto jsou těžaři za tuto činnost odměňováni dvěma typy odměn, jednak za každý vyřešený hlavolam obdrží od protokolu pevně stanovenou částku bitcoinů (odměna za blok, viz tabulka 6) a navíc mohou jednotlivci, kteří se chovají jako těžaři, za registrace transakce nabídnout poplatek. Čím vyšší je tento poplatek, tím vyšší je motivace těžařů, aby příslušnou transakci zařadili do dalšího registrovaného bloku. Pevná částka získaná z protokolu za každý registrovaný blok bude mít v průběhu let tendenci klesat (halving – půlení odměny za vytěžený blok těžařům), až do svého zániku, poté budou těžaře odměňovat pouze poplatky zaplacené za registraci transakcí.

**Tabulka 6 Výše odměny a objem vytěžených BTC (2009-2036)**

Rok	Odměna za blok	Vytěžené BTC celkem	Nově vytěžené BTC	% všech vytěžených BTC
2009	50	0	0	0,00 %
2012	25	10 500 000	10 500 000	50,00 %
2016	12,5	15 750 000	5 250 000	75,00 %
2020	6,25	18 375 000	2 625 000	87,50 %
2024	3,125	19 687 500	1 312 500	93,75 %
2028	1,5625	20 343 750	656 250	96,88 %
2032	0,78125	20 671 875	328 125	98,44 %
2036	0,390625	20 835 937,5	164 062,5	99,22 %

Zdroj: vlastní zpracování z blockpit.io (2024)

Dimitri (2017) dodává, že těžební činnost lze chápat jako soutěž, ve které těžaři soupeří o odměnu za vyřešení hádanky. Ti, kteří neuspějí, mohou přijít o své investice, pokud je nedokážou znovu využít jinde. Pravděpodobnost výhry je označována jako soutěžní funkce. V Nashově rovnováze těžební herního modelu s dokonalými informacemi je rozhodnutí stát se aktivním těžařem závislé na vlastních mezních nákladech ve srovnání se strukturou nákladů konkurentů, nikoli na výši odměny za blok. Efektivita konkurentů je tedy klíčovým faktorem při rozhodování o aktivní těžbě, nikoli výše získaných bitcoinů.

Stroukal a Skalický (2018) vysvětlují, že jednotlivci, kteří vykonávají těžbu se mohou sdružovat do mining poolů, mezi které se patří i český Slushův pool, a silou své výpočetní techniky participovat na těžbě, která kolektivně celému poolu zvyšuje šanci na vytěžení bloku ve srovnání s individuální těžbou. Členové poolu si rozdělují odměny získané za těžbu, což znamená, že každý těžař obdrží menší výdělek, ale zároveň minimalizuje riziko spojené s neúspěšným samostatným těžením.

## 3.4 Investování

Investování má mnoho podob, avšak co je stejné je to, že každý racionálně uvažující investor vytváří investiční majetek za účelem jeho zhodnocení. Rozhodování proč investovat je u každého individuálního investora jiný, musí si položit mnoho otázek a definovat cíl, kterého chce pravidelným investováním dosáhnout například důchod, vlastní bydlení nebo ochrana peněz před inflací. Obecně také platí, že čím později s investováním investor začne, tím více bude muset investovat, aby dosáhl požadovaného cíle.

Investor musí mít hlavně disciplínu a jasně vytyčené cíle. Cíle se v průběhu života sice můžou měnit, ale disciplínu by si měl s sebou nést během celé doby. Emoce hrají svou velkou roli v životě investora a investování, proto je důležitá disciplína, aby se přes menší kolísání investor neztratil a nevybočil z cesty, kterou si vytyčil.

Kromě vytváření investičního portfolia je nutná i jeho správa a servis, stejně jako tomu je u auta nebo bydlení, samotným pořízením to nekončí.

### 3.4.1 Investiční strategie

Investiční strategie je plán, který je na míru šitý pro jednotlivého investora, který má určité finanční a investiční cíle, a pomáhá mu docílit krátkodobých až dlouhodobých cílů.

Osobní investiční strategie se odvíjí od cílů, životní situace, věku, hodnoty vloženého kapitálu, očekávaného výnosu, míry likvidity a rizika (Revenda et al., 2012). Z toho vyplývá, že taková strategie se v průběhu vývoje podle okolností mění, stejně tak jako se mění chování a potřeby investora.

### 3.4.2 Hodnocení efektivnosti investice

Jak uvádí Revenda (2012): „*cílem většiny investorů je maximalizovat výnos ve vztahu k riziku a k likviditě.*“. Jak ale říká teorie magického investičního trojúhelníku, není možné mít všechno - tj. investici, která by poskytovala nejvyšší výnosnost, nejvyšší likviditu a zároveň nejnižší riziko. Je tedy nutné činit kompromisní rozhodnutí, která optimalizují a reflektují cíle stanovené v investiční strategii.

## **Výnos**

Výnos není nikdy zaručen a nelze vycházet z principu, že investiční instrument vykazoval historicky výnos, tudíž jej bude vykazovat znovu a můžeme jej očekávat i v budoucím období (Revenda et al., 2012). V takovém případě musíme i zohlednit čas, při kterém cena v krátkodobém a střednědobém horizontu bude jistě náchylná k volatilitě. Výnos z investice investor může očekávat ve dvou formách – dividendou nebo kapitálovým výnosem. Dividenda je odměnou akcionářům za vlastnictví akcií, kterou se společnost rozhodla předat jako podíl na zisku společnosti a to zejména, protože jí tu umožňuje její finanční zdraví, nebo tak činí z rozhodnutí vedení společnosti, které vyplývá z její strategie. Kapitálový výnos je rozdílem mezi kupní cenou a cenou nominální v daném čase, za kterou může být cena investice realizována při prodeji (Revenda et al., 2012).

## **Riziko**

Čím vyšší očekávaný budoucí výnos, tím větší je riziko ztráty a naopak, čím nižší je očekávaný budoucí výnos, tím je riziko ztráty menší. Proto je pro investora nezbytné odhadnout míru rizika a realisticky posoudit potenciální výnos, který z investice může očekávat.

Rizika, která působí na výši výnosů jsou buďto jedinečná nebo systematická. Ze svého působení a hospodaření vyplývají rizika jedinečná, pakliže se mluví o firmách, a jejich vlastní činností, tak přímo působí na míru rizika (Revenda et al., 2012). Naopak systematická rizika jsou mimo kontrolu (firem nebo investičních instrumentů) a závisí na celkovém vývoji ekonomiky a makroekonomických faktorech (Revenda et al., 2012).

## **Likvidita**

Likvidita investičního nástroje označuje rychlost, s jakou lze investici prodat a získat tak finanční prostředky, přičemž tento proces zahrnuje finanční a časové náklady, které se mohou lišit v závislosti na charakteru investice, přičemž náklady mohou dosahovat od desetin procenta až po desítky procent z hodnoty investice (Revenda et al., 2012).

## 4 Vlastní práce

### 4.1 Bitcoin jako prostředek směn

Bitcoin s sebou nepřináší pouze technologické inovace, ale také revoluci v oblasti toho, co je považováno za peníze a jak jsou využívány, a to bez prostředníka nebo někoho v centrální roli s vyšším postavením. Aby se toto skutečně stalo, musí Bitcoin projít jednotlivými fázemi vývoje a zároveň dostatečně zakořenit v paměti veřejnosti a upoutat její pozornost, aby nakonec dosáhl uživatelů, kteří jej budou chtít využívat.

Návrhy, jak Bitcoin využívat jako prostředek směn a peněz, jsou navrženy tak, aby chronologicky odpovídaly od počátečního procesu opatření až k zdanění a regulacím.

#### 4.1.1 Návrh pro uskutečňování směn, uchovávání a manipulaci

Ještě před samotným opatřením, obchodováním a jinou manipulací je prvním krokem, tak jako u všeho, dobře se prvně informovat. Bitcoin je něco jiného, na co jsou běžní lidé zvyklí, a proto před opatřením a využíváním bitcoinu je správné tyto informace mít k tomu, aby mohli uživatelé bezpečně se svými bitcoiny nakládat a vyhnuli se tak běžným chybám, trikům a podvodům ze strany útočníků.

#### Peněženky

Podle Stroukala a Skalického (2018) je Bitcoin unikátní kód, který musí být někde uložen a stejně jako fyzické peníze, které není vhodné tahat po kapsách, tak stejně tomu není jinak u bitcoinu. Proto prvním nezbytným krokem je pořízení peněženky, aby měly být kde bitcoiny uloženy. Na Bitcoinové peněženke se doporučuje uchovávat jen malé množství, které uživatel uzná za vhodné pro běžné transakce a zbytek je dobré dát stranou na bezpečné místo, ideálně mimo internetovou síť. Pravidelné zálohování peněženky může ochránit prostředky, které jsou na ní uloženy. Selhání lidského faktoru je časté a podobně tomu tak je i u techniky, například počítačů a mobilních zařízení. Dojde-li ke ztrátě nebo poškození, záloha poskytne možnost se ke svým prostředkům dostat zpátky.

Podle různých potřeb a kritérií, například uživatelské přívětivosti, kontroly, zabezpečení, transparentnosti, zátěže na životní prostředí, poplatků a jiných funkcí je možné si zvolit ze čtyř základních podob peněženek. Jejich výhody a nevýhody jsou srovnány v tabulce 7, která čerpá z informací od Stroukala a Skalického (2018) a zároveň z původní

registrované stránky Bitcoin.org (2024), přičemž ani jeden toho druhého nerozkuluje a spíše doplňuje určité poznatky a informace.

**Tabulka 7 Výhody a nevýhody jednotlivých forem peněženek**

Formy	Výhody	Nevýhody	Příklady
<b>Desktopové (softwarové peněženky)</b>	Kontrola nad finančními prostředky, včetně poplatků v síti; podpora hardwarové peněženky	Obtížné využití QR kódů při provádění transakcí; náchylnost na škodlivý malware/spyware/viry kradoucí bitcoin	Bitcoin Core; Electrum; Armory
<b>Webové peněženky</b>	Přístupnost odkudkoliv a kdykoliv; jednoduchost a integrace s jinými službami a burzami	Závislost na třetí straně (ztráta kontroly nad klíči); jednoduchost a integrace s jinými službami a burzami	Blockchain.com; Coinbase
<b>Mobilní peněženky</b>	Navrženo pro použití QR kódu k rychlému a bezproblémovému provádění transakcí	Tržiště aplikací (App Store, Google Play) mohou peněženku delistovat ze své nabídky, což ztěžuje přijímání budoucích aktualizací; poškození nebo ztráta zařízení může potenciálně vést ke ztrátě finančních prostředků	Unstoppable; Coinomi
<b>Hardwarové peněženky</b>	Jeden z nejbezpečnějších způsobů ukládání finančních prostředků; ideální pro ukládání velkého množství bitcoinů.	Obtížné používání v mobilu, není určen pro skenování QR kódů; ztráta zařízení bez řádného zálohování může způsobit, že prostředky nebudou obnovitelné; počáteční náklady	Trezor

Zdroj: Vlastní zpracování z Choose your wallet – Bitcoin (2024)

Podle Stroukala a Skalického (2018) v případě desktopových (softwarových) peněženek je první možností si stáhnout oficiálního bitcoinového klienta – Bitcoin Core z webu bitcoin.org, který však není příliš uživatelsky přívětivý, protože software zaznamenává celý blockchain protokol, který je značně rozsáhlý a zabírá příliš mnoho paměti dostupné na uživatelském zařízení, konkrétně při první instalaci 500GB paměti a dalších 5-10GB měsíčně, pakliže není aktivována funkce prořezávání (pruning), která eliminuje potřebu stahovat a zaznamenávat staré, již proběhlé transakce a tím dojde k menší zátěži na paměť. Tato možnost se spíše doporučuje náročnějším/šouravějším uživatelům, kteří se chtějí přiblížit, co nejbližší k samotnému jádru systému. Pro ty, kteří nevyužijí desktopového rozhraní a pořád si chtějí uchovat možnost nahlédnout do blockchainu tu existuje například stránka Blockchain.info, která umožňuje nahlížení do ledgeru bez nutnosti cokoli stahovat a instalovat.

Mezi další možnost desktopových peněženek je dle Stroukala a Skalického (2018), ale i dle oficiální bitcoinové stránky bitcoin.org (2024) program Electrum, který je dostupný na webové stránce electrum.org, jehož zaměření je na rychlost a jednoduchost s nízkou spotřebou zdrojů. Používá vzdálené servery, které se starají o nejsložitější části Bitcoinového systému, a umožňuje obnovit peněženku s pomocí tajné fráze (seed). Stejně tak jako oficiálního bitcoinového klienta, tak i Electrum poskytuje naprostou kontrolu nad finančními prostředky, operuje na bázi open-source, což kterémukoliv vývojáři umožňuje nahlédnout do jádra celého programu, tak aby si sám mohl ověřit, že program neschovává žádné tajnosti. Zároveň má funkci dvojitého ověření (2FA) – funkce, která vyžaduje minimálně dvou účtů nebo zařízení k udělení přístupu. Po stažení a instalaci programu, program ihned vybere k vygenerování peněženky a zároveň se odkáže, na jaké místo má uložit soubor s klíči k bitcoinům. I samotný soubor s klíči je po vyzvání programu možné ihned zabezpečit heslem a přidat mu tak o úroveň ochrany navíc. To zásadní je, že program vygeneruje dvanáct slov, která poslouží při ztrátě nebo poškození zařízení, tak aby byl znovu poskytnut přístup k bitcoinům. Samotné uživatelské rozhraní je jednoduché, nabízí kolonky s historií plateb a kolonky pro příjem nebo odeslání bitcoinů s možností vygenerování QR kódu. Pro usnadnění rozhodování mezi desktopovými peněženkami se ještě nabízí Armory, které se prezentuje dle Armory (2024) jako: *„nejbezpečnější a nejkomplexnější řešení, které je k dispozici uživatelům a institucím pro generování a ukládání soukromých klíčů Bitcoinu.“* Platby se provádí skrze internetovou síť, avšak privátní klíče jsou uloženy na off-line počítači, a tím je značně redukováno riziko útoků hackerů.



Mezi uživatelsky nejpřívětivější se řadí mobilní aplikace do chytrých mobilních zařízení, které umožňují rychlý přístup k vlastním penězům. Mezi jednu z nejlepších aplikací se řadí Unstoppable, která je pro uživatele jak androidových operačních systémů, tak i těch, kteří mají iOS. Její výhody spočívají v (Unstoppable – Bitcoin & Crypto Wallet, 2024):

- naprosté kontrole nad prostředky;
- možnosti spravovat vícero peněženek;
- decentralizaci;
- DeFi peněženec;
- analytických údajích o trhu;
- možnosti přijímat/odesílat a uchovávat NFT.

Stroukal a Skalický (2018) zmiňují, že dobrou mobilní kryptoměnovou peněženkou je i Coinomi, Podle stránky Coinomi (2024) u které jsou její značné výhody hlavně v:

- nepřetržité zákaznické podpoře;
- cross-platform využití mezi vícero zařízeními (Android a iOS pro mobilní zařízení/desktopová zařízení);
- zabudované směnárně, která funguje tak, že spojuje uživatele, kteří mají zájem prodat a ty, kteří mají zájem koupit;
- SegWit;
- Passphrase.

Nejbezpečnější a doporučenou volbou je zvolit hardwarových peněženek, které se podobají USB flash diskům. Používají tak, že se připojí do počítače pomocí kabelu nebo přes Bluetooth, a i když transakce reálně provádí přes obrazovku počítače, samotné potvrzení transakcí je již procesem odehrávajícím se mimo počítač přímo v zabezpečeném zařízení, protože penženka generuje privátní klíče bezpečně v režimu off-line a nikam je neodesílá. Pokud se hardwarová penženka poškodí nebo ztratí, je jednoduché ji obnovit pomocí seedu, který je získán při prvním spuštění zařízení a je nutné ho zapsat na bezpečné místo.

Jak Stroukal a Skalický (2018), tak i Finex.cz (2024) se zmiňují o Trezoru – penženka české firmy Satoshi Labs s.r.o., která se začala věnovat výrobě hardwarových peněženek poté, co jí samotné bylo odcizeno několik tisíc bitcoinů. Jednou z tří nabízených

hardwarových peněženek je Trezor Safe 3, který sedí na cenovém středu mezi zbylými dvěma. Podporuje bitcoin a většinu altcoinů a zároveň je kompatibilní se všemi desktopovými operačními systémy a stejně tak i s těmi mobilními. Rozhraní spočívá v malém monochromatickém displeji, který spoléhá na dvě tlačítka. Stejně tak jako Coinomi, tak i Trezor Safe 3 nabízí passphrase jako druhou vrstvu zabezpečení. Uživateli je po prvním připojení zařízení k počítači stažen plugin k webovému prohlížeči, který přenesení uživatele do rozhraní blízkému tomu, jaké je v internetovém bankovníctví. V tomto prostředí se zadávají transakční detaily a samotný podpis platby už probíhá mimo něj na zařízení Trezor (Kryptoměnové peněženky – Jak vybrat tu správnou? Kompletní srovnání pro rok 2024, 2024).

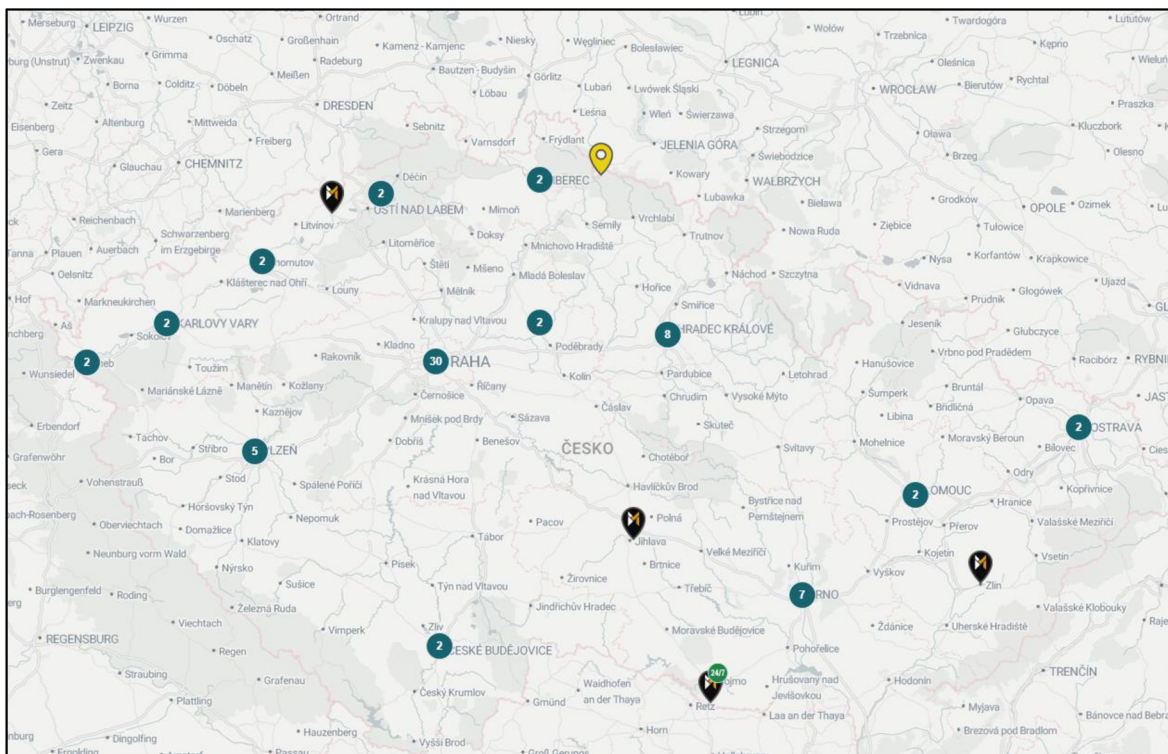
### **Směnové nástroje a platformy**

Dle Stroukala a Skalického (2018) i Hanuše (2023) jsou čtyři způsoby, jak koupit bitcoin, a to skrze:

- Bitcoinové bankomaty;
- Local;
- Bitcoinové směnárny;
- Bitcoinové burzy;
- CFD obchodování s kryptoměnami.

Dle Stroukala a Skalického (2018) a InvestPlus (2024) je nejpohodlnější cestou jak si opatřit svůj první bitcoin jsou Bitcoinové automaty, ke kterým stačí mít peněženku a QR kód s odkazem na adresu peněženky, který stačí jen přiložit ke čtečce bankomatu. Pak už jen stačí vložit peníze v požadované výši, které automat v daném kurzu a s marží (poplatkem) přepočítá. Nevýhodou jsou značně vysoké poplatky, které jsou zahrnuty ve směnných kurzech a při menších částkách nevyplácí (v rozmezí 5 % a 10 %). Kromě variabilního poplatku je tu i fixní poplatek, který je ve výši 50 až 200 Kč. Výhodou pak je obchodování bez registrace, pakliže se jedná o menší výši, a pakliže uživatel nevlastní již peněženku Bitcoinový automat mu novou v papírové podobě přidělí. Na papíře bude obsažen veřejný klíč a soukromý klíč. V ČR jich stojí již desítky, konkrétně již 73 (viz obrázek 8), a kromě Bitcoinu si lze zakoupit i jiné kryptoměny.

**Obrázek 8 Síť Bitcoinových automatů v ČR**



<https://coinatmradar.com/country/57/bitcoin-atm-czech-republic> (1.3.2024)

Stroukal a Skalický (2018) se zmiňují o dalším snadném způsobu, jak získat bitcoin, a tím je tzv. local (face-to-face). Předkládají návrh na využití serveru localbitcoins.com, avšak po prohledání se uživatel dozví, že kvůli poklesu objemu transakcí a podílu na trhu musel být tento projekt ukončen. Existuje však alternativní možnost – Vexl. Stejně tak jako LocalBitcoins, tak i Vexl nabízí možnost obchodovat P2P s Bitcoinem, jde tak o kompletně anonymizovanou formu domlouvání obchodů s Bitcoinem. K založení účtu v mobilní aplikaci stačí jen telefonní číslo, které slouží jako ochrana před falešnými útočníky a boty. SMS zprávou přijde potvrzovací kód, zvolí se přezdívka a profil je nastaven. Zprávy jsou šifrované a párované, zprávy mají svůj veřejný a privátní klíč, stejně tak jako Bitcoinové adresy. Aplikace nabízí inzertní místo, kde se zadá nabídka nebo poptávka s popisem požadované transakce (měna, množství, lokalita, online nebo osobně, platební měna a spouštěče, které inzerát uveřejní, jako například dosažení určité ceny bitcoinu, a ještě možnost volby převodu pomocí on-chain nebo Lightning Networku). Jestliže je nabídka přijata, tak pak už vše zbývá na domluvě. Opatrnost si vyžaduje samotné setkání (face-to-face), i přes možnost odhalení si vzájemné identity v aplikaci, uživatel nikdy neví, koho potká osobně. Cena, kterou uživatel platí za naprostou svobodu při tomto způsobu. Doporučení – potkat se na veřejném místě a vzít s sebou někoho dalšího (informovat o této

skutečnosti protistranu). Výhody aplikace Vexl spočívají hlavně v možnosti zvýšení likvidy a její nevýhodou je především limit plateb, který lze provést v hotovosti a možnost referencí, kterou například LocalBitcoins poskytovala (Recenze aplikace Vexl, 2024).

Podle Stroukala a Skalického (2018) jsou specializované směnárny dobrým a rychlým způsobem, jak pořídit bitcoiny. Zmiňují se o simplecoin, která je největší směnárnou kryptoměn působící v ČR od roku 2013. Stačí mít svou kryptoměnovou peněženku s adresou, zaregistrovat se skrze emailovou adresu a heslo (lze i bez nutnosti registrace, avšak uživatel přichází o jisté množstevní slevy) a pak už jen zbývá zadat objednávku. Emailem zaslané pokyny k platbě přijdou po zadání objednávky a samotná transakce bitcoinů za fiat měny proběhne po obdržení platby průměrně do 30 min. Nevýhodou je, že platby lze bez určitých požadavků na ověření uživatele provádět jen do výše 200 € a to v rozmezí deseti dnů, pak je vyžadována, kromě povinné registrace, i fotografie osobních dokladů, selfie s dokladem, ověřovací platba a telefonát, prokázání účelu transakce a při výši přesahující 10 000 € už i nutnost doložit příjmy (Simplecoin, 2024).

Obrázek 9 ukazuje, jaká je relativní výše poplatků u bitcoinových automatů, směnárny Simplecoin a burzy Coinmate.

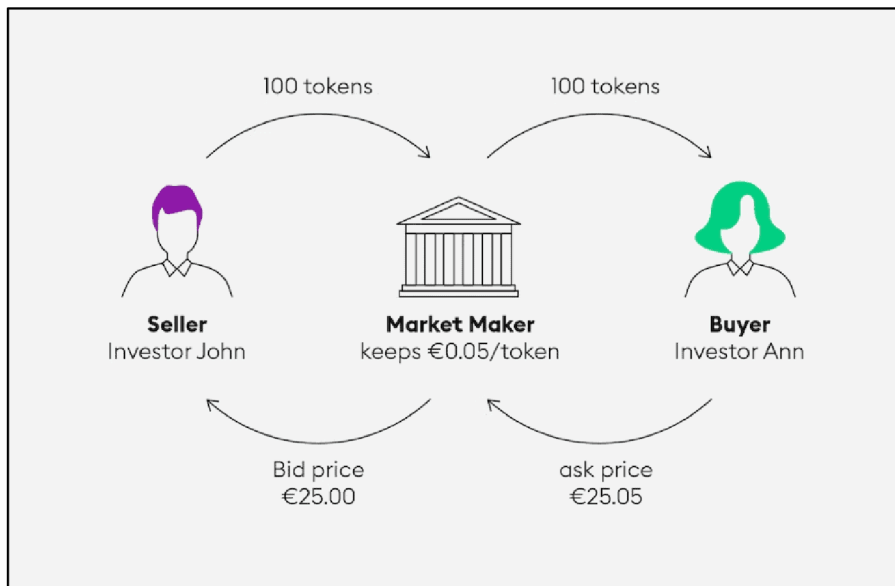
**Obrázek 9 Relativní výše poplatků při zpracování transakce u kryptoměnových automatů, směnárny a burz**

	<b>Bitcoin</b>	<b>Ethereum</b>	<b>Litecoin</b>
<b>ATM (WBTCB)</b>	7 %	7 %	–
<b>ATM (Bitcoinmat.sk)</b>	7 %	8 %	8 %
<b>ATM (General Bytes)</b>	5 %	–	7 %
<a href="#">Simplecoin</a>	2.1 %	2.1 %	2.1 %
<a href="#">Coinmate</a>	0.5 %	0.6 %	0.7 %

<https://investplus.cz/kryptomeny/bitcoin-bankomaty> (1.3.2024)

Kromě obchodování na specializovaných směnárnách je forma nákupu skrze specializované burzy to lepší volbou. Umožňují provedení obchodu některého z měnových párů, například BTC-USD, BTC-EUR, ale i nákup a prodej bitcoinu za jiné kryptoměny. Pakliže se naskytuje situace, kdy uživatel chce ve větším množství a frekventovaněji provádět nákup nebo prodej, tak by měl zvolit burzy, kde může i vyzkoušet trading. Na burze se střetávají ti, co chtějí prodat a ti, kteří chtějí nakoupit. Obchod zprostředkovává tzv. „Market maker“, kterým je většinou instituce spolupracující s burzou a dodávají tak na likviditě. Market maker umožňuje plynulý chod burzy a za své služby si účtuje spread, který tvoří fixní poplatek (viz obrázek 10) (Doležal, 2024).

**Obrázek 10 Role Market maker na burze**



<https://finex.cz/rubrika/kryptomeny/burzy> (11.3.2024)

Doležal (2024) uvádí poplatky, které se vyskytují na burzách zahrnují kromě poplatku pro market maker ještě další, například:

- taker poplatek, který se liší od maker poplatku tím, že je vykonaný okamžitě;
- poplatky za vklady a výběry;
- minimální měsíční poplatky;
- poplatky v síti (blockchain) za odesílání a výběr kryptoměn z burzy těžařům.

Stroukal a Skalický (2018) a Pfolio (2023) se zmiňují o dalším způsobu, který se nabízí při využití kryptoměnových burz nebo brokerů. Mezi největší světové burzy se řadí Binance. Její výhody jsou české uživatelské prostředí, nízké poplatky a možnost pokročilých funkcí. Mezi hlavní nevýhodu však pomalá zákaznická podpora. Nabízí základní a pokročilou platformu, které v obou případech spolehlivě fungují bez zamrzání. Účet lze vést v kryptoměnách, případně v eurech nebo amerických dolarech. Kromě bitcoinu si uživatel může zakoupit další kryptoměny, kterých je téměř 150. Mezi další kryptoměnových burzy se řadí česká Coinmate burza, která vznikla v roce 2014. Mezi její jednodušší a pokročilejší platformou je hlavní rozdíl v tom, že ta základní funguje jako směnárna, která umožňuje obchodovat za aktuální kurz, na rozdíl od té pokročilejší, která funguje jako klasická burza (stejně tak tomu je i u Coinbase). Výhodou jsou nízké poplatky a možnost vést účet v českých korunách, případně kryptoměnách nebo eurech. Nevýhodou je kupodivu chybějící

čeština, přestože společnost vznikla v ČR, tak jej nenabízí a velmi nízký objem obchodovaných aktiv (6). Jednou z burz, která patří vůbec k nejstarším je Bitstamp. Její vznik se datuje k roku 2011 a prošla si tak už časovým testem. Počet kryptoměn je zde velmi omezený (5), ale její dlouholetá historie je něco, čeho si uživatelé nejvíce vychvalují. Nabízí nízké poplatky a kvalitní platformu, která je vedena ale pouze v anglickém jazyce. Z řad nevýhod se dá vypíchnout absence demo účtu a pomalá zákaznická podpora. Ať už si uživatel vybere jakoukoliv burzu, tak by měl dávat pozor na:

- transparentnost obchodních podmínek;
- snahy chránit uživatele a jejich data;
- výši poplatků;
- likviditě burzy (problém burzy FTX);
- recenze od ostatních uživatelů;
- přehlednosti platformy a uživatelského rozhraní.

S pádem burz přišli mnozí o své bitcoiny nenávratně. Děje se to i v současnosti, kdy uživatelé své peněženky dostatečně nezabezpečí nebo využívají při větším množství stále nedostatečné ochrany. Prolomit Bitcoinový protokol a zaútočit na celý systém je prakticky nemožné (51 % útok na Bitcoin), avšak napadnout jednotlivé uživatele už takovým problémem pro útočníky není. Využijí škodlivého souboru, který může být součástí přílohy elektronické komunikace a v ten okamžik získají skrytou kontrolu nad počítačem, ze kterého extrahují bitcoiny uživatele a převedou si je na vlastní peněženku (Stroukal, & Skalický, 2018).

Z řád brokerů lze doporučit XTB, který sice nabízí omezené množství kryptoměn, za to je regulovaný mimo jiné Českou národní bankou, což mu dodává na důvěře. Online založený účet nabízí možnost demo účtu a kompletní podporu v českém jazyce, což značně zpřehledňuje orientaci na platformě. Zkušený obchodník jistě ocení možnost obchodování s pákou. Nevýhodou takovýchto platforem, jako je XTB, že uživatel nikdy nevlastní své bitcoiny, vše je v rukou třetí strany.

Tabulka 8 zobrazuje jednoduché doporučení dle výše hodnoty, způsobu pořízení a formy držení bitcoinu.

**Tabulka 8 Doporučení pro držení bitcoinu dle výše hodnoty, způsobu pořízení a formy držení**

<b>Výše hodnoty bitcoinu</b>	>10 000 Kč	>10 000 Kč <100 000 Kč	>1 000 000 Kč
<b>Způsob pořízení</b>	Simplecoin	Coinmate	Bitstamp
<b>Forma držení</b>	Unstoppable; Coinomi	Trezor	Trezor

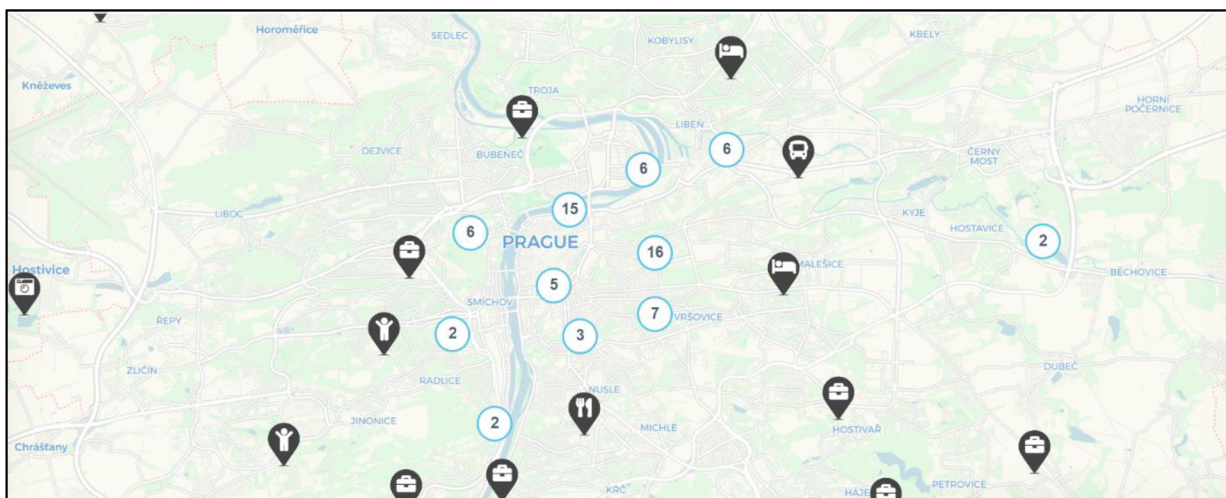
Zdroj: převzato z Bitcoin a jiné kryptopeníze budoucnosti (Stroukal, & Skalický, 2018)

### **Praktické aspekty užívání**

Pakliže se uživatel rozhodne své bitcoiny využít k platbě, není nic jednoduššího než si otevřít webové stránky [coinmap.org](http://coinmap.org) (viz obrázek 11), které ukazují všechny obchodníky s kryptoměny a kryptoměnové bankomaty nejen v ČR, ale i v zahraničí. Pokud chce uživatel utratit své bitcoiny za zábavu, lze tak učinit dle [coinmap.org](http://coinmap.org) (2024) například při hraní únikových her ([escapetheroom.cz](http://escapetheroom.cz)) nebo v kině Bio Oko ([biooko.net](http://biooko.net)) na pražských Holešovicích. Platbu bitcoiny za občerstvení nabízí například Paralelní polis ([paralelnipolis.cz](http://paralelnipolis.cz)), které sdružuje pod jednou střechou kavárnu, coworkingové místo, Institute of Cryptoanarchy, které poskytuje vzdělávací programy, a od roku 2020 i online vysílání. Další z řad poskytovatelů občerstvení je Avocado Bistro ([avocadobistro.cz](http://avocadobistro.cz)), které na svých pobočkách také přijímá kryptoměny. Za ubytování lze zaplatit v síti hotelů a hostelů a&o ([aohostels.com](http://aohostels.com)). Kromě toho lze bitcoiny zaplatit i za produkty a služby jako fotografování, móda a design nebo například za elektroniku v pobočkách Alza.cz ([alza.cz](http://alza.cz)). Konkrétně Alza zprovoznila platby bitcoinem v roce 2017. Umožňuje provádět on-chain transakce, ale zároveň nabízí i platbu přes Lightning Network, který významně zvyšuje rychlost transakce a zároveň snižuje poplatky za provedení takové platby. Kromě placení Alza nabízí i samotný nákup bitcoinu přes bitcoinové automaty, které má ve svých prodejnách (V Alze zaplatíte i Bitcoiny, 2023).



**Obrázek 11 Obchodníci přijímající kryptoměny v Praze**



*<https://coinmap.org> (11.3.2024)*

Pro samotné obchodníky Bitcoin a bitcoinové platby přináší mnoho výhod, jak zmiňuje Krause (2023), tak některé z výhod jsou například:

- praktické nulové poplatky, které platí zákazník při provedení transakce;
- jednoduchost a zbytečnost terminálu;
- platbu nelze refundovat a nemůže se tak stát, že by zákazník později o ní požádal zpět;
- reklama a rozšíření povědomí.

Avšak Krause (2023) ještě zmiňuje, že není radno zapomenout na účetnictví a vykázání příjmu bitcoinem v nich.

Mimo nákupy za statky a služby, lze bitcoinem investovat, například na burzách a spekulovat na vývoj ceny. Také je možné jej uplatit při nákupu NFT, nemovitostí nebo při výplatě mezd. Jedna ze světově prvních bitcoinových transakcí na nákup nemovitosti proběhla v roce 2017, kdy ruský občan koupil byt v Praze za 35 bitcoinů, což zhruba v tu dobu činilo (po kurzovém přepočtu k datumu 21.12.2017) necelých 13 milionů korun (Čeperová, 2017).

### **Regulace, účetnictví a daně**

Stránka eToro (b.r.) popisuje, jak se liší regulace kryptoměn mezi jednotlivými zeměmi a regiony. Některé země mají přísné předpisy a zákony, zatímco jiné jsou otevřenější vůči kryptoměnám. Ve světě neexistuje jednotný přístup, jak regulovat a jak přistupovat ke kryptoměnám. Jsou si vědomi, že je třeba legalizovat tento platební instrument pod obavou

hrozeb daňových úniků, které plynou z neukotvení v právním řádu. Snaží se tak definovat pravidla, podle nichž by se transakce s kryptoměny mohly uskutečňovat. V zemích Severní Ameriky s Bitcoinem nemají problém, je legálním ve Spojených státech, Kanadě a Mexiku, ba i dokonce v Salvadoru začali využívat bitcoin jako legální platidlo, které je všude v zemi obecně přijímáno. Salvador se tak stal první zemí, která uznala bitcoin jako své zákonné platidlo poté, co jej parlament 7. září 2021 legislativně schválil (Bitcoin Law) („El Salvador’s Experiment with Bitcoin as Legal Tender”, 2022). V určitých státech Jižní Ameriky jsou svým přístupem odlišni, například v Brazílii nemají žádné regulace. V Argentině je zase vláda vnímá jako prostředek směny nebo uchovatele hodnoty. Naopak s utahováním kryptoměn jsou sžiti v Bolívii nebo Ekvádoru, kde zcela pragmatičtěji zakazují to, nad čím nemají kontrolu. Evropské státy obecně bitcoin akceptují, hledají přístup, jak jej regulovat při obchodování nebo zdanění. Například v Asii, konkrétně v Číně, jej významně regulují a omezují. Uživatelům zablokovali přístup ke kryptoměnovým burzám a významně tak omezili přístup k obchodování na kryptoměnovém trhu. V Japonsku kromě legality se považuje dokonce i za zákonné platidlo.

Regulaci v České republice provádí Česká národní banka, která zaujímá stanovisko vůči Bitcoinu, které jej definuje jako nehmotnou movitou věc, ne jako investiční prostředek, na který se dá uplatnit časový test jako tomu je u akcií, tzn. že je třeba danit veškeré výnosy nehledě na dobu držení (Regulace Bitcoinu ve světě, b.r.). K regulacím se ještě váže možná výše, kterou lze provést při transakci v hotovosti, například jako tomu je u face-to-face transakcí, které jsou zmíněny v možnostech pořízení bitcoinu. Výše hotovostní platby v jeden den je limitem stanovena na 270 000 Kč. Při jejím překročení je nutné provést platbu bezhotovostně a tato povinnost spadá na všechny fyzické i právnické subjekty v zemi (Česká republika, 2004).

Ti, kteří se nechtějí zabývat daněním kryptoměn se nabízí jednoduché řešení – Hodl, jinak řečeno držet a neprodávat. Pro ty, kteří by rádi přenechali své starosti v oblasti práva a zdanění kryptoměn, tak se nabízí možnost využít skupiny smpl (smpl.cz), která se zabývá daňově-optimalizační strukturou a daněním kryptoměn (Smpl, 2024).

Jak zmiňuje Michal Hanych et al (2018), tak zdanění u fyzických osob podléhají všechny příjmy, u kterých dochází ke zvýšení majetku, a to jak u příjmu peněžených, tak i nepeněžených. Jinak tomu není u směny, tzn.: „*že danění podléhá směna kryptoměny na fiat, za jinou kryptoměnu nebo pořízení zboží či služeb.*“

Dle Hanycha et al (2018) praxí finančních úřadů doposud byla, že danění podléhá ve fázi převodu kryptoměn zpět na fiat měnu, avšak to jen proto, že zákon není stavěný na velké objemy transakcí u fyzických osob, při kterých dochází k tak výrazné změně hodnoty i během jediného dne. Ke správě vlastních kryptoměn a obchodování s nimi není zapotřebí živnostenského oprávnění. To platí do doby, dokud nedochází k aktivní těžbě, která už takové oprávnění vyžaduje. Osvobození od daně z příjmu se vztahuje obecně u příležitostných činností, které nepřesáhnou výše 30 000 Kč (příjem, nikoliv zisk), avšak správa vlastního majetku není činností, která by spadala pod toto osvobození (muselo by se jednat o výpomoc, za kterou si jeden nechá vyplatit odměnu do 30 000 Kč). Osvobozeno od daně je i darování mezi příbuznými v přímé linii, některých v pobočné linii a manžela. Příjemce takového daru však musí nahlásit jeho přijetí, pakliže je hodnota kryptoměn k danému dni větší než 5 000 000 Kč. Jestliže obdarovaný kryptoměny prodá, zdanění se rozdíl ceny k okamžiku nabytí a cenou, za kterou prodej realizuje. Časový test, jako tomu je u cenných papírů nelze uplatnit na kryptoměny, tzn. že po uplynutí 3 let nedochází k osvobození od daně. Zdanění při prodeji by se uskutečnilo následovně podle obrázku 12.

**Obrázek 12 Příklad zdanění prodeje bitcoinu**

Nakoupili jste 1 BTC za 200.000 Kč. Po čase prodáte 1 BTC za 300.000 Kč. Dílčí základ daně podle § 10 bude 100.000 Kč (prodejní cena 300 000 – pořizovací cena 200 000). Daň bude 15.000 Kč (15 %), ale celková daňová povinnost se bude lišit podle vašich zbývajících příjmů. Můžete uplatnit slevu na dani na poplatníka apod.

*<https://www.zdanenikryptomen.cz/zdanenikryptomen.pdf> (10.3.2024)*

Při pořizování bitcoinu průběžně, lze využít dvou metod k výpočtu celkové pořizovací ceny:

- FIFO (first in, first out);
- metoda váženého aritmetického průměru.

Rozdíl v dílčím základu daně bude rozdílný podle vybrané metody (viz obrázek 13).  
**Obrázek 13** Výše dílčího základu daně při použití metody FIFO a metody váženého aritmetického průměru

*FIFO: Nakoupili jste 1 BTC za 100.000 Kč a 4 BTC každý za 50.000 Kč. Po čase prodáte 2 BTC každý za 200.000 Kč (celkově 400.000 Kč). Dílčí základ daně podle § 10 bude 250.000 Kč (prodejní cena 400.000 – pořizovací cena (100.000 + 50.000)).*

*Aritmetický průměr: Nakoupili jste 1 BTC za 100 000 Kč a 4 BTC každý za 50 000 Kč. Po čase prodáte 2 BTC každý za 200.000 Kč (celkově 400.000 Kč). Dílčí základ daně podle § 10 bude 280.000 Kč (prodejní cena 400.000 – pořizovací cena (300.000/5 \*2 = 120 000)).*

<https://www.zdanenikryptomen.cz/zdanenikryptomen.pdf> (10.3.2024)

Při častých transakcích, obzvlášť v případě obchodování na burze je podstatný až moment, kdy dochází k výběru prostředků do vlastní peněženky (Hanych et al, 2018).

#### 4.1.2 Naplnění podstaty prostředku směn

Bitcoin má potenciál se stát novou formou peněz, již dnes vykazuje minimálně 2 ze 4 fází vývoje z předmětu až na společností uznávanou formu peněz, tak jako tomu je v tabulce 9, která přesně znova popisuje jednotlivé fáze vývoje, stav a odůvodnění proč tomu tak je.

**Tabulka 9** Fáze vývoje Bitcoinu, aktuální stav a odůvodnění

Fáze vývoje	Stav Bitcoinu	Odůvodnění
<b>Sběratelský předmět</b>	✔	Mnoho lidí si jej uchovává kvůli jeho vzácnosti a vztahují k němu určité emoce, ať už ze zvědavosti, nadšení nebo naděje na lepší budoucnost a finanční nezávislost
<b>Uchovatel hodnoty</b>	✔	Je považován mnoha lidmi a investory za bezpečný prostředek k uchování hodnoty a ochraně proti inflaci
<b>Prostředek směny</b>	✘✔	Velmi omezeně, obecně se s ním dá obchodovat, avšak není ještě celospolečensky uznávaným platidlem, kterým by šlo zaplatit za zboží a služby
<b>Zúčtovací jednotka</b>	✘	Dosud neslouží jako něco, čím se vyjadřuje hodnota zboží nebo služeb, protože stále spíše dochází k přepočtu na fiat měnu

Zdroj: vlastní zpracování (2024)

Tabulka 10 následně popisuje vlastnosti, které by měl naplňovat dobrý uchovatel hodnoty, tak aby měl potenciál se stát všeobecně přijímanými penězi.

**Tabulka 10 Vlastnosti Bitcoinu, jakožto dobrého uchovatele hodnoty**

Vlastnosti	Stav	Odůvodnění
Trvanlivost	✓	Nepodléhá zkáze, jako tomu je u bankovek
Přenositelnost	✓	Snadné přenášení přes internet, rychlé a jednoduché transakce po celém světě
Zaměnitelnost	✓	Každý bitcoin je stejný jako každý jiný
Ověřitelnost	✓	Transakce jsou ověřovány v rámci blockchainu, což každému umožňuje nahlédnout do ledgeru a ověřit historii jednotlivých mincí
Dělitelnost	✓	1 bitcoin je dělitelný až na osm desetinných míst s nejmenší jednotkou 1 satoshi
Vzácnost	✓	Bitcoin má pevně stanovený omezený počet mincí, který je postupně uvolňován těžbou
Historická prověřenost	✗	Přestože si bitcoin prošel mnohými zkouškami, tak je svou dobou existence ještě na trhu krátko, avšak považuje se za hodnotné aktivum
Odolnost vůči cenzuře	✗ ✓	Decentralizovaný systém mimo kontrolu a dosah centrální autority. Využívá se v zemích s omezenou mírou finanční svobody, avšak je cílem státních regulací z důvodu nepochopení a strachu vlád

Zdroj: vlastní zpracování (2024)

#### 4.1.3 Komparace bitcoinu s tradičními fiat měnami a jinými formami majetku

Jak se bitcoin drží a jak si konkuruje s fiat měnami a zlatem je vyobrazeno na obrázku 14, který komparuje jednotlivé vlastnosti.

Obrázek 14 Bitcoin vs zlato vs fiat

	Bitcoin	Zlato	Fiat
Trvanlivost	B	A+	C
Přenositelnost	A+	D	B
Zaměnitelnost	B	A	B
Ověřitelnost	A+	B	B
Dělitelnost	A+	C	B
Vzácnost	A+	A	F
Historická prověřenost	D	A+	C
Odolnost vůči cenzuře	A	C	D

(Boyapati, 2023)

Jak zmiňuje Boyapati (2023), tak svou trvanlivostí nic nepřebije zlato, u kterého naprostá většina distribuované produkce přetrvala dodnes, a ještě tomu tak bude po tisíciletí. Co se týče Bitcoinu a fiat měn, tak se zde nehledí na nosič fyzické podoby (bitcoinové peněženky/mince a bankovky), ale jako na digitální záznamy, které jsou emitovány pod určitým subjektem. Fiat měny spadají pod libovůli centrálních bank a vlád, které je emitují. Z historického hlediska už mnoho fiat měn zaniklo, předcházelo tomu pád emitenta nebo vlády, případně chybou monetární nebo fiskální politiky, která neplnila své cíle a znehodnotila měnu do té fáze, kdy jí lidé přestanou věřit a přejdou na jinou měnu, případně na jinou formu majetku. Jedinou výjimkou je americký dolar a britská libra, které vznikly

ke konci 18. století a v případě libry ke konci 17. století. Bitcoin nevydává žádná centrální autorita a dokud bude fungovat protokol a budou tu tací, kteří udrží systém v chodu, tak téměř nic nebrání tomu, aby přetrval dále.

Svou schopností přenášet hodnotu na velkou vzdálenost bitcoinu nic nekonkuruje. Je totiž nejnáze přenositelným prostředkem k uchování hodnoty. Značné množství bitcoinů ve velké hodnotě lze poslat téměř okamžitě přes celý svět, aniž by bylo nutné kontroly a hlášení autoritám jako u fiat měn (digitální podoba). Hotovostní peníze s sebou nesou značné riziko při uchování, přepravě, ztrátě nebo odcizení. Zlato, ať už v podobě mincí nebo slitků je značně těžké a omezené ve své přenositelnosti, zároveň s sebou také rizika stejně tak jako tomu je u fiat měn.

Zlato je sice vysoce zaměnitelné, taková mince přetavená zlatého slitku bude stejná jako každá jiná, ale za to zlato může být ovlivněno příměsemi, a tak může docházet k úpravě ryzosti. Takové mince pak nemusí být na první pohled rozpoznatelné a je třeba verifikovat jeho ryzost u odborníků, ať už podle magnetického testu nebo testy hustoty (Boyapati, 2023). Nevýhoda zlata může plynout z jeho původu, protože takový slitek, který podléhá trestné činnosti lze jednoduše přetavit nebo roztavit na menší díly, u kterých hledání jejich původu bude téměř nemožné. Bitcoinové mince jsou značně zaměnitelné za jiné, pakliže ale dojde u jiných mincí spětí s trestnou činností, mohou být obchodníci donuceni, aby tyto bitcoiny nepřijímali. U bitcoinu je v ledgeru vidět, odkud jednotlivé bitcoiny putovaly do peněženky příjemce. Bitcoin je tak vysoce ověřitelný a každý má tu možnost nahlédnout do historie jednotlivých mincí. U fiat měn je pak zaměnitelností limitován jen tím, jak moc je obchodník ochotný je přijmout. Například taková pětistícová bankovka není moc vítanou mezi obchodníky. Za to ověřitelnost fiat měn je v praxi celkem různorodá, bankovky a mince obsahují určité bezpečnostní prvky, které je nesnadné falzifikovat, avšak pořád dochází k případům, kdy se tomu tak stane. Na základě statistiky vydané Českou národní bankou tomu tak činilo v roce 2023 u 3539 případů bankovek a mincí s nejčastěji padělanými bankovkami v nominální hodnotě 5 000 Kč (Kubelková, 2024).

Bitcoin se dá dělit až na jeden satoshi, který představuje  $10^{-8}$  BTC (1 satoshi = 0.000000001 BTC) (viz tabulka 11). Posílat takové množství po síti se sice ekonomicky nevyplácí (kvůli poplatkům), ale je to možné (Stroukal, & Skalický, 2018). U fiat měn, konkrétně u českých korun, je nejmenší dělitelnost hotovostní jednotkou 1 Kč a u bezhotovostní podoby 1 halíř, což je z hlediska praktického užití dostatečné. Zlato se dá dělit

až na zrnka zlata, které se stejně neprodává v menším množství než 1 gram, který v přepočtu na české koruny (k datu 12.3.2024) činí 1612 Kč (Zlato – aktuální cena zlata, 2024).

**Tabulka 11 Existující odvozené jednotky bitcoinu**

Jednotka	Hodnota v BTC
<b>BTC</b>	1
<b>Centibitcoin</b>	0,01
<b>Milibitcoin</b>	0,001
<b>Mikrobitcoin</b>	0,000001
<b>Satoshi</b>	0.000000001

Zdroj: převzato z Bitcoin a jiné kryptoměny budoucnosti (Stroukal, & Skalický, 2018)

Jsou současné bankovky a digitální peníze ještě vůbec vzácné, pokud je možné je natisknout v libovolném požadovaném množství téměř kdykoliv, podle libovůle centrálních bankéřů (Stroukal & Skalický, 2018)? Neustálé navyšování peněžní nabídky vede k nafukování peněžní zásoby a k znehodnocení úspor lidí. Zlato je odjakživa vzácné, ale jeho zásoba se dá navyšovat a jsou tu teoretické způsoby, jak zvýšit jeho celkovou zásobu (těžení z mořského dna nebo asteroidů) (Boyapati, 2023). Za to bitcoinu více nebude, neumožňuje tomu tak Bitcoinový protokol, který limituje celkovou zásobu na 21 milionů bitcoinů.

Zlato prošlo už dlouhým časovým testem – a ustálo ho. Pořád je validním uchovatelem hodnoty, avšak ztratilo podstaty prostředku směny nebo zúčtovací jednotky. Nejstarší fiat měny jsou tu již stovky let, také se dá říci, že prošly značnou časovou zkouškou, avšak už od jejich zrodu měli panovníci pokušení k jejich znehodnocování, například ubráním na ryzosti a přimícháním jiným kovů. Krátkodobě si svou hodnotu uchovávají, avšak inflace vždy podemele jejich hodnotu.

Bitcoin naprosto předčil zlato a fiat měny, co se týče odolnosti vůči cenzuře. Není pod kontrolou centrální autority nebo vlády. Transakce probíhají přímo mezi účastníky sítě a jsou chráněny kryptografií. Zlato má fyzickou podobu, která je náchylná například na konfiskaci (Boyapati, 2023). Vládní regulace a zákony mohou omezit jeho prodej,



vlastnictví nebo přepravu. Přepravovat zlaté slitky napříč státy určitě není jednoduchou záležitostí, zatímco Bitcoin (privátní a soukromé klíče) stačí mít klidně i na kusu papíru. Fiat měny podléhají kontrole a regulacím ze strany emitenta. Banky samotné musí hlásit veškeré „podezřelé“ platby a případně jednotlivé transakce nebo účty úplně zakázat nebo uzavřít.

## 4.2 Bitcoin jako investiční aktivum

Ponechat peníze negativním vlivům inflace a neinvestovat je, představuje ušlou příležitost pro každého investora, který chce aspoň do určité míry své peníze ochránit nebo případně zhodnotit. Bouška (2023) vysvětluje, jak se Bitcoin stává stále atraktivnějším investičním nástrojem pro různé typy investorů, kteří hledají:

- **ochranu před inflací** (znehodnocování peněz);
- **diverzifikaci investičního portfolia**;
- **růstový potenciál** s vidinou vysokého zhodnocení;
- **spekulativní aktivum**, kde můžou profitovat z vysoké volatility.

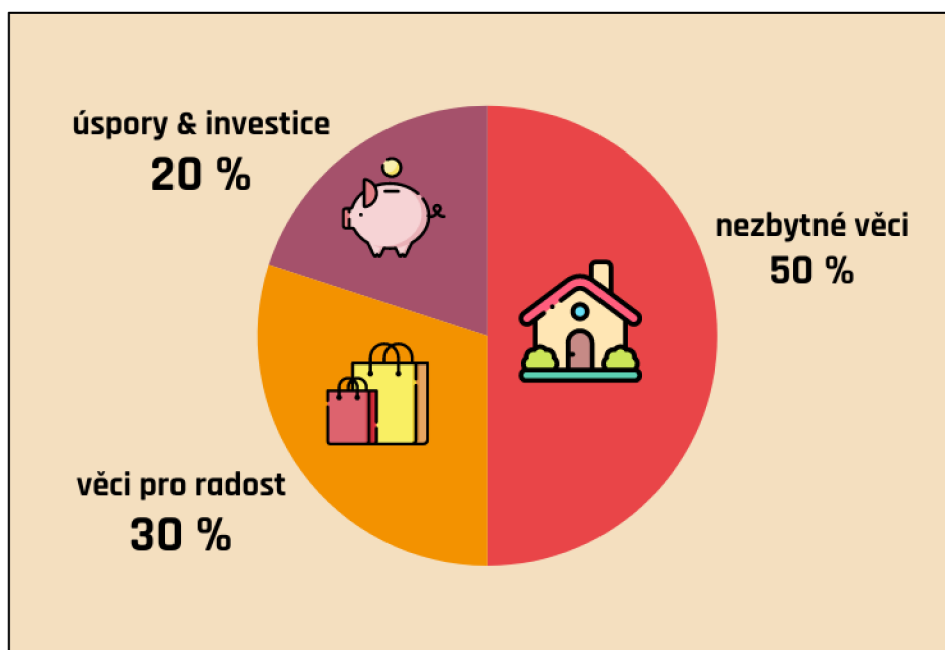
Investování do Bitcoinu se stalo atraktivním pro mnohé, ať už pro zkušené, tak i pro nové investory. Pro ty, kteří se rozhodnou investovat bez plánu, může být takové investování riskantní a podobné hazardu. Každá investice nese rizika, a zejména kryptoměny jsou považovány za spekulativní aktivum. Historická zhodnocení Bitcoinu s sebou přitáhlo pozornost mnoha lidí a zejména investorů. Nicméně minulost také ukázala, že cena Bitcoinu může prudce klesnout, což může přinést ztráty těm, kteří jsou ovlivněni emocemi. Investice do kryptoměn by měla být prováděna s rozvahou a s vědomím, že je možné ztratit většinu nebo všechny zainvestované prostředky.

Proto je důležité dodržovat několik zásad a doporučení při investování do Bitcoinu (Jak investovat do Bitcoinu, b.r.):

- **být disciplinovaný** – nedovolit emocím ovlivnit obchodování;
- **nečasovat trh** – vyhnout se pokusům časovat nákupy a prodeje na základě krátkodobých výkyvů cen;
- **diverzifikovat riziko** – rozložení investic mimo Bitcoin aktivity, které mají odlišnou korelaci s Bitcoinem, tak aby při poklesu neklesala hodnota celého investičního portfolia;
- **investovat podle možností** – stanovit investovanou částku, kterou je investor ochoten a schopen ztratit, aniž by ovlivnila jeho finanční stabilitu nebo životní úroveň (Pravidlo 50:30:20).

Pokud jde o množství finančních prostředků, které je investor ochoten riskovat, je dobré se řídit zlatým pravidlem 50:30:20 (viz obrázek 15), které ukazuje, jak rozdělit příjmy a výdaje v měsíční peněžní bilanci. Podle tohoto pravidla by se 50 % mělo věnovat na nezbytné a často fixní výdaje, jako jsou životní náklady (bydlení, potraviny, léky a další), 30 % na zábavu, volný čas, cestování a na věci zbytné povahy, a zbývajících 20 % na investice a spoření (Zkroťte své peníze: jak sestavit osobní nebo rodinný rozpočet, 2022).

Obrázek 15 Pravidlo 50:30:20



Pokud si investor vytvořil alespoň tříměsíční rezervu, může začít uvažovat o dalších investicích. Pro minimalizaci rizika je užitečné stanovit investiční strategii, která zahrnuje alespoň tři aktiva, do kterých bude investor pravidelně investovat. Co se kryptoměn týče, obecně se doporučuje, aby představovaly 5-10 % celkové hodnoty investičního portfolia. Dále je důležité si uvědomit, že investování není krátkodobým procesem, který by měl trvat dny, týdny nebo měsíce, ale spíše roky. Investoři musí být trpěliví a počítat s tím, že výnosy z investic se projeví až v delším časovém horizontu. Pokud investor není ochoten tento přístup přijmout a místo toho se snaží krátce profitovat na kolísání trhu, není to investování, ale spíše spekulace nebo hazardní hra (Jak investovat do Bitcoinu, b.r.).

Krátkodobé investování přináší řadu výhod a nevýhod. Výhody jsou zejména:

- potenciální vysoký zisk;
- rychlá likvidita pozic;
- vyhodnocování ukazatelů může pomoci lépe načasovat vstupy a výstupy.

Nevýhody:

- vysoké riziko;
- emoční rozhodování;
- náklady spojené s poplatky za likvidování pozic.

#### 4.2.1 Krátkodobá investiční strategie

Krátkodobé investování je zaměřováno na správné načasování trhu, vyhledávání trendů a spekulaci s cenami. I když se jedna ze zásad investování týká časování (nečasování) trhu, při podstatě krátkodobé investiční strategie je vyžadován opak. Zde je kritická schopnost být disciplinovaným a udržovat emoce pod kontrolou. Tato strategie je prováděna následujícími metodami:

- **obchodování na základě technické analýzy** – přání investora vidět v grafu určité souvislosti a předpokládat, že se pomocí prodloužení čar trh zachová tak, jak by si přál;
- **obchodování na základě událostí** – zprávy a výroky ovlivňující chování investorů (např. výroky Elona Muska; vysoce spekulativní).

## Obchodování na základě technické analýzy

Technická analýza se zaměřuje na analýzu cenových grafů a historických dat za účelem identifikace trendů a vzorů, které mohou naznačovat vývoj budoucí ceny. Investor využívající poznatků technické analýzy bude interpretovat výsledky jinak než ten druhý. Základní myšlenkou je, že se cena nepohybuje libovolně a místo toho každý pohyb ceny skrývá nějaký příběh, z kterého lze předpovědět, co se stane příště. Příběh si investor vyloží pomocí grafů a indikátorů.

Indikátory, které se běžně užívají pro účely technické analýzy jsou například (Nambiampurath, 2024):

- **Simple Moving Average (SMA; jednoduchý klouzavý průměr)** – vypočítání součtu řady cen a vydělení počtem datových bodů (viz graf 1);
- **Relative Strength Index (RSI; index relativní síly)** – matematicky znázorněný vzorec, který ukazuje, jestli je aktivum překoupené nebo předprodané.

**Graf 1** Příklad Simple Moving Average při obchodování BTC na burze Bitstamp



Zdroj: vlastní zpracování na platformě TradingView (15.3.2024)

Osa  $x$  zobrazuje datumové rozpětí a osa  $y$  rozsah hodnoty ceny bitcoinu. Modrá křivka na svíčkovém grafu vykresluje pohyb průměrné ceny bitcoinu a tím pomáhá určit směr trendu.

Každá svíčka má své charakteristiky:

- **tělo svíčky** – otevírající a zavírající pozici, například během jednoho obchodovacího dne;
- **knot** – ukazující maximum a minimum pohybu ceny během dne;
- **barvu** – indikující pohyb ceny nahoru (zelená) nebo dolů (červená).

Krátkodobé investování s rychlou likvidací pozic se silně subjektivní proces.

Podle zjištění, které přinesla burza na obchodování s CFD eToro, tak mediánová ztráta 90 % investorů je 36,3 % jejich obchodních účtů (Paulson, b.r.), proto je třeba zvážit schopností a možností každého investora.

#### 4.2.2 Dlouhodobá investiční strategie

Spočívá na principu dlouhodobého držení bitcoinu se zaměřením na dlouhodobý růst a budoucí výnosy plynoucí z investice. Důraz je kladen na dlouhodobě udržitelné investice a diverzifikaci portfolia bez spekulativního obchodování. Tato strategie je vhodná pro investory začínající nebo pro investory pasivní povahy, kteří se chtějí zabezpečit proti emocím, které při vysoké volatilitě vedou k neuváženým rozhodnutím vymykající se jejich osobní investiční strategii. Metody pro tuto strategii jsou následující:

- **All-in** – jednorázová velká investice, která spoléhá na správné načasování trhu. Investice se dlouhodobě nemusí vyplatit, pakliže je nákup proveden těsně před zlomem a propadem ceny;
- **Dollar Cost Averaging (DCA)** – průměrování nákladů investováním stejné částky peněz v pravidelných intervalech;
  - **Stock-to-Flow** – model predikující vývoj ceny na základě celkového cirkulovaného množství bitcoinů a toku nově vytěžených bitcoinů každý rok.

#### **All-in**

All-in metoda se obecně nedoporučuje kvůli vysokým rizikům plynoucím z nesprávného načasování trhu, avšak při správném načasování se hodnota vysoce zvýší.

## Dollar Cost Averaging

Jako spolehlivou metodou pro dlouhodobou investiční strategii se jeví metoda DCA. Stanovením stejné částky, která se investuje v pravidelném intervalu, většinou týdenním nebo měsíčním. Nákup bitcoinu probíhá neohledě na cenu a vývoj na trhu.

Podle Hájka (2022) investování s pomocí DCA funguje pouze v případě, kdy hodnota bitcoinu trvale roste. Zmiňuje, že DCA metoda historicky fungovala na akciové indexy a věří, že stejně tak tomu bude i u bitcoinu, který tuto tendenci vykazuje. Výhody spočívají hlavně v:

- minimalizaci rizika;
- nízké počáteční investici;
- šanci nakupovat ve slevě.

A mezi nevýhody řadí:

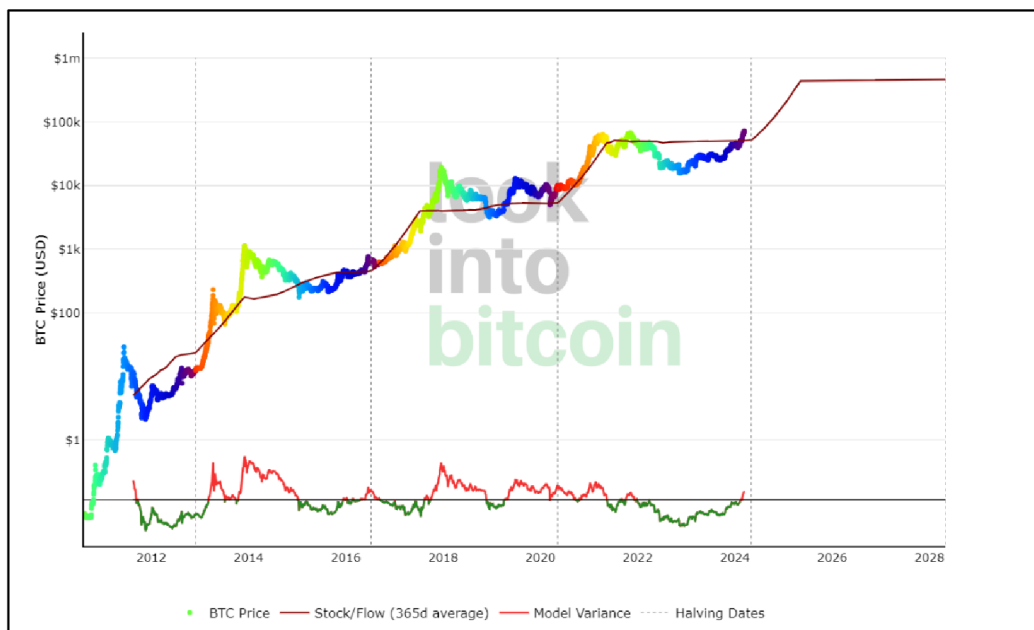
- eliminování nákupu propadů (dips);
- pomalý růst hodnoty investice;
- nižší výnosy v bull marketu.

Burza, která nabízí investování s DCA je například česká burza Coinmate.io, která ve spolupráci s webem Štosuj.cz umožňuje nastavit pravidelný nákup v týdenním nebo měsíčním intervalu (Hájek, 2022). Propojení účtu na webu s burzou je otázka několika minut.

## Stock-to-Flow

Mezi modely k popisování a predikování trhu se řadí model Stock-to-Flow (viz obrázek 12), který se dlouhodobě jeví jako užitečným nástrojem pro každého, kdo plánuje investovat do bitcoinu (Best Bitcoin Investing Strategy for 2020, 2020). Dokázal předpovědět velké cykly, které historicky trvají čtyři roky, při kterých dochází ke střídání bull a bear marketu. Cykly se doposud opakují, jen dochází k relativní změně vývoje ceny a ke změně době trvání bull a bear marketu.

Graf 2 Stock-to-Flow model



*www.lookintobitcoin.com (13.3.2024)*

Jednou z hlavních výhod modelu S2F je způsob, jakým jasně ukazuje, kdy je bitcoin podhodnocený nebo nadhodnocený, a to porovnáním očekávané hodnoty bitcoinu s jeho aktuální tržní cenou. Pokud je tato hodnota vyšší než aktuální tržní cena, lze bitcoin považovat za podhodnocený, zatímco pokud je očekávaná hodnota nižší než aktuální tržní cena, lze jej považovat za nadhodnocený („Best Bitcoin Investing Strategy for 2020”, 2020).

#### 4.2.3 Komparace investičních strategií

Stanovená celková výše investice, která slouží pro stanovení efektivnosti dlouhodobého investování za pomoci strategie All-in a Dollar Cost Average, je s maximální odchylkou 21 Kč. Výše investovaných nákladů nepřevyší v součtu 39 000 Kč.

Tabulka 12 obsahuje data k jednotlivým datům, které jsou použity pro výpočet zhodnocení bitcoinového investičního portfolia.

**Tabulka 12 Údaje o datumu počáteční investice, časovém rozpětí (od první investice až po poslední/zhodnocení), hodnotách ceny BTC, směnného kurzu k danému datu**

Datum počáteční investice	Časové rozpětí	Hodnota BTC v USD	Směnný kurz USD/CZK	Hodnota BTC v Kč
13.3.2019	5 let	3 926,60	22,52	88 427,03
13.3.2021	3 roky	61 683,86	21.91	1 351 493,37
13.3.2024	-	65 155,10	23,43	1 479 723,99

Zdroj: vlastní zpracování

Tabulka 13 vykazuje výsledky mezi jednotlivými zvolenými strategiemi, a to především ve výsledné hodnotě investičního portfolia vůči počáteční/celkové investici.

**Tabulka 13 Výsledky dlouhodobých investičních strategií během tří let.**

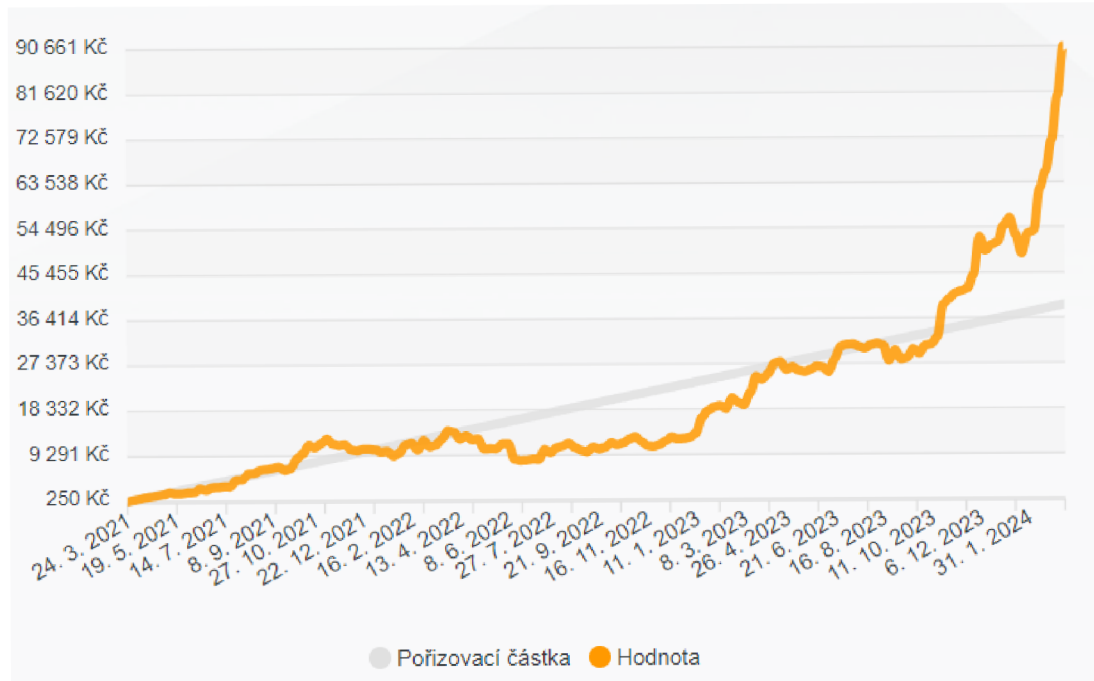
Investiční strategie a metoda	Počáteční hodnota investice v Kč	Časový interval investování	Výsledné absolutní zhodnocení v Kč	Výsledné relativní zhodnocení v %
Dlouhodobá – All-in	39 000	jednorázový	42 700,35	9,49
Dlouhodobá – DCA	250	týdenní	90 661	132,46
Dlouhodobá – DCA	1 054 (v součtu investováno 38 998)	měsíční	90 569	132,46

Zdroj: vlastní zpracování



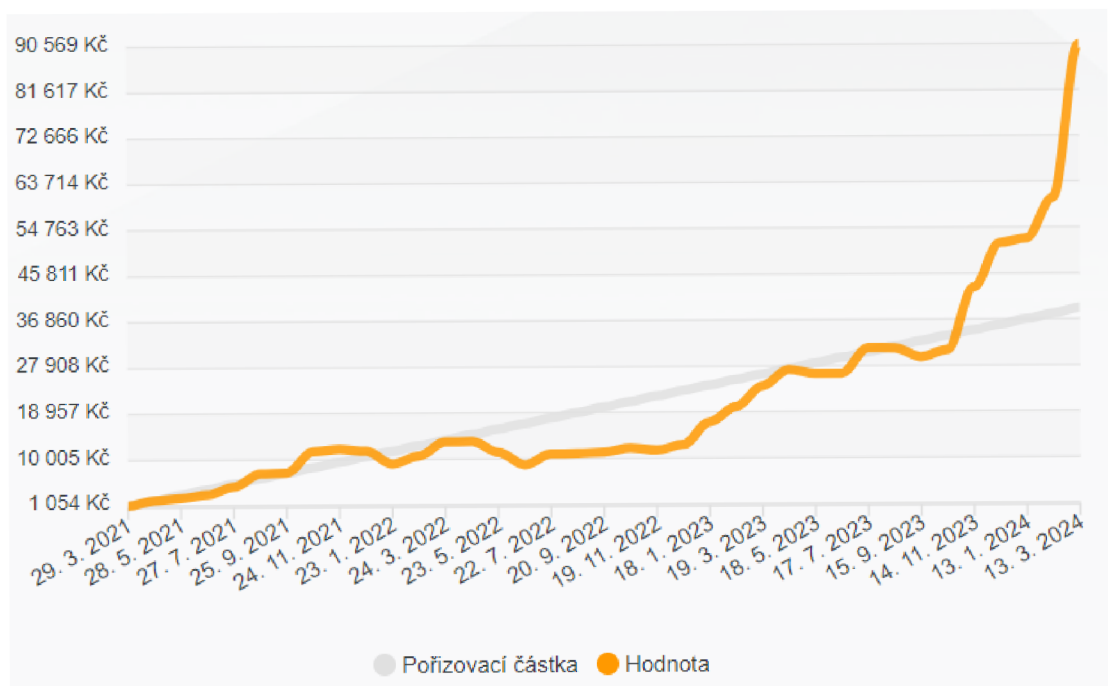
Graf 3 a 4 znázorňuje vývoj hodnoty investiční portfolia s nákladovou křivkou s rozdílem četnosti reinvestování během tří let.

**Graf 3 Dollar Cost Averaging po dobu tří let s týdenní reinvesticí 250 Kč**



Zdroj: vlastní zpracování na platformě Štosuj (13.3.2024)

**Graf 4 Dollar Cost Averaging po dobu tří let s měsíční reinvesticí 1 054 Kč**



Zdroj: vlastní zpracování na platformě Štosuj (13.3.2024)

Tabulka 14 vykazuje výsledky mezi jednotlivými zvolenými strategiemi se změnou v době trvání investice.

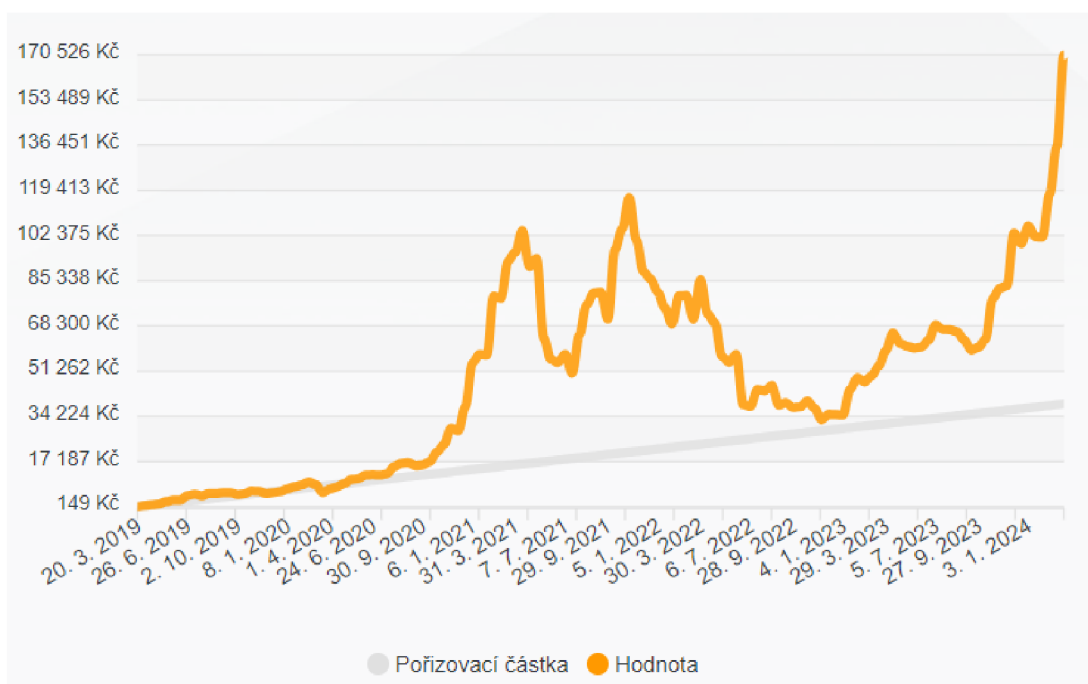
Tabulka 14 Výsledky dlouhodobých investičních strategií během pěti let.

Investiční strategie a metoda	Počáteční hodnota investice v Kč	Časový interval investování	Výsledné absolutní zhodnocení v Kč	Výsledné relativní zhodnocení v %
Dlouhodobá – All-in	39 000	jednorázový	53 720,40	37,74
Dlouhodobá – DCA	149 (v součtu investováno 38 998)	týdenní	170 526	338,49
Dlouhodobá – DCA	639 (v součtu investováno 38 979)	měsíční	165 879	325,56

Zdroj: vlastní zpracování

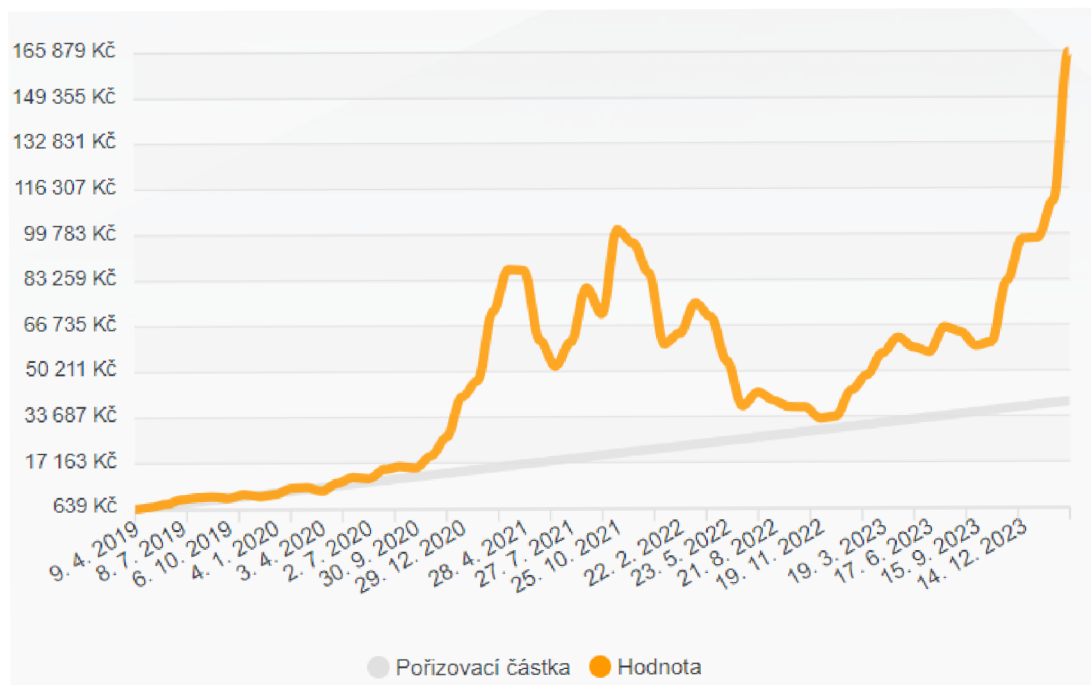
Graf 5 a 6 znázorňuje vývoj hodnoty investiční portfolia s nákladovou křivkou s rozdílem četnosti reinvestování během pěti let.

Graf 5 Dollar Cost Averaging po dobu pěti let s týdenní reinvesticí 149 Kč



Zdroj: vlastní zpracování na platformě Štosuj (13.3.2024)

Graf 6 Dollar Cost Averaging po dobu pěti let s měsíční reinvesticí 639 Kč



Zdroj: vlastní zpracování na platformě Štosuj (13.3.2024)

#### 4.2.4 Zhodnocení dlouhodobých investičních strategií

Tabulka 15 znázorňuje výsledky dlouhodobých investic do bitcoinu. Porovnává výsledné zhodnocení bitcoinového investičního portfolia, které je sestaveno na období tři a pět let se stejnou celkovou investovanou částkou, která vykazuje jen mírnou odchylku v hodnotě 21 Kč.

Tabulka 15 Výsledky dlouhodobých investičních strategií během pěti let

Investiční strategie a metoda	Celková hodnota investice v Kč	Výsledné absolutní zhodnocení v Kč	Výsledné relativní zhodnocení v %
All-in (tři letá)	39 000	42 700,35	9,49
DCA (tři letá s týdenní reinvesticí)	39 000	90 661	132,46
DCA (tři letá s měsíční reinvesticí)	38 979	90 569	132,46
All-in (pět letá)	39 000	53 720,40	37,74
DCA (pět letá s týdenní reinvesticí)	38 998	170 526	338,49
DCA (pět letá s měsíční reinvesticí)	38 979	165 879	325,56

Zdroj: vlastní zpracování

Během období tří let se nejvíce efektivní ukázala investice za pomoci strategie Dollar Cost Averaging, ať už s týdenní nebo měsíční reinvesticí. Celkově bitcoinové investiční portfolio dosáhlo zhodnocení 132,46 % vůči celkově investovaným nákladům. All-in strategie nevyšla tak uspokojivé zhodnocení z důvodu špatného načasování trhu (vysoká cena nákupu, dlouhá korekce a s odrazem během lednu minulého roku).

Investiční strategie projektované na období pěti let vykázaly v každé jednotlivé strategii vyšší míru zhodnocení investovaných nákladů. Nejvíce zhodnocení napomáhala nákupní cena v období 2019 až 2020 a po bull marketu v období 2020 až 2023. Během pěti let se ukázala nejvíce výnosnou strategie Dollar Cost Averaging s týdenním reinvestováním, která přesáhla relativní hodnotu 338 % oproti hodnotě celkové investice.



## 5 Zhodnocení výsledků

Na základě výsledků v kapitole Bitcoin jako prostředek směn se dá říci, že fází vývoje předmětu k penězům se teprve prochází a je na půli cesty. Prostředkem směn je velmi omezeně. Obchodníků, kteří by jej přijímali, je malý počet a celospolečensky uznávaným platidlem také není. Jedná se spíše o kuriozitu a zajímavost, nebo spíše o marketingový tah, který má přilákat nové potenciální zákazníky. Za to, co se Bitcoinu nedá vytknout jsou vlastnosti dobrého uchovatele hodnoty, již dnes splňuje minimálně 6 z 8 vlastností. Historickou prověřenost mu nelze dávat za zlé, protože technologie je ještě mladá a v porovnání s ostatními formami majetku je tu jen krátce. I přes tuto krátkou dobu je trh kryptoměn jedním z největších. A na jeho pomyslném vrcholu stojí právě Bitcoin. Jakmile se státy a jejich vlády postaví k Bitcoinu jako rovnému, beze strachu, může dojít k tomu, že bude přijímaný jako obecně uznávané platidlo, jako tomu je v případě El Salvadoru.

Přestože svou vnitřní povahou byl Bitcoin vytvořen jako digitální měna, tak i s tou lze obchodovat na trhu, pakliže si získá dostatečnou pozornost a zájem investorů. Tak jako se investuje na trhu komodit, akcií, dluhopisů atd., tak se investuje na kryptoměnovém trhu s Bitcoinem, kterému investoři svěřují svoji důvěru v naději, že jim pomůže naplnit jejich osobní investiční cíle, jako například ochrana úspor před inflací.

Ať už jedno nebo druhé, tak Bitcoin má své místo mezi lidmi, kteří mu přisuzují tu, či onu povahu. Právě velký zájem investorů mu pomáhá s informováním o jeho pravé povaze a myšlence, kterou si pro něj Satoshi přál.

## 6 Závěr

Hlavním cílem této bakalářské práce bylo určit, zda Bitcoin spíše vykazuje předpoklady aktiva s investičním růstovým potenciálem nebo efektivního prostředku vhodného pro směnu hodnot.

Prvním dílčím cílem bylo vytvoření návrhu pro uskutečňování směn, uchovávání a manipulaci s Bitcoinem. K dosažení tohoto cíle byla provedena komparace peněženek, směnových nástrojů a obchodních platforem. Bylo zjištěno, že pro vlastnění Bitcoinu je důležité mít vlastní peněženku pro uchovávání, tak aby bylo zajištěno, že bitcoinové mince nezůstanou v držení třetích stran. Pro směnu Bitcoinů v částce nepřesahující 10 000 Kč bylo doporučeno využít mobilní peněženky Unstoppable nebo Coinomi, které jsou navrženy pro rychlé a bezproblémové provádění transakcí a zároveň poskytují uživatelům dostatečné zabezpečení a kontrolu nad jejich prostředky. Pro uskutečnění směny v dané peněžní částce je doporučeno využít služeb Bitcoinových automatů nebo směnáren, které svou jednoduchostí umožňují nejrychlejší možnou směnu za cenu vyšších poplatků. Při větších finančních prostředcích se doporučuje využít hardwarovou peněženku Trezor, která poskytuje nejvyšší úroveň bezpečnosti pro uchovávání většího množství Bitcoinů. Pro směnu Bitcoinu v hodnotě finančních prostředků přesahující 10 000 Kč je doporučeno využívat služeb Bitcoinových burz, které snižují výši poplatků za jednotlivé nákupy. Dále bylo nastíněno praktických aspektů užívání, regulatorních opatření, účetních náležitostí a daňových povinností, které plynou z vlastnění Bitcoinu.

Aby bylo možné vykázat, jestli Bitcoin vykazuje podstatu prostředku směn nebo investičního aktiva bylo třeba popsat fáze vývoje prostředku směn a vlastnosti dobrého uchovatele hodnoty pro Bitcoin, přičemž bylo zjištěno, že Bitcoin se vyskytuje v druhé fázi, jako uchovatel hodnoty s přesahem do prostředku směny, avšak třetí fázi ještě zcela nenaplnuje z omezení plynoucích s obchodováním. Bitcoin se svými vlastnostmi minimálně šest z osmi vlastností dobrého uchovatele hodnoty, konkrétně mu zbývá naplnit historickou prověřenost a odolnost vůči ceně. Zároveň bylo porovnáno, jak si ob stojí se zlatem a fiat měnou, kdy v pěti z osmi hledisek vykazuje také lepší vlastnosti než u zbylých formách majetku.

Dalším dílčím cílem bylo zhodnocení investičních strategií do kryptoměny Bitcoin, které reflektují individuální přístup investora vzhledem k časovému horizontu a očekávaných výnosů. Pro dosažení tohoto cíle bylo zapotřebí nastínit přístup investora, který

očekává v dlouhodobém horizontu výnos z investice plynoucí do kryptoměny Bitcoin. Dále bylo potřeba stanovit vybrané metody dlouhodobé investiční strategie. Krátkodobé investiční strategie se nedoporučují kvůli své vysoké rizikovosti a potřeby velkých obchodních zkušeností. Pro výpočet bylo stanoveno kritérium investiční částky, která v celkovém horizontu nepřesahovala 39 000 Kč. Podle stanoveného kritéria investora, metod dlouhodobé strategie a finančního kritéria bylo zjištěno, že nejefektivnější metodou je DCA s časovým horizontem pěti let a týdenní reinvesticí 149 Kč.

Z veškerých zjištění lze konstatovat, že Bitcoin dosud nenaplňuje všechny charakteristiky peněz, které vyplývají z role dobrého uchovatele hodnoty a vývoje prostředku směny. Jako prostředek směny je jeho použití omezené a jen menší část obchodníků je ochotna tento prostředek akceptovat. Na druhou stranu, jako investiční aktivum s růstovým potenciálem se Bitcoin projevil v dlouhodobém horizontu jako perspektivní investice



## 7 Seznam použitých zdrojů

Coinmap [online], 2024. [cit. 2024-03-11]. Dostupné z: <https://coinmap.org/>

Coinomi: The blockchain wallet trusted by millions [online], 2024. [cit. 2024-03-10]. Dostupné z: <https://www.coinomi.com/en/>

Smpl [online], 2024. [cit. 2024-03-11]. Dostupné z: <https://www.smpl.cz/>

A Beginner's Guide to Cryptocurrency Technical Analysis, 2023. KuCoin [online]. [cit. 2024-03-15]. Dostupné z: <https://www.kucoin.com/learn/trading/beginners-guide-to-crypto-technical-analysis>

Armory, 2024. Best Bitcoin Wallet Armory | Multi-Signature Cold Storage [online]. [cit. 2024-03-06]. Dostupné z: <https://www.bitcoinarmory.com/>

Best Bitcoin Investing Strategy for 2020, 2020. DcaBTC [online]. [cit. 2024-03-13]. Dostupné z: <https://dcabtc.com/bitcoin-investing-strategy>

El Salvador's Experiment with Bitcoin as Legal Tender, 2022. BELSIE, Laurent. National Bureau of Economic Research [online]. [cit. 2024-03-11]. Dostupné z: <https://www.nber.org/digest/202207/el-salvadors-experiment-bitcoin-legal-tender>

TUWIMER, Jordan, 2024. How Many Bitcoins Are There? How Much Supply Left to Mine? Buy Bitcoin Worldwide [online]. [cit. 2024-01-24]. Dostupné z: <https://buybitcoinworldwide.com/how-many-bitcoins-are-there/>

Choose your wallet - Bitcoin, 2024. Bitcoin.org [online]. [cit. 2024-03-06]. Dostupné z: <https://bitcoin.org/en/choose-your-wallet?&step=1>

Jak danit kryptoměny v Česku dle legislativy, 2021. KOHOUT, Martin. FREEBIT [online]. [cit. 2024-03-11]. Dostupné z: <https://freebit.cz/jak-danit-kryptomeny-v-cesku-dle-legislativy/?fbclid=IwAR0bUIeCq3oB3r-xAeW2qkeENad56NIRg5x9mbLsL8VdO0djUW-y4pK5Ulw>

Jak investovat do Bitcoinu, b.r. Jak Na Krypto [online]. [cit. 2024-03-14]. Dostupné z: <https://jaknakrypto.cz/jak-investovat-do-bitcoinu/>

Jak investovat do Bitcoinu, b.r. Jak Na Krypto [online]. [cit. 2024-03-13]. Dostupné z: <https://jaknakrypto.cz/jak-investovat-do-bitcoinu/#startujem>

KRAUSE, Tomáš, 2023. Jednoduše a bez poplatků. Jak (a proč) v obchodě přijímat platby bitcoinem? Finmag [online]. [cit. 2024-03-11]. Dostupné z: <https://www.finmag.cz/inspirace/445167-jednoduse-a-bez-poplatku-jak-a-proc-v-obchode-prijimat-platby-bitcoinem>

DOLEŽAL, Martin, 2024. Kryptoměnové burzy - Recenze a velké srovnání pro rok 2024. Finex.cz [online]. [cit. 2024-03-11]. Dostupné z: <https://finex.cz/rubrika/kryptomeny/burzy/>  
Kryptoměnové peněženky - Jak vybrat tu správnou? Kompletní srovnání pro rok 2024, 2024. DOLEŽAL, Martin a Matouš VONDRÁK. Finex.cz [online]. [cit. 2024-03-10]. Dostupné z: <https://finex.cz/rubrika/kryptomeny/penezenky/>

Regulace Bitcoinu ve světě, b.r. EToro [online]. [cit. 2024-03-11]. Dostupné z: <https://www.etoro.com/cs-cz/crypto/legality-of-bitcoin/>

ČEPEROVÁ, Klára, 2017. Rus koupil v Praze byt za 35 bitcoinů. Jde teprve o druhou nemovitost na světě, za kterou někdo zaplatil virtuální měnou. Hospodářské noviny [online]. [cit. 2024-03-11]. Dostupné z: <https://byznys.hn.cz/c1-65998020-v-praze-se-prodal-byt-jen-za-bitcoiny-jako-teprve-druha-nemovitost-na-svete-rus-za-nej-dal-35-bitcoinu>

Simplecoin, 2024. Simplecoin - Největší směnárna kryptoměn v ČR [online]. [cit. 2024-03-07]. Dostupné z: <https://www.simplecoin.eu/cs>

Some things you need to know – Bitcoin, 2024. Bitcoin.org [online]. [cit. 2024-03-07]. Dostupné z: <https://bitcoin.org/en/you-need-to-know>

Speculative Bitcoin Adoption/Price Theory, 2016. Medium [online]. [cit. 2024-03-12]. Dostupné z: <https://medium.com/@mcasey0827/speculative-bitcoin-adoption-price-theory-2eed48ecf7da>

HÁJEK, Kryštof B., 2022. Strategie DCA aneb průměrování nákladů – jak vlastně funguje? Coinmate.io [online]. [cit. 2024-03-13]. Dostupné z: <https://coinmate.io/cz/strategie-dca-prumerovani-nakladu/>

PAULSON, Alex, b.r. The Reasons Why 90% of Crypto Traders Lose Money [online]. [cit. 2024-03-14]. Dostupné z: <https://www.crypto-rating.com/forecasts/the-reasons-why-90-of-crypto-traders-lose-money/>

TOP 12: Nejlepší krypto burzy 2024 – recenze a srovnán, 2023. GALLA, Andrea. Pfolio [online]. [cit. 2024-03-11]. Dostupné z: <https://pfolio.cz/krypto-burzy/>

RIZ, Jibi, 2023. Understanding Bitcoin's 4 year Cycle. Binance [online]. [cit. 2024-03-13]. Dostupné z: <https://www.binance.com/en/feed/post/522308>

Unstoppable – Bitcoin & Crypto Wallet, 2024. Unstoppable Wallet [online]. [cit. 2024-03-07]. Dostupné z: <https://unstoppable.money/>

V Alze zaplatíte i Bitcoin, 2023. Alza.cz [online]. [cit. 2024-03-11]. Dostupné z: <https://www.alza.cz/platba-bitcoiny-a-btc-automaty-alza>

HÁJEK, Kryštof B., 2022. Ve spolupráci se Štosuj.cz přinášíme DCA. Coinmate.io [online]. [cit. 2024-03-13]. Dostupné z: <https://coinmate.io/cz/ve-spolupraci-se-stosuj-cz-prinasime-dca/>

What Are The Four Types Of Digital Currency And How Do They Differ?, 2024. NTT DATA Payment Services India [online]. [cit. 2024-02-28]. Dostupné z: <https://www.nttdatipay.com/blog/types-of-digital-currency/>

Zkroťte své peníze: jak sestavit osobní nebo rodinný rozpočet, 2022. Fondee [online]. [cit. 2024-03-13]. Dostupné z: <https://www.fondee.cz/blog/zkrotte-sve-penize-jak-sestavit-osobni-nebo-rodinny-rozpocet>

Zlato - aktuální cena zlata, 2024. Kurzy.cz [online]. [cit. 2024-03-12]. Dostupné z: <https://www.kurzy.cz/komodity/zlato-graf-vyvoje-ceny/>

NAMBIAMPURATH, Rahul, 2024. 10 Rules of Investing in Crypto. Investopedia [online]. [cit. 2024-03-14]. Dostupné z: <https://www.investopedia.com/investing-in-crypto-6502543#toc-9-use-crypto-indicators-to-inform-decision-making>

HANUŠ, Daniel, 2023. 4 způsoby, jak koupit Bitcoin a jiné kryptoměny v roce 2024. Pfolio [online]. [cit. 2024-03-09]. Dostupné z: <https://pfolio.cz/jak-koupit-bitcoin/>

ČESKÁ REPUBLIKA, 1993. Zákon České národní rady o České národní bance: § 12 zákona České národní rady č. 6/1993 Sb. In: Sběrka zákonů České republiky (12. 12. 1992 — 31. 12. 1999). 3/1993, číslo 6.

ČESKÁ REPUBLIKA, 2004. Zákon o omezení plateb v hotovosti: a o změně zákona č. 337/1992 Sb., o správě daní a poplatků, ve znění pozdějších předpisů. In: Sběrka zákonů (Česká republika 1. 1. 2000 — 31. 12. 2023). 83/2004, číslo 254.

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

REVENDA, Zbyněk, Martin MANDEL, Jan KODERA, Petr MUSÍLEK a Petr DVOŘÁK, 2012. Peněžní ekonomie a bankovníctví. 5. aktualizované vydání. Praha: Management Press. ISBN 978-80-7261-240-6.

BOUŠKA, Kamil, 2023. Velká kniha o Bitcoinu a kryptoměnách, aneb, Finanční gramotnost pro každého. [Praha]: Braiins Publishing. ISBN 978-80-908709-5-6.

Bitcoinmat recenze: Jak funguje Bitcoin bankomat, poplatky, zkušenosti [online], 2024. In: . [cit. 2024-03-07]. Dostupné z: <https://investplus.cz/kryptomeny/bitcoin-bankomaty/>

NAKAMOTO, Satoshi, 2008. Bitcoin P2P e-cash paper [online]. In: . [cit. 2024-03-01]. Dostupné z: <https://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html>

KUBELKOVÁ, Karina, 2024. Padělky 2023: Padělané a pozměněné bankovky a mince zadržené na území ČR [online]. In: . s. 7-9 [cit. 2024-03-12]. Dostupné z: [https://www.cnb.cz/export/sites/cnb/cs/verejnost/.galleries/pro\\_media/konference\\_projevy/vystoupeni\\_projevy/download/kubelkova\\_20240304\\_padelky\\_2023.pdf](https://www.cnb.cz/export/sites/cnb/cs/verejnost/.galleries/pro_media/konference_projevy/vystoupeni_projevy/download/kubelkova_20240304_padelky_2023.pdf)

HANYECZ, Laszlo, 2010. Pizza for bitcoins? [online]. In: . [cit. 2024-03-02]. Dostupné z: <https://bitcointalk.org/index.php?topic=137.msg1195#msg1195>

Recenze aplikace Vexl: Marketplace pro Peer-to-Peer obchody s Bitcoinem [online], 2024. In: . [cit. 2024-03-07]. Dostupné z: <https://finex.cz/recenze/vexl/>

MANJULA, B.C., B.S. SHILPA a M. SUNDARESH, 2022. Analysis of Cryptocurrency, Bitcoin and the Future. East Asian Journal of Multidisciplinary Research [online]. 2022(1(7), 1293-1302 [cit. 2024-02-29]. Dostupné z: doi:<https://doi.org/10.55927/eajmr.v1i7.803>

NAKAMOTO, Satoshi, 2009. Bitcoin: A Peer-to-Peer Electronic Cash System [online]. 9 [cit. 2024-01-24]. Dostupné z: <https://bitcoin.org/bitcoin.pdf>

DIMITRI, Nicola, 2017. Bitcoin Mining as a Contest. Ledger [online]. 2017(Vol. 2), 31-37 [cit. 2024-03-04]. Dostupné z: doi:<https://doi.org/10.5195/ledger.2017.96>

THAKUR, Krishna Kumar a G. G. BANIK, 2018. Cryptocurrency: Its Risks And Gains And The Way Ahead. IOSR Journal of Economics and Finance [online]. 2018(9), 38-42 [cit. 2024-02-04]. ISSN 2321-5933. Dostupné z: doi:10.9790/5933-0902013842

FRANKENFIELD, Jake, 2024. Digital Currency Types, Characteristics, Pros & Cons, Future Uses. Investopedia [online]. [cit. 2024-02-28]. Dostupné z: <https://www.investopedia.com/terms/d/digital-currency.asp#toc-what-is-a-digital-currency>  
Digitální peníze centrálních bank (CBDC) [online], 2022. 21 [cit. 2024-02-28]. Dostupné z: <https://www.cnb.cz/export/sites/cnb/cs/platebni-styk/.galleries/digitalni-penize-centralnich-bank-cbdc/download/digitalni-penize-centralnich-bank-CBDC.pdf>

CHEN, James, ESTEVEZ, Erik, ed., 2020. Liberty Reserve: What It is, How It Works [online]. New York City [cit. 2024-02-04]. Dostupné z: <https://www.investopedia.com/terms/l/liberty-reserve.asp>

SZABO, Nick, 2002. Shelling Out: The Origins of Money I Satoshi Nakamoto Institute [online]. Satoshi Nakamoto Institute [cit. 2024-01-15]. Dostupné z: <https://nakamotoinstitute.org/shelling-out/>

GEORGE, Kevin, 2023. The Largest Cryptocurrency Hacks So Far [online]. [cit. 2024-02-29]. Dostupné z: <https://www.investopedia.com/news/largest-cryptocurrency-hacks-so-far-year/>

GILEAD, Isaac, 1991. The Upper Paleolithic in the Levant. Journal of World Prehistory [online]. 1991(5), 51 [cit. 2024-01-18]. Dostupné z: doi:10.1007/BF00974677

ABRAR, Waleed, 2014. Untraceable Electronic Cash with DigiCash [online]. Universität Konstanz, 3 [cit. 2024-02-03]. Dostupné z: [https://www.researchgate.net/profile/Waleed-Abrar/publication/277598468\\_Network\\_and\\_communication\\_Privacy\\_Digi\\_cash/links/556e5fc008aeab777226a488/Network-and-communication-Privacy-Digi-cash.pdf](https://www.researchgate.net/profile/Waleed-Abrar/publication/277598468_Network_and_communication_Privacy_Digi_cash/links/556e5fc008aeab777226a488/Network-and-communication-Privacy-Digi-cash.pdf)

GLYN, Davies, 2002. A History of Money: From Ancient Time to the Present Day [online]. Third edition, with revisions. University of Wales Press [cit. 2024-01-15]. ISBN 0-7083-1773-1. Dostupné z: [https://library.uniteddiversity.coop/Money\\_and\\_Economics/A\\_History\\_of\\_Money-From\\_Ancient\\_Times\\_to\\_the\\_Present\\_Day.pdf](https://library.uniteddiversity.coop/Money_and_Economics/A_History_of_Money-From_Ancient_Times_to_the_Present_Day.pdf)

BOYAPATI, Vijay, 2023. Bitcoin je budoucnost [online]. Braiins Systems [cit. 2024-02-21]. ISBN 978-80-908709-2-5. Dostupné z: <https://www.bitperia.cz/>

JAN, Černohorský, 2020. Finance: od teorie k realitě [online]. Grada Publishing [cit. 2024-02-28]. ISBN 9788027118090. Dostupné z: [https://books.google.cz/books?hl=cs&lr=&id=eykPEAAQBAJ&oi=fnd&pg=PA10&dq=funkce+pen%C4%9Bz&ots=7m-sSu9rjq&sig=v0SWrbQEpN\\_CT9rZME8tdwutsD0&redir\\_esc=y#v=onepage&q=funkce%20&f=false](https://books.google.cz/books?hl=cs&lr=&id=eykPEAAQBAJ&oi=fnd&pg=PA10&dq=funkce+pen%C4%9Bz&ots=7m-sSu9rjq&sig=v0SWrbQEpN_CT9rZME8tdwutsD0&redir_esc=y#v=onepage&q=funkce%20&f=false)

ANTONOPOULOS, Andreas M. a David A. HARDING, 2023. Mastering Bitcoin [online]. Third Edition. O'Reilly Media [cit. 2024-02-01]. ISBN 978-1-098-15009-9. Dostupné z: <https://github.com/bitcoinbook/bitcoinbook/blob/develop/BOOK.md>

HANYCH, Michal, Anna DRGOVÁ a Michal GREMLICA, 2018. Zdanění kryptoměn [online]. Brno: Michal Hanych [cit. 2024-03-11]. ISBN 978-80-87934-07-4. Dostupné z: <https://www.zdanenikryptomen.cz/zdanenikryptomen.pdf>

Gigi, 2022. 21 lekcí: Co mě naučil pád do bitcoinové králičí nory [online]. Braiins Systems [cit. 2024-02-22]. ISBN 978-80-908709-0-1. Dostupné z: <https://www.bitperia.cz/>

## 8 Seznam obrázků, tabulek, grafů a zkratk

### 8.1 Seznam obrázků

Obrázek 1 Náhrdelník z wampumu

Obrázek 2 Nejvýznamnější kryptoměny podle tržní kapitalizace a dominance na trhu kryptoměn

Obrázek 3 Bitcoinová dominance na trhu kryptoměn (2014-2024)

Obrázek 4 „nejsem Dorian Nakamoto.“

Obrázek 5 Záznam transakce na Blockchainu

Obrázek 6 Bitcoin Pizza Index

Obrázek 7 „Genesis blok“

Obrázek 8 Síť Bitcoinových automatů v ČR

Obrázek 9 Relativní výše poplatků při zpracování transakce u kryptoměnových automatů, směnárna a burz

Obrázek 10 Role Market maker na burze

Obrázek 11 Obchodníci přijímající kryptoměny v Praze

Obrázek 12 Příklad zdanění prodeje bitcoinu

Obrázek 13 Výše dílčího základu daně při použití metody FIFO a metody váženého aritmetického průměru

Obrázek 14 Bitcoin vs zlato vs fiat

Obrázek 15 Pravidlo 50:30:20

### 8.2 Seznam tabulek

Tabulka 3 Typy digitálních měn a jejich klíčové aspekty

Tabulka 4 Žebříček nejrozsáhlejších útoků na krypto síť a burzy (2011-2023)

Tabulka 3 Rozdíl mezi Bitcoinem a altcoiny

Tabulka 4 Rozdíl mezi Bitcoinem a altcoiny (rychlost transakcí, výše poplatků a jejich celkové zásoby)

Tabulka 5 Výhody a nevýhody Bitcoinu

Tabulka 6 Výše odměny a objem vytěžených BTC (2009-2036)

Tabulka 7 Výhody a nevýhody jednotlivých forem peněženek



Tabulka 8 Doporučení pro držení bitcoinu dle výše hodnoty, způsobu pořízení a formy držení

Tabulka 9 Fáze vývoje Bitcoinu, aktuální stav a odůvodnění

Tabulka 10 Vlastnosti Bitcoinu, jakožto dobrého uchovatele hodnoty

Tabulka 11 Existující odvozené jednotky bitcoinu

Tabulka 12 Údaje o datumu počáteční investice, časovém rozpětí (od první investice až po poslední/zhodnocení), hodnotách ceny BTC, směnného kurzu k danému datu

Tabulka 13 Výsledky dlouhodobých investičních strategií během tří let.

Tabulka 14 Výsledky dlouhodobých investičních strategií během pěti let.

Tabulka 15 Výsledky dlouhodobých investičních strategií během pěti let

### **8.3 Seznam grafů**

Graf 1 Příklad Simple Moving Average při obchodování BTC na burze Bitstamp

Graf 2 Stock-to-Flow model

Graf 3 Dollar Cost Averaging po dobu tří let s týdenní reinvesticí 250 Kč

Graf 4 Dollar Cost Averaging po dobu tří let s měsíční reinvesticí 1 054 Kč

Graf 5 Dollar Cost Averaging po dobu pěti let s týdenní reinvesticí 149 Kč

Graf 6 Dollar Cost Averaging po dobu pěti let s měsíční reinvesticí 639 Kč