Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra ekonomických teorií

Diplomová práce

Investice do kryptoměny Bitcoin

Bc. Matouš Machálek

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Matouš Machálek

Hospodářská politika a správa
Podnikání a administrativa

Název práce

Investice do kryptoměny Bitcoin

Název anglicky

Investment in cryptocurrency Bitcoin

Cíle práce

Primárním cílem diplomové práce je zhodnocení Bitcoinu jako investičního aktiva. Dílčím cílem práce je zjednodušení a vysvětlení kroků potřebných pro investici do této kryptoměny a současně určení fundamentu Bitcoinu, tedy kryptoměny, která kombinuje vlastnosti internetových peněz a digitálního zlata. Dalším dílčím cílem diplomové práce je predikce vývoje ceny a predikce růstu uživatelů této kryptoměny. Posledním dílčím cílem je na základě získaných informací určit postup při investování do Bitcoinu s využitím investičních strategií a investic do těžby Bitcoinu.

Metodika

Diplomová práce bude rozdělena na teoretickou a praktickou část.

Teoretická část práce bude zpracována formou literární rešerše a studie odborné literatury českých a zahraničních autorů a odborných internetových zdrojů. Budou vysvětleny základní problematiky spojené s kryptoměnou Bitcoin – fundament Bitcoinu, historický vývoj Bitcoinu, funkcionalita a proces fungování Bitcoinu, fungování peněz, inflace a jiné. Vysvětleny budou také základní pojmy spojené s Bitcoinem, kryptoměnovou a investiční problematikou, se kterými se lze při běžném používání setkat.

Praktická část diplomové práce bude zaměřena na vytvoření praktické příručky, jak investovat do Bitcoinu. Popsány budou kroky, jak používat Bitcoin v praxi. Dojde k vysvětlení, jak získat a investovat do kryptoměny Bitcoin – nákup a analýza výhod jednotlivých krypto burz, dále P2P portály nebo fyzické bitcoinmaty a následné bezpečné uložení na tzv. „cold storage“, softwarové peněženky nebo tzv. „hot storage“, tedy využití úročení Bitcoinu v „krypto bankách“ a porovnání výhod a případných rizik. V případě pravidelné investice vysvětlení použití metody DCA (= dollar-cost averaging) a možného využití investičních robotů, které automaticky investují dle nastavených parametrů, výstupní strategie a prodej Bitcoinu s následným zdaněním. Popsána bude možnost investice do těžby Bitcoinu – nákup specializovaného ASIC mineru na těžbu Bitcoinu s následným využitím těžebních poolů. Dále se práce zaměří na predikci investičního potenciálu ve spojení

s hodnotou Bitcoinu na základně získaných dat z historického vývoje ceny a predikce vývoje kurzu Bitcoinu vůči americkému dolaru. Práce také bude doplněna o současné aktuality ze světa ohledně využití Bitcoinu. Na Bitcoin bude v této práci nahlíženo jako na dlouhodobou investici a kurz Bitcoinu bude zachycen vůči americkému dolaru. V praktické části budou využity metody jako literární a internetová rešerše, sběr dat, práce s informacemi a jejich třídění, komparativní analýza, predikce, vyhodnocení a interpretace výsledků.

Doporučený rozsah práce

60 – 80

Klíčová slova

Bitcoin, blockchain, decentralizace, deflace, inflace, investice, kryptoměna, peníze, proof-of-work, Satoshi Nakamoto

---

Doporučené zdroje informací

AMMOUS, S. The Bitcoin Standard: The decentralized alternative to central banking. John Wiley & Sons Inc, 2018. ISBN 978-11-194738-6-2.

KALISKÝ, B. *Bitcoin a ti druzí : nepostradatelný průvodce světem kryptoměn.* [Praha]: IFP Publishing, 2018. ISBN 978-80-87383-71-1.

PRITZKER, Y. Vynález jménem Bitcoin. Braiins Systems, 2020. ISBN 978-80-907975-0-5.

SOUKUP, J. – POŠTA, V. – NESET, P. – PAVELKA, T. *Makroekonomie.* Praha: Management Press, 2018. ISBN 978-80-7261-537-7.

STROUKAL, D. Dark web: Sex, drogy a bitcoiny. Grada Publishing, 2020. ISBN 978-80-271-2934-8

STROUKAL, D. – SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti : historie, ekonomie a technologie kryptoměn, stručná příručka pro úplné začátečníky.* Praha: Grada Publishing, 2021. ISBN 978-80-271-1043-8.

TĚTEK, J. Bitcoin: Odluka peněz od státu. Braiins Systems, 2021. ISBN 978-80-907975-8-1.

Předběžný termín obhajoby

2022/23 LS – PEF

Vedoucí práce

Ing. David Křížek, Ph.D.

Garantující pracoviště

Katedra ekonomických teorií

Elektronicky schváleno dne 29. 8. 2022

doc. PhDr. Ing. Lucie Severová, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 2. 11. 2022

doc. Ing. Tomáš Šubrt, Ph.D.

Děkan

V Praze dne 29. 11. 2022

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Investice do kryptoměny Bitcoin" jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 1.4.2023 _____

Poděkování

Rád bych touto cestou poděkoval panu Ing. Davidu Křížkovi, Ph.D. za odborné vedení, cenné rady a v neposlední řadě jeho vstřícnost a čas, který vynaložil na pomoc při tvorbě této diplomové práce.

Investice do kryptoměny Bitcoin

Abstrakt

Předmětem diplomové práce je investice do kryptoměny Bitcoin. Problematika investice do Bitcoinu se stává v posledních letech stále populárnějším tématem a mnoho investorů zařazuje Bitcoin do svého investičního portfolia, které často obsahuje tradiční investice, jako jsou drahé kovy, dluhopisy, akci, nemovitosti a další.

V teoretické části práce jsou vysvětleny všechny teoretické pojmy, jako je základní terminologie Bitcoinu, investiční a ekonomické základy, ve stručnosti je shrnuta historie Bitcoinu, jeho fungování, těžba Bitcoinu, fundament Bitcoinu a jeho vývoj, ekonomické základy Bitcoinu, úloha Bitcoinu jako měny a jeho potencionální rizika, problémy a mýty. Je tak vysvětlen fundament Bitcoinu, který by měl každý investor do Bitcoinu dobře znát.

Praktické část práce je zaměřena na reálná postup investice do Bitcoinu. Je zanalyzována aktuální situace na trhu, následně je vysvětlen postup nákupu Bitcoinu s jeho bezpečným uložením, potenciál investice do těžby Bitcoinu, predikce ceny Bitcoinu a výstup z investice do Bitcoinu v podobě prodeje Bitcoinu a následného zdanění zisků. Data byla jsou doplněna o vhodné obrázky, grafy a tabulky pro lepší vysvětlení problematiky.

Bitcoin je vyhodnocen jako vhodné investiční aktivum, které by mělo mít procentuální zastoupení ve všech investičních portfoliích. V současné době se Bitcoin pohybuje v hodnotách 70 % od svého cenového maxima a jedná se tak o zajímavou investiční příležitost. Pro nákup a prodej bitcoinů byla vybrána burza Coinmate s následným uložením na hardwarovou peněženku Trezor. Nejvhodnější metodou pro investici do Bitcoinu byla zvolena metoda DCA s doplněním o případné nákupy při poklesu ceny BTC.

Klíčová slova: Bitcoin, bitcoin, blockchain, burza, cena bitcoinu, investice, nákup bitcoinu, peněženka, prodej bitcoinu, těžba bitcoinu, transakce

Investment in cryptocurrency Bitcoin

Abstract

The subject of the diploma thesis is an investment in the cryptocurrency Bitcoin. Investing in Bitcoin has become an increasingly popular topic in recent years and many investors are including Bitcoin in their investment portfolio which often includes traditional investments such as precious metals, bonds, stocks, real estate and more.

In the theoretical part of the thesis, all academic terms are explained such as the basic terminology of Bitcoin, investment and economic foundations, the history of Bitcoin, Bitcoin functioning, Bitcoin mining, the foundation of Bitcoin and the development of Bitcoin, the economic foundations of Bitcoin, the role of Bitcoin as a currency and its potential risks, problems and myths. This explains the fundamentals of Bitcoin which every investor in Bitcoin should know well.

The practical part of the thesis is focused on the actual process of investing in Bitcoin. The current situation on the market is analyzed followed by the process of buying Bitcoin with its safe storing, analysing the potential of investing in Bitcoin mining, predicting the price of Bitcoin with the coverage of the exit from investment in Bitcoin in the form of selling Bitcoin and subsequent taxation of profits. The data was supplemented with appropriate images, graphs and tables for a better explanation of the topic.

Bitcoin is evaluated as a suitable investment asset that should have a percentage representation in all investment portfolios. Bitcoin is currently trading at 70 % of its price peak, making it an interesting investment opportunity. The Coinmate exchange was chosen for the purchase and sale of bitcoins, followed by storage on the Trezor hardware wallet. The most suitable method for investing in Bitcoin was chosen the DCA method with the addition of possible purchases when the price of BTC drops.

Keywords: Bitcoin, bitcoin, blockchain, exchange, price of bitcoin, investment, buying bitcoin, wallet, selling bitcoin, mining bitcoin, transaction

Obsah

1 Úvod

Tématem diplomové práce je investice do kryptoměny Bitcoin. Toto téma se stalo v posledních letech velmi aktuálním a diskutovaným tématem. Bitcoin nabízí investici odlišného typu, nežli jsou tradiční investice do zlata, stříbra, druhopisů, obligací, akcií, akciových indexů, nemovitostí a dalších. Současně se však jedná o nejstabilnější investici z kryptoměnového trhu, nežli je investice do různých altcoinů, je jsou Ethereum, Cardano, Solana, Dogecoinu či investice do NFT.

Jak v knize The Bitcoin Standart vyjádřil jeden z největších a nevlivnějších investorů do Bitcoinu Michaal J. Saylor, předseda a bývalý CEO společnosti MicroStrategy: *„Jak se dnes moderní společnost může ochránit své finanční zdroje v prostředí monetární inflace, kde měna ztrácí 15 % kupní síly každý rok? Bitcoin představuje největší současnou příležitost pro ty, kteří si přejí vytvořit něco nového a skvělého, řešení problému uchovatele hodnoty pro 7,8 miliard lidí, více než 100 milionů společností a stovek bilionů kapitálu investorů.“* [1]

Současná situace na finančním trhu nabízí investiční příležitost, vzhledem k aktuální ceně Bitcoinu, která se v roce 2023 pohybuje zhruba 70 % od svého cenového maxima. Před první investicí do kryptoměny Bitcoin by však každý investor měl znát fundament Bitcoinu, jeho podstatu, základní fungování a cenové výkyvy. Vyvaruje se tak případným emočně podloženým ztrátovým prodejům či nákupům pod vlivem FOMO, které obvykle vedou k nevýhodným investicím.

Jednotlivé kroky investice do Bitcoinu se z počátku jako složitější, nicméně při nastudování a pochopení základních kroků je jedná v celku o jednoduchý postup, který muže být dokonce z velké většiny automatizován a vyžaduje tak minimální časovou investici.

Bitcoin tedy nabízí mnoho výhod a příležitostí, které by měl investor dnešní doby minimálně zvážit.

[1] AMMOUS, S. *The Bitcoin Standard.* 2018, Foreworld by Michael J. Saylor

2 Cíl práce a metodika

2.1 Cíl práce

Primárním cílem diplomové práce je zhodnocení Bitcoinu jako investiční aktivum.

Cílem teoretické části práce je identifikace fundamentu Bitcoinu, vysvětlení základní terminologie spojenou s touto problematikou, stručně shrnuta historie Bitcoinu, popsání fungování ekosystému Bitcoinu, jakým způsobem se těží, k jakému vývoji dochází na této kryptoměně, nastínění ekonomických základů Bitcoinu a pojmy s ním spojené, jakým způsobem lze pokládat za měnu a následně jeho potencionální rizika, problémy a mýty spojené.

Cílem praktické části práce je identifikace jednotlivých kroků, které jsou v praxi třeba provést pro investici do Bitcoinu. Je popsána aktuální situace na trhu, počáteční nákup či těžba, následně bezpečné uložení investovaných prostředků, predikce vývoje ceny, odprodej Bitcoinu a následně zdanění zisku.

Dílčím cílem diplomové práce je zjednodušení a vysvětlení kroků potřebných pro investici do této kryptoměny a současně určení fundamentu Bitcoinu, tedy kryptoměny, která kombinuje vlastnosti internetových peněz a digitálního zlata. Dalším dílčím cílem diplomové práce je predikce vývoje ceny a predikce růstu uživatelů této kryptoměny. Posledním dílčím cílem je na základě získaných informací určit postup při investování do Bitcoinu s využitím investičních strategií a investic do těžby Bitcoinu.

2.2 Metodika

Diplomová práce je rozdělena na teoretickou a praktickou část. Teoretická část práce je zpracována formou literární rešerše a studie odborné literatury českých a zahraničních autorů jak se zaměřením na Bitcoinovou a celkovou kryptoměnovou problematikou, tak i obecnou ekonomickou tématikou s doplněním z odborných internetových zdrojů. Jsou vysvětleny základní problematiky spojené s kryptoměnou Bitcoin – fundament Bitcoinu, historický vývoj Bitcoinu, funkcionalita a proces fungování Bitcoinu, fungování Bitcoinu jako měna, základ rakouské školy, inflace a jiné. Vysvětleny jsou také základní pojmy spojené s Bitcoinem, kryptoměnovou a investiční problematikou, se kterými se lze při běžném používání setkat.

Praktická část diplomové práce je zaměřena na vytvoření praktické příručky, jak investovat do Bitcoinu, jenž může využít i nezkušený investor. Na základě osobního testování s doplněním z aktuální internetových zdrojů budou popsány kroky, jak používat Bitcoin v praxi.

Je detailně vysvětleno, jakým způsobem přesně postupovat při investici do kryptoměny Bitcoin. Zpracována je analýza aktuální situace na trhu a současného vývoje ceny Bitcoinu. V nákupním procesu Bitcoinu budou osobně testovány kryptoměnové burzy Binance, Coinbase, Coinmate, kryptoměnová směnárna Anycoin, decentralizovaná burza Bisq a nákup přes bitcoinový ATM. Všechny tyto vybrané nákupní prostředí jsou vzájemně porovnána ve srovnávací analýze nákupního prostředí, ze které je vybrána právě jedno nákupní prostředí pro následné provedení nákupu Bitcoinu s detailním popsání tohoto procesu. Současně je osobně testováno a popsáno prostředí Štosuj.cz, které je využito pro nastavení pravidelných nákupních příkazů, které automaticky investují do Bitcoinu dle nastavených parametrů metodou DCA, která spořívá v pravidelných nákupech bitcoinů s efektem průměrování pořizovací ceny v čase.

Zakoupené bitcoiny budou následně uloženy na tzv. „cold wallet“, tedy hardwarovou peněženku Trezor s detailním popsání jednotlivých kroků, jak nastavení samotného zařízení Trezor, tak i odeslání zakoupených bitcoinů z vybrané burzy na toto zařízení. Popsány je také alternativy softwarových či hardwarových peněženek, které investor může využít.

Práce se zaměřuje i na predikci investičního potenciálu ve spojení s hodnotou Bitcoinu na základně získaných dat z historického vývoje ceny a predikce vývoje kurzu Bitcoinu vůči americkému dolaru. Cena Bitcoinu je predikovaná na základě mnoha predikční nástrojů, jako je meziroční růst ceny Bitcoinu, Fear & Greed indexu, potenciálu dorovnání tržní kapitalizace zlata, cyklického pohybu ceny, Stock-to-flow modelu a jiných predikčních nástrojů společně s vysvětlenou problematikou fundamentální analýzy, technické analýzy a analýzy sentimentu.

Následně je popsán odprodej Bitcoinu společně s kroky vedoucí k odeslání bitcoinů z uložiště Trezoru na vybranou burzu s popsáním jednotlivých kroků prodeje. Současně je popsáno nastavení exitová strategie, kterou by se měl investor v průběhu prodeje Bitcoinu řídit. Na závěr procesu je popsán proces zdanění zisků z prodeje Bitcoinu s výběrem metody pro stanovení kupní ceny a ukázka výpočtů daně.

V práce je popsána i možnost potencionální investice do těžby Bitcoinu. Tento proces je popsán od počáteční srovnávací analýzy pro rozhodovací proces nákupu specializovaného ASIC mineru na těžbu Bitcoinu. Je vypočtena aktuální profitabilita těžby, do které jsou zahrnuty všechny faktory, které profitabilitu ovlivňují, jako je dostupnost a cena vybraného ASIC mineru, úroveň hash rate, úroveň difficulty, cena elektrické energie a další.

Na Bitcoin je v této práci nahlíženo jako na dlouhodobou investici a kurz Bitcoinu je zachycen vůči americkému dolaru. V praktické části jsou využity metody literární a internetová rešerše, sběr dat, práce s informacemi a jejich třídění, komparativní analýza, predikce, vyhodnocení a interpretace výsledků. Práce je doplněna vhodnými obrázky z ukázek jednotlivých prostředí burz, peněženek, těžebních poolů, aplikací společně s grafy a tabulky pro lepší vysvětlení a snadnější pochopení problematiky investice do Bitcoinu.

3 Teoretická východiska

3.1 Základní terminologie Bitcoinu

Nežli práce začne rozebírat kryptoměnu Bitcoin. logo zobrazeno na obrázku 1, do větších podrobností, je nutné vysvětlit základní terminologii, se kterou se bude následně pracovat.

Obrázek 1 Logo Bitcoinu

Zdroj: 1000 Logos. *Bitcoin logo*[online]. Dostupné z: https://1000logos.net/bitcoin-logo/

Adresa je pojem jednoznačné identifikace příjemce zaslané platby. Ekvivalentem v klasickém bankovním systému by bylo číslo bankovního účtu. Je znázorněna dlouhým číslem zakódovaným do řetězce alfanumerických znaků s následujícími vlastnostmi:

- délka v rozmezí 27-34 znaků (v případě nového formátu Bech32 dle BIP 174 je délka 14-74 znaků)
- rozlišuje velká a malá písmena (neplatí pro Bech32)
- začíná číslicí „1“, „3“ označující verzi
- neobsahuje znaky typograficky zaměnitelné např. „0 x O“ nebo „1 x l“
- poslední znaky obsahují kontrolní součet, což je zabezpečení proti špatnému vykopírování či opsání
- příklad:
    - 1KT8NVCG6GKNhYT7f6Ef4Rdpvu54KDh

- bc1h6rkkgajdknvr7hdjwrth98ghtzukldb5356ul

Adresu je možné vygenerovat off-line, vzhledem k tomu, že se jedná o hash veřejného klíče. Generování adres není nijak drahou či náročnou záležitostí, proto je možné vygenerovat novou adresu pro každou nesouvisející transakci, což zabraňuje jejich stopování. Adresy jsou spravovány bitcoinovými peněženkami. Uživatel prokazuje vlastnictví konkrétní adresy tím, že podepíše zprávu svým soukromým klíčem, který mu přísluší k adrese.[2]

Altcoin je zkrácený výraz pro alternativní měnu, tedy všechny kryptoměny kromě Bitcoinu, a to jak ty od něj odštěpené, jako Bitcoin Cash a Bitcoin Gold, tak i samostatně vzniklé, jako je druhá největší kryptoměna Ethereum, dále například Cardano, Dogecoin, Litecoin, Ripple a jiné.[3] V dnešní době existuje tisíce altcoinů.[4]

Asymetrická kryptografie neboli „Public Key Cryptography" je souhrn kryptografických metod, u kterých šifrovací a dešifrovací klíč je odlišný.[5] Využívá se k utajení posílaného obsahu. Jedná se v podstatě o řetězy písmen, čísel a znaků, které za pomocí šifrovacího algoritmu zašifrují obsah.[6] Adresátovi šifrované zprávy je možné pomocí asymetrie klíčů nasdílet odesílatelem tajný dešifrovací klíč, tedy soukromý klíč, a druhý, veřejný klíč, zveřejnit. Jednou z aplikací asymetrické kryptografie je digitální neboli elektronický podpis. Při procesu podpisu zprávy se podpis spočítá za pomocí soukromého klíče. Tento akt může učinit pouze jeho vlastník. Ověřit podepsání zprávy může naopak za pomocí veřejného klíče úplně každý. Podpis i šifrování lze kombinovat. Protokol Bitcoinu využívá algoritmus digitálního podpisu ECDSA.[7]

ATH zkráceně „all time high", přeloženo jako nové cenové maximum. Jedná se o bod, kdy hodnota bitcoinu je ke vztahu k jiné měně nejvyšší za svoji existenci, tedy mohu dostat za jeden bitcoin nejvíce amerických dolarů, popřípadě jiné měny.[8]

---

[2] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 42
[3] Atcmarket. *Altcoiny* [online]. Dostupné z: https://www.atcmarket.cz/articles/26318
[4] Coin Market Cap. *Cryptocurrencies* [online]. Dostupné z: https://coinmarketcap.com/
[5] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 122
[6] KALINSKÝ, B. *Bitcoin a ti druzí.* 2018, s. 8
[7] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 122
[8] KALINSKÝ, B. *Bitcoin a ti druzí.* 2018, s. 26

Bitcoin je decentralizovaná kryptoměna založena na peer-to-peer transakcích.[9] **Bitcoin**, psán s velkým B, se označuje technologie či protokol. Naopak **bitcoin**, psáno s malým b, je označení pro peněžní jednotku.[10]

Časové razítko nebo také známé jako „time stamp" se v bitcoinové síti přidělují k transakcím a mají funkci evidence, kdy byla transakce provedena. Současně pomáhá zamezit nekalé manipulaci s blockchainem.[11]

Fiat je termín pro státní peníze, které vznikají z příkazu. Nejčastější je označení pro papírové peníze, které nejsou kryty drahými kovy. [12]

FOMO je zkrácená verze pro „Fear Of Missing Out", tedy strach vznikající z myšlenky, že byla zmeškána výnosná investiční příležitost a vede často k impulzivnímu chování například při růstu ceny bitcoinu. Při této situaci nezkušení či nedostatečně informovaní investoři podléhají dojmu, že jim uniká jedinečná příležitost zhodnotit své finance a rychle tak zbohatnout. To vše následně obvykle vede k impulzivním investicím při vysokých cenách a následným finančním ztrátám.[13]

Fork je situace, kdy dva či více bloků jsou zapojeny za stejných předchozí blok. Dochází k němu, pokud v době mezi vytěžením bloku a jeho zapsání do sítě došlo k vytěžení jiného bloku. Fork může být také následkem změny bitcoinového protokolu – softfork, hardfork. Pojmem fork můžeme nazvat i odvětví softwaru vytvořeného za účelem nezávislého vývoje, jedná se však o jiný význam nežli fork blockchainu.[14]

FUD je zkratka pro „fear, uncertainty, doubt", přeloženo jako strach, nejistota a pochybnosti. Jedná se o situaci, kdy v médiích, sociálních sítích či prostřednictvím jiných

[9] Coin Market Cap. *Bitcoin* [online]. Dostupné z: https://coinmarketcap.com/currencies/bitcoin/
[10] TĚTEK, J. *Bitcoin: Odluka peněz od státu.* 2021, s. 7
[11] PRITZKER, Y. *Vynález jménem Bitcoin.* 2019, s. 107
[12] TĚTEK, J. *Bitcoin: Odluka peněz od státu.* 2021, s. 8
[13] KALINSKÝ, B. *Bitcoin a ti druzí.* 2018, s. 23
[14] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 132

forem zveřejněna informace, často i neověřená, o negativním ovlivnění Bitcoinu či finančního trhu a obvykle dochází k propadu ceny bitcoinu.[15]

Hardfork je označení změny bitcoinového protokolu, pro kterou platí, že bloky a transakce vytvořeného dle nového pravidla či pravidel nejsou obecně validní podle pravidel starých. Tato změna již na rozdíl od softforku není zpětně kompatibilní. Důvodem je, že stará verze softwaru pokládá nová data obecně za nevalidní. V tomto případě je tedy třeba provést aktualizaci, aby bylo možné síť nadále využívat. Hardfork pravidla uvolňuje, a tedy množinu validních dat zvětšuje. [16]

HODL je terminologie používána v Bitcoinové komunitě, která vznikla překlepem z anglického slova „hold“, tedy držet a ve spojení s Bitcoinem se používá jako jednoslovné vyjádření pro dlouhodobé držení bitcoinů navzdory volatilitě ceny.[17] Hodler je poté slangově osoba, která drží bitcoiny dlouhodobě.[18]

Kryptografie je matematická disciplína zaměřující se na šifrování, tedy převodem zprávy do a z, která je bez znalosti šifrovacího klíče nečitelná. V případě, že klíč k dešifrování není identický jako klíč k zašifrování zprávy jedná se o kryptografii asymetrickou. Bitcoin využívá kryptografii k zajištění bezpečnosti fungování, zejména hashovací funkce a digitální podpis.[19]

KYC je zkratka pro „Know Your Customer“ neboli „Poznej svého zákazníka“. Jedná se o kontroly požadující po poskytovatelích finančních služeb, například na kryptoměnových burzách, identifikování a ověření zákazníků. KYC přispívá v boji proti praní špinavých peněz či proti financování terorismu a nelegálních činností. KYC shromažďuje informace o zákazníkovi a následně je ověřuje. Zlepšuje se tak důvěryhodnost kryptoměnového světa a

[15] KALINSKÝ, B. *Bitcoin a ti druzí.* 2018, s. 23
[16] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 135
[17] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 67
[18] TĚTEK, J. *Bitcoin: Odluka peněz od státu.* 2021, s. 7
[19] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 28

pomáhá burzám řídit rizika. Negativním názor na KYC tvrdí, že KYC ubírá na anonymitě a decentralizaci kryptoměn.[20]

Merklům strom neboli binární hashovací strom je druhem datové struktury, která se využívá v kryptografii. Užívá se k efektivnímu zakódování dat v řetězci důkazů o vykonané práci. Je díky němu možno ověřit konkrétní transakce z jednotlivých bloků bez potřeby načtení celého řetězce.[21]

NFT je zkratkou Non-Fungible Tokenu neboli nezaměnitelného tokenu a označuje transparentní doklad o vlastnictví digitální položky a umožňuje jasné určení majitele. NTF se vztahují vždy jen ke konkrétní unikátní položce a nesou informace o vlastnictví, které je zapsané na blockchainu. Položkou může být například obrázek, video, skladba, herní předmět či jiný virtuální objekt. [22]

Orphan blok, volně přeloženo jako osiřelý blok, označujeme bloky forku, které nebudou použity pro další návaznost blockchainu.[23]

P2P neboli „peer-to-peer" je terminologie používána pro označení počítačových sítí, kde všechny uzly jsou si navzájem rovnocenné a uživatelé společně přímo komunikují bez potřeby centrálního uzlu/serveru. Výhodou modelu P2P je, že s rostoucím počtem uživatelů roste i přenosová kapacita sítě. Naopak nevýhodou je obtížnost při počátečním navázání komunikace. Touto formou je postavena bitcoinová síť.[24]

Peněženka nebo také wallet, je software sloužící ke správě soukromých klíčů příslušejících k bitcoinovým adresám jednotlivých uživatelů. Peněženka slouží ke správně aktiv, tedy zobrazení zůstatku na adrese, zadání pokynů transakce ve formě odeslání platby, vedení historie transakcí či evidenci již známých adres. Peněženka může mít verzi

---

[20] Binance Academy. *Co je postup KYC (poznej svého klienta)?* [online]. Dostupné z: https://academy.binance.com/cs/articles/what-is-kyc-know-your-customer
[21] NAKAMOTO, S. *Bitcoin Whitepaper: A Peer-to-Peer Electronic Cash System.* 2008, s. 13
[22] e15. *NFT přehledně: Kde koupit a jak vytvořit token, jenž hýbe kryptosvětem* [online]. Dostupné z: https://www.e15.cz/kryptomeny/nft-prehledne-kde-koupit-a-jak-vytvorit-token-jenz-hybe-kryptosvetem-1383564
[23] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 132
[24] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 28

softwarovou ve formě aplikace na mobilní telefonu, online podobu a jiné. Verze hardwarové peněženky je ve formě separátního hardwarového zařízení určenou pouze pro tyto účely.[25]

Pool je místo k distribuované těžbě BTC, které funguje jako pojištění zisku za vložený výpočetní výkon. Správce poolu má za úkol zorganizovat zúčastněným uzlům práci. To v praxi znamená, že správce rozděluje uzlům data k hashování a sleduje jejich hashovací rychlost. Celkovou hashovací rychlost poolu získáme součtem hashovací rychlosti všech zapojených uzlů. S vyšší rychlostí roste pravděpodobnost vytěžení bloku. Správce poolu následně rozděluje odměnu za vytěžený blok zúčastněným blokům dle jejich poskytnutého výpočetního výkonu, kterým do poolu přispěly. Je nemožné, aby si odměnu nechal pouze uzel, který blok nalezl.[26]

Poplatek za transakci je rozdílem mezi vstupní a výstupní hodnotou transakce.[27] Poplatky mají funkci ochrany sítě před spamovým útokem a současně slouží jako odměna těžařům, za potvrzování transakcí a jejich poskytnutý výpočetní výkon.[28]

Potvrzení transakce neboli „confirmation" je stav transakce, při kterém se transakce považuje za potvrzenou a dojde k jejímu zápisu do blockchainu. Transakce je pokládá za bezpečnější, čím více je „pohřbena" neboli obsažena hlouběji v blockchainu. Hloubkou je myšlen počet bloků mezi blokem, který zahrnuje transakci ve svých datech. S počtem potvrzení se hrozba zvratitelnosti transakce exponenciálně snižuje, a proto je i nízký počet dostačující pro pokládání transakce za nezvrátitelnou. U transakcí s větším objemem se v praxi vyžaduje alespoň 6 a více potvrzeních.[29]

QR kód je zkrácenina pro „Quick Response Code", a tedy dvou dimenzionální čárový kód, obvykle ve tvaru čtverce, pro optické strojové zpracování. QR kód je tvořen z černých čtverečků v matici o velikosti 21x21-177x177 polí s bílým pozadím. Výhodou je, že kód obsahuje čtyř úrovňové zabezpečení Reed-Solomon, díky kterému je odolný proti chybám,

[25] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 47
[26] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 45
[27] NAKAMOTO, S. *Bitcoin Whitepaper: A Peer-to-Peer Electronic Cash System.* 2008, s. 5
[28] Binance Academy. *Co jsou blockchainové transakční poplatky?* [online]. Dostupné z: https://academy.binance.com/cs/articles/what-are-blockchain-transaction-fees
[29] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 91

jako by mohlo být znečištění plochy, ustřižený roh a jiné. Je využívám pro transakce v bitcoinové síti.[30]

Satoshi nebo také zkráceně **sats**, je nejmenší jednotka bitcoinu. Jeden bitcoin je roven 100.000.000 satoshi neboli jeden satoshi je 0,00000001 bitcoinu.[31]

Seed je 12 až 24 číselný seznam náhodných anglických slov (např. ill, door, sun atd.) v náhodném pořadí, který při ztrátě peněženky umožní její obnovení. Pro obnovu peněženky je třeba zadat právě těchto 12 až 24 slov ve správném pořadí.[32]

Segwit je zkráceně „segregated witness" neboli oddělený svědek, což znamená vnitřní reorganizaci dat bloku způsobem, že dojde k oddělení podpisu transakcí od samotných transakcí. Lehčí uzly sítě mohou vypouštět ověřené podpisy již starších transakcí a ušetřit tak tímto místo v bloku. Důsledkem oddělením podpisu je také odstranění melaability transakce, které tak zjednodušuje škálování na vrstvách nad Bitcoinem. Vlivem oddělení podpisu je možné transakce podepisovat antichronologicky, což tedy umožňuje rozšíření prostoru pro schémata výměny částečně podepsaných transakcí.[33]

Softfork je pojem označující změnu bitcoinového protokolu, pro kterou platí, že bloky a transakce vytvořené podle nového pravidla či pravidel jsou vždy validní i dle pravidel starých. Takováto změna je zpětně kompatibilní vzhledem k tomu, že stará verze softwaru přijímá noví data stále jako validní. Uživatel sítě tedy nemusí provádět aktualizaci softwaru, pokud nemá zájem o využívání nových funkcionalit, které přinášení nová pravidla. Softfork tedy pravidla sítě zpřísňuje, množinu validních dat tím zvětšuje a některým rezervovaným hodnotím v protokolu dává nový význam. Významné softforky jsou například P2SH neboli „pay to script hash" či segwit.[34]

[30] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 81
[31] AMMOUS, S. *The Bitcoin Standard.* 2018, s. 174-175
[32] KALINSKÝ, B. *Bitcoin a ti druzí.* 2018, s. 32
[33] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 139
[34] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 134

Soukromý klíč neboli „Private Key“ je jedním z páru klíčů pro asymetrickou kryptografii. Privátní klíč musí zůstat tajným a jeho majitel ho používá pro dešifrování jemu určených zpráv či podepsání jím ověřené zprávy. V bitcoinové síti se používá digitální podpis, v šifrování však nikoliv. Za pomocí soukromého klíče se podepisují zprávy s informací, kdo bude novým majitelem zaslaných bitcoinů. Každá bitcoinová adresa má jeden soukromý klíč, jenž je uložen v bitcoinové peněžence. V případě využití techniky „HD Wallets“ může jeden soukromý klíč příslušet více adresám.[35]

Split je důsledkem hardforku, který vede k rozdělení blockchainu trvalým forkem, Příkladem známého hardforku bylo rozdělení blockchainu na Bitcoin a Bitcoin Cash.[36]

Těžba, v anglickém jazyce mining, je proces, ve kterém se zapotřebí strojového výpočtu hledá další blok pro napojení do blockchainu, za který je následně vyplácena odměna. Problematice těžby se tato práce následně zabývá podrobněji. [37]

Transakce je označována informace o převodu části, celého či více bitcoinů z určité dresy na jinou adresu. Transakce je datová struktura, která obsahuje množinu vstupů a množinu výstupů, kde vstup referencuje výstup v již existující transakci. Výstupy uvolňují odeslané bitcoiny, Celkový objem transakce je možné mezi výstupy nové transakce rozdělit libovolně za předpokladu, že součet výstupů není větší nežli vstup. Pokud je výstup menší nežli vstup, rozdíl je označován jako poplatek za transakci. Pro uvolnění výstupu je nutné podepsat data transakce soukromým klíčem patřící k jeho adrese.[38] U transakce platí obecná podmínka, že součet hodnot vstupů, výstupů a poplatku za transakci musí být nulový.[39]

[35] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 98
[36] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 135
[37] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 90
[38] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 49
[39] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 95

Uzel v bitcoinové sítě představuje každý počítač nebo zařízení, které je připojené k síti. V síti si vyměňuje data s okolními uzly a uchovává kopii řetězce, potvrzuje transakce, nové bloky a současně je skrze něj možné odeslat transakci k ostatním uzlům v síti. Vzhledem k tomu, že bitcoinové síť funguje na principu peer-to-peer, jsou si všechny uzly rovny.[40]

Veřejný klíč neboli „Public Key" je druhým z páru klíčů pro asymetrickou kryptografii. Kdokoliv ho může používat k zašifrování zprávy určenou majiteli soukromého klíče nebo k ověření jeho podpisu. Veřejný klíč má v bitcoinové síti význam adresy příjemce platby. Adresa se vypočítává z veřejného klíče.[41]

Ostatní terminologie je vysvětlena ve zbylé části práce, kde je zasazena do kontextu.

[40] NAKAMOTO, S. *Bitcoin Whitepaper: A Peer-to-Peer Electronic Cash System.* 2008, s. 12
[41] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 100

3.2 Investiční a ekonomické základy

Vzhledem k tomu, že je práce zaměřena na investiční problematiku, je nutné vysvětlení základních investičních a ekonomických pojmů, se kterými je možné se setkat v obecné problematice investic či ve specifické problematice investice do Bitcoinu.

Investor je osoba, které investuje své finanční prostředky s očekáváním jejich zhodnocení. Investor spoléhá na finanční nástroje, by jeho investice dosáhla co největší míry návratnosti. Každý investor musí mít plán a strategii k dosažení svých finančních cílů. Základním pravidlem pro investora je, že hledá právě takovou investici, která maximalizuje výnosy a minimalizuje riziko. Jednotlivé kroky investora by tedy měly být podloženy dostatečnou znalostí a studiem dané problematiky.[42]

Spekulant je opakem investora. Investor postupuje na základě strategie podložené studiem a znalostí problematiky, spekulant se řídí zejména na bázi emočního rozhodování. Nejlépe je rozdíl mezi těmito dvěma pojmy popsán jako: *„Investiční operace je taková, která po důkladné analýze slibuje bezpečné zachování jistiny a odpovídající výnos. Operace, které nesplňují tyto požadavky, jsou spekulace.“*[43]

Trader a investor se liší zejména periodou, tedy dobou, jak dlouho drží své investiční aktivum. V tradingu se obecně využívá krátkodobé držení zakoupených aktiv, ať už se jedná o měsíce, týdny, dny, či dokonce hodiny. Trader drží zakoupené aktivum pouze po krátkou dobu a s růstem ceny aktivum se ziskem prodává. Investor nakupuje aktiva pro držení po dobu několika let. Krátkodobá fluktuace trhu je v dlouhodobé investiční horizontu nevýznamná.[44]

---

[42] LYNX. [online]. Dostupné z: https://www.lynxbroker.cz/investovani/burzovni-trhy/burzovni-informace/obchodovani-burza/investicni-pojmy/
[43] GRAHAM, B. *Inteligentní investor*. 2007, s. 35
[44] LYNX. [online]. Dostupné z: https://www.lynxbroker.cz/investovani/burzovni-trhy/burzovni-informace/obchodovani-burza/investicni-pojmy/

Portfolio označuje jakoukoliv kombinaci zakoupených aktiv. Obvykle bývá navrženo dle tolerance rizika investora, časového rámce investice a investičních cílů. Správné portfolio by mělo být dostatečně diverzifikované.[45]

Každé investiční portfolio obsahuje spekulativní faktor, který investor musí rozpoznat a držet tuto složku v minimálním mezích, být tak finančně a psychicky připraven na nepříznivý vývoj, který může mít krátkodobé, ale i dlouhodobé trvání.[46]

Existuje inteligentní investice, tak i inteligentní spekulace. Je však třeba se vyvarovat situacím, kdy investice či spekulace je čistě neinteligentní a její charakteristiky jsou:

- investor spekuluje, ale domnívá se, že investuje;
- investice není podložena patřičnými znalostmi a dovednostmi;
- investicí je podstoupen risk ztráty finanční prostředků, více, nežli je možno si dovolit.[47]

Diverzifikace je rozložení investovaných prostředků do různých typů aktiv. Cílem diverzifikace je snížení celkového rizika portfolia s dlouhodobě stabilnějšími výsledky. V případě poklesu ceny jednoho aktiva v portfoliu bude mít u diverzifikovaného portfolia menší vliv na jeho celkovou hodnotu nežli u portfolia s malou či žádnou diverzifikací.[48]

Riziko představuje nedosažení očekávaného výsledku či výnosu, tedy nejistoty zisku z investice. Investice s vyšší mírou rizika mají také obvykle vyšší zisky. Riziko lze předcházet vhodným řízením a sestavením portfolia společně s nastavením dlouhodobého investičního horizontu. Fundamentální analýza investičního aktiva značně snižuje vzniklé riziko investice, vzhledem k tomu, že investor si bude vědou většiny vlastností investičního aktiva i jeho možný cenový výnos a eliminuje tak emoční reakce na změnu ceny.[49]

---

[45] LYNX. [online]. Dostupné z: https://www.lynxbroker.cz/investovani/burzovni-trhy/burzovni-informace/obchodovani-burza/investicni-pojmy/
[46] GRAHAM, B. *Inteligentní investor*. 2007, s. 36-37
[47] GRAHAM, B. *Inteligentní investor*. 2007, s. 36-37
[48] Portu. [online]. Dostupné z: https://www.portu.cz/blog/11-pojmu-ktere-by-mel-znat-kazdy-zacinajici-investor/
[49] Portu. [online]. Dostupné z: https://www.portu.cz/blog/11-pojmu-ktere-by-mel-znat-kazdy-zacinajici-investor/

Finanční aktiva, jak jsou označovány různé druhy finančních produktů, které přinášení pravidelný příjem či zisk. V procesu investice jsou finanční aktiva vnímána jako jeden z investičních nástrojů, které investor drží za účelem dosažení zisku.

Likvidita označuje, jak snadno a rychle lze převést investiční aktivum na hotovost, tedy jak rychlé je možné investici prodat či směnit. Peněžní hotovost je nejlikvidnější aktivem. [50]

Finanční páka označována také jako obchodování s marží je způsob nákupu aktiv za použití dluhu. V případě investice s použitím investiční páky a následného zvýšení hodnoty zakoupeného aktiva, vede díky finanční páce k větším ziskům. V opačném případě snížení hodnoty zakoupených aktiv má v případě využití finanční páky za následek větší ztráty. Finanční páka tak jde proti zásadě inteligentního investora a v práci se dále nebude uvažovat.[51]

Návratnosti investice označováno jako „Return on Investment“ (ROI) je měřítko výkonu a efektivnosti investice. Zle použít také pro porovnání jednotlivých investic. ROI měří míru návratnosti konkrétní investice ve vztahu k vynaloženým nákladům na investici. Vypočítává se jako:

- ROI = (současná hodnota investice – náklady na investici) / náklady na investici.

Výsledek je vyjádřen v procentech nebo jako poměr.[52]

[50] LYNX. [online]. Dostupné z: https://www.lynxbroker.cz/investovani/burzovni-trhy/burzovni-informace/obchodovani-burza/investicni-pojmy/
[51] LYNX. [online]. Dostupné z: https://www.lynxbroker.cz/investovani/burzovni-trhy/burzovni-informace/obchodovani-burza/investicni-pojmy/
[52] LYNX. [online]. Dostupné z: https://www.lynxbroker.cz/investovani/burzovni-trhy/burzovni-informace/obchodovani-burza/investicni-pojmy/

Rentabilita investice se označuje také jako míra návratnosti či „Rate of Return“ (ROR) určuje čistý zisk nebo ztrátu investice za určité časové období a je vyjádřena jako procento původní investice, určuje se tedy procentuální změna od počátku investice až do konce. Vypočítává se jako:

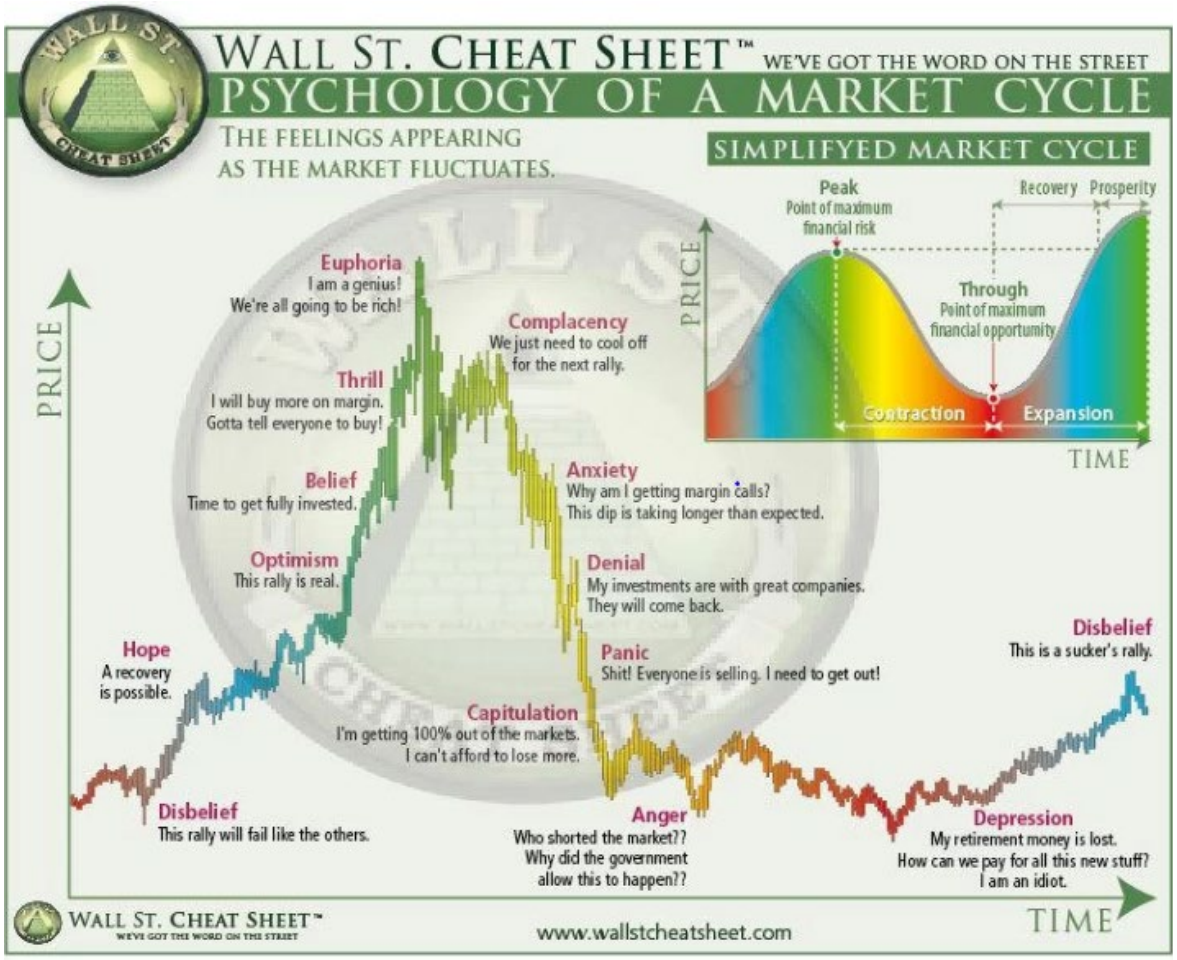
- ROR = ((současná hodnota investice – původní hodnota investice) / původní hodnota investice) x 100.[53]

Býčí trh neboli „bull market“ či „bull run“ není trh v pravém slova smyslu. Jedná se o označení tendence, trendu daného trhu. Býčí trh má obecně stoupající trend s rostoucí cenou trhu. Býčí trh obvykle začíná bodem pesimismu na trhu, tedy přechází se z medvědího trhu k býčímu. Postupuje přes úrovně optimismu až na úrovně euforie.

Medvědí trh neboli „bear market“ či „bear run“ také není trhem, ale trendem daného trhu. Jedná se o pokles trhu a cenový propad. Obvykle trend medvědího trhu začíná z přechodu od býčího trhu, tedy od úrovní euforie či velkého optimismu. Medvědí trh končí, když se aktivum zotaví z cenového propadu a dosáhne nových maxim. Medvědí trh obvykle trvá déle nežli trh býčí.[54] Trend trhu je zachycen v základním grafu 1 využívaný pro odhad vývoje trhu.

[53] LYNX. [online]. Dostupné z: https://www.lynxbroker.cz/investovani/burzovni-trhy/burzovni-informace/obchodovani-burza/investicni-pojmy/
[54] LYNX. [online]. Dostupné z: https://www.lynxbroker.cz/investovani/burzovni-trhy/burzovni-informace/obchodovani-burza/investicni-pojmy/

Graf 1 Wall St. Cheat Sheet



Zdroj: Coindesk [online]. Dostupné z: https://www.coindesk.com/markets/2018/12/11/panic-mode-what-a-wall-street-chart-tells-us-about-bitcoins-price/

Úroková míra či úroková sazba je označení částky, která je účtována za použití aktiv vyjádřena v procentech. Jednoduše řečeno se jedná o částku, kterou si banka či věřitel účtuje za poskytnutí finančních prostředků. Nejčastěji se udává v procentech za rok, tedy p.a.[55]

Inflace je s Bitcoinovou terminologií často spojována, současně tak i pojem deflace. Inflace je definována jako: „projev ekonomické nerovnováhy, jejíž vnějším znakem je růst cenové hladiny," obecně vyjadřuje růst spotřebitelských cen a je jedním z makroekonomických ukazatelů vypovídající o stavu ekonomiky státu. Projevuje se na zdražování statků a služeb a současně vyvolává znehodnocení peněz.[56]

[55] LYNX. [online]. Dostupné z: https://www.lynxbroker.cz/investovani/burzovni-trhy/burzovni-informace/obchodovani-burza/investicni-pojmy/
[56] BRČÁK, J.; SEKERKA, B.; STARÁ, *D. Makroekonomie – teorie a praxe*. 2014, s. 127

K inflaci dochází v případě rostoucí cenové hladiny a míra inflace je definována jako míra změny cenové hladiny, která je měřena například indexem spotřebitelských cen CPI. Inflace tedy měří trend průměrné cenové hladiny.[57]

Deflace je opakem inflace, které snižuje cenovou hladinu, dochází k ní však spíše sporadicky a bývá doprovázena útlumem ekonomiky. V momentu, kdy dochází ke stagnaci inflace a reálného produktu, je pojem označován jako stagflace, je ovlivněna nezaměstnanost formou růstu. [58]

Vzhledem k tomu, že ekonomika dnešní doby má charakter inflačního prostředí je osoba mající finanční příjmy v podstatě nucena něco se svými penězi nělat, pokud nechce, aby mu peníze „seděly“ na běžném bankovním účtu a ztráceny svou hodnotu v řáduje jednotek až desítek procent každý rok. Se současnou situacá vysoké inflace v České republice, ale i ve světe, je tato problematika aktuální jak jen může být.

V dnšní době existuje mnoho finanční aktiv, které může investor zařadit do svého portfolia. Mezi tradiční investiční aktiva patří dluhopisy, dluhopisové fondy, státní dluhopisy, akcie, akcioné fondy, ostatní fondy, drahé kovy, nemovitosti či kryptoměny, pod které patří i Bitcoin, na která se tato práce zaměří.[59]

Bitcoin je tak relativně novým investičním aktivem, které finančí trh nabízí. Nežli však osoba investuje do Bitcoinu, měla by co Bitcoin představuje, jak funguje a jaké jsou jeho cenové vývoje. Nákupem Bitcoinu by se tak osoba měla stát skutečným investorem do Bitcoinu s patřičnými znalostmi a ne pouze spekulante, který doufá, že Bitcoinu mi přinese rychlé bohaství.

[57] SAMUELSON, P.; NORDHAUS W. *Ekonomie*. 1991, s. 306
[58] BRČÁK, J.; SEKERKA, B.; STARÁ, *D. Makroekonomie – teorie a praxe*. 2014, s. 127

[59] Miras. [online]. Dostupné z: https://www.miras.cz/akcie/moznosti-investovani.php

3.3 Historie Bitcoinu

Rok 2008-2009

Bitcoin byl jako protokol vytvořen koncem roku 2008 a spuštěn v roce 2009 vývojářem či týmem vývojářů pod pseudonymem Satoshi Nakamoto, jeho anonymita zůstala zachována až do dnešní doby. Již v roce 2008 byl uveřejněn základní dokument známý jako **Bitcoin Whitepaper**: A Peer-to-Peer Electronic Cash Systém.[60] Do dnes se spekuluje, že zachování anonymity hlavním vývojářem je pro samotnou kryptoměnu velmi důležité až v podstatě zásadní.[61] Co však víme s určitostí je, že znalost tvůrce je pro samostatné fungování měny absolutně nepotřebná. Tvůrce již nemá nad bitcoinovou sítí žádnou moc.[62] Naopak se ukázalo, jak je důležité zachovat anonymitu autora, vzhledem k tomu, že v podstatě nelze vytvořit konkurenci státním penězům, aniž by autor dříve či později neskončil u soudu, jak tomu bylo u podobných projektů z minulých let.[63]

Bitcoin se získává procesem zvaným těžba. První bitcoiny byly vytěženy dne 3. ledna 2009 v 18:15 a vytěžil je samotný zakladatel Satoshi Nakamoto. První odměna za vytěžený blok byla 50 bitcoinů a blok je do dnes známý jako tzv. **genesis blok** [64] a nese název 000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f.[65]

Rok 2010

V roce 2010 byla provedena první transakce na bitcoinové síti, kterou provedl samotným tvůrce Satoshi Nakamoto, ve 170. bloku. Současně došlo k prvnímu ocenění BTC ve vztahu k americkému dolaru. Náklady na vytěžení jednoho bitcoinu se dle propočtů pohybovaly na hodnotě 0,0008 dolarů, přičemž jeden bitcoin se obchodoval za 0,000003 dolaru.[66]

Satoshi Nakamoto později tohoto roku odprodal své přístupy k uložištím kódům a současně také k doménám Bitcoinu novému vývojáři. S jeho odstoupením od projektu se

[60] KALINSKÝ, B. *Bitcoin a ti druzí.* 2018, s. 14
[61] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 28
[62] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 30
[63] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 33
[64] KALINSKÝ, B. *Bitcoin a ti druzí.* 2018, s. 14
[65] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 41
[66] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 43

Bitcoin mohl vyvíjet svobodně a jako decentralizovaný systém, v kterém nezávisí na jeho samotném názoru, ale na názoru komunity. Po svém odchodu do ústraní Satoshi Nakamoto nepřesunul statisíce bitcoinů na prvotních bitcoinových protokolech a tyto bitcoiny již s velkou pravděpodobností nikdy nezmění svého majitele.[67]

Zájem o Bitcoin vzrostl a došlo ke vzniku prvního Bitcoin Marketu a také první Bitcoinové burzy. Nejvýznamnější událost tohoto roku proběhla dne 22. května 2010, kdy došlo k první bitcoinové transakci. Na bitcoinovém fóru se objevila nabídka na zakoupení 2x velké pizzy, v hodnotě okolo 25 USD, za 10.000 bitcoinů a někdo se rozhodl této nabídky využít.[68] Do dnes je tento den známý jako „Bitcoin pizza day".[69]

Objevila se i první chyba bitcoinové sítě, při které bylo možné vytvořit bitcoiny mimo pravidla těžby a někdo se rozhodl této chyby využít a vytvořil pro sebe 184 miliard bitcoinů. Uživatelé si však rychle vzniklé chyby všimli a během několika hodin za pomocí forku, vlastně úplně prvního softfortu,[70] a bitcoinová síť se navrátila opět do normálu.[71]

Rok 2011

V roce 2011 trží kapitalizace přesáhla hodnotu 1 milionu amerických dolarů a hodnota bitcoinu současně dosáhla parity s americkým dolarem (1 BTC = 1 USD).[72]

Tržní kapitalizace znázorňuje celkovou velikost kryptoměny Bitcoin a její umístění na trhu. Pro výpočet tržní kapitalizace musíme vynásobit počet vydaných mincí v oběhu cenou jedné mince, tedy cena 1 BTC x počet vytěžených bitcoinů.[73] Obvykle je hodnota kryptoměny vyčíslena v americkém dolaru.[74]

Přibývalo množství nabídek na obchody za bitcoiny a možností platby bitcoinem na e-shopech.[75] Po značném nárůstu hodnoty Bitcoinu ve vztahu k USD přišlo období, které je

[67] KALINSKÝ, B. *Bitcoin a ti druzí.* 2018, s. 14-15
[68] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 43
[69] Coindesk. *What is Bitcoin Pizza Day* [online]. Dostupné z: https://www.coindesk.com/learn/what-is-bitcoin-pizza-day/
[70] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 142
[71] KALINSKÝ, B. *Bitcoin a ti druzí.* 2018, s. 15
[72] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 47
[73] Kriptomat. *Co je tržní kapitalizace kryptoměny?* [online]. Dostupné z: https://kriptomat.io/cs/kryptomeny/co-je-trzni-kapitalizace-kryptomeny/
[74] KALINSKÝ, B. *Bitcoin a ti druzí.* 2018, s. 24
[75] KALINSKÝ, B. *Bitcoin a ti druzí.* 2018, s. 16

známo jako „Velká bublina roku 2011“. Za pouhé 4 dny došlo k poklesu ceny 1 BTC ze 31,91 USD na 10 USD, což znamenalo propad o necelých 70 % ceny.[76]

Rok 2012–2013

V roce 2012 se začaly vyskytovat první možnosti platby bitcoiny, jak na internetových stránkách, tak i platby v restauracích, u lékaře, právníka, za taxi služby, fyzické zboží a v neposlední řadě, se bitcoin začal využívat k hazardním hrám, díky nízké regulovanosti, zdanění a vysoké rychlosti transakcí. O Bitcoinu se začalo opět více mluvit, psát v novinách a vysílat v televizních zprávách, dokonce vznikaly první bitcoinové vyučovací kurzy na vysokých školách.[77]

Ve stejném roce došlo k první krádeži čítající 46.000 bitcoinů z bitcoinové směnárny. Při útocích docházelo zejména ke krádežím soukromých klíčů. V reakci na krádeže soukromých klíčů začat vývoj první hardwarové peněženky Trezor. Současně v tomto roce došlo k úplně prvnímu halvingu neboli snížení odměny za těžbu bloku z 50 bitcoinů na 25 bitcoinů.[78]

Tržní kapitalizace překonala hranici jedné miliardu USD, poté 10 miliard amerických dolarů. V dubnu roku 2013 dosáhla cena 1 BTC na hranici 100 USD a zastavila se až na bodě 266 USD za 1 BTC, což znamenalo nárůst ceny o více než 2000 %. Poté opět přišel pád až na bod 150 USD/1 BTC.[79]

Negativním aspektem byl však růst ilegálního serveru „Silk Road“, na kterém byly nabízeny deset tisíc různých produktů, ze kterých 75 % tvořily drogy. V následujících měsících byl však provozovatel zatčen a server uzavřen, což mělo vliv na pokles ceny Bitcoinu.[80] I díky tomuto spojení je Bitcoin do dnešní doby v myslích některých lidí spojován s drogovými a jinými nelegálními aktivitami, jako je „praní špinavých peněz“. Tato domněnka je ovšem mylná a Bitcoin v tomto případě ukázal, jaké slabiny má pro využití v ilegální činnosti. Díky blockchainu a jeho zaznamenávání transakcí, které jsou veřejně přístupné, se povedlo snadno vysledovat odesílatele či příjemce bitcoinů. Nejčastěji se jedná

[76] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 47-51
[77] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 52-60
[78] KALINSKÝ, B. *Bitcoin a ti druzí.* 2018, s. 16
[79] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 52-60
[80] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 56-60

o případ, kdy příjemce vloží své bitcoiny na burzu, která je však podrobena ověřením KYC. V tento moment se stane uživatel snadno identifikovatelným. [81]

Nadále docházelo ke vzniku podobných nelegálních serverů, které však pokračovaly v zániku, či zrušení. Bitcoin i tak nadále postupoval v nárůstu popularity, které se mu znovu nedostalo až do roku 2017.[82]

Rok 2014–2015

Začátkem roku 2014 se stala doposud jen z největších událostí v historii Bitcoinu. Burza Mt.Cox, která ovládala téměř 75 % všech obchodů s bitcoiny, přestala vyplácet peníze a zbankrotovala. Uživatelé na této burze získávali své bitcoiny, obchodovali s nimi a také je zde prodávali. Burza Mt.Cox však měla problémy již v minulém roce kdy, jíž přestala vyplácet svým uživatelům americké dolary. Následně trvalo týdny a měsíce, než uživatelům přišli své peníze, nakonec burza zastavila veškeré vyplácení a došlo k již zmíněnému krachu, a tedy zastavení působnosti. Burza tvrdila, že šlo o problém spojený s maleabilitou transakce, což se však nikdy nepotvrdilo. Tato skutečnost způsobila pád ceny BTC, pošramotila důvěryhodnost kryptoměnového světa.[83]

Maleabilita transakce je možnost úpravy dosud nepotvrzené transakce tak, že význam jejich dat se nezmění, ale změní se její hash. V momentu, co se do blockchainu dostane namísto původní transakce její upravená verze, může nevhodně navržený software, který potvrzuje transakce na základě jejího hashe a ne na základě obsažených dat transakce, vyhodnotit danou transakci jako neprovedenou. Software se může následně pokusit o znovu provedení transakce uvolněním jiným bitcoinů, kterými disponuje, čímž předmětnou platbu provede vícekrát. Následně poté předpokládá, že výstup použitý v upravené transakci má stále k dispozici. Tento fakt působí problém při pokusech o uvolnění prostředků v jiné transakci. Tato skutečnost způsobila dočasný pokles hodnoty Bitcoinu a jeho důvěryhodnost. Problém byl následně odstraněn.[84]

V tomto roce prohlásit britský úřad pro výběr daní a cel BTC za soukromá aktiva, ze kterých není povinnost platit daň z přidané hodnoty. Evropská unie se současně rozhodla

[81] KALINSKÝ, B. *Bitcoin a ti druzí.* 2018, s. 18
[82] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 56-60
[83] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 62
[84] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 62

vydat dokument, který podporoval myšlenku, aby byly kryptoměnové burzy povinnými osobami, které musí hlásit vyšší objemy přes ně protékající z důvodu zabránění praní špinavých peněz a narušení financování teroristických organizací. Tato skutečnost umožnila bankám pokládat bitcoiny za tradiční finanční aktiva.[85]

V České republice došlo ke dvěma významným událostem. Byla vytvořena první hardwarová peněženka Trezor, která výrazně pomohla ochraně bitcoinů před ztrátou a odcizením. Druhou událostí bylo otevření institutu Paralelní Polis, ve kterém probíhali pravidelné přednášky o Bitcoinu. Byl zde také umístěn bitcoinový automat a kavárna, ve které šlo platit pouze bitcoiny. V neposlední řadě se koncem roku společnost Microsoft rozhodla přijímat bitcoiny jako platbu za své nabízení služby a v průběhu následujícího roku další společnosti pouze přibývaly. Vše tedy ukázalo na to, že propad ceny BTC neznamenal současně propad zájmu o Bitcoin. V roce 2015 Evropský soudní dvůr rozhodl, že na směnu bitcoinu není vztaženo DPH a na bitcoiny se tak současně vztahuje ustanovení o transakcích pomocí oběživa, bankovek a mincí v podobě zákonného platidla.[86]

Na Bitcoin navázané byznysy a velké firmy ukázaly, jak flexibilní mohou být, vzhledem k tomu, že ve státech s nekladně se vyvíjející regulační či daňovou legislativou se firmy začaly přesouvat do států, ve kterých takovéto „nepříjemností“ nebude až tak značně pociťovat. Státy přijímající tyto firmy získaly na oplátku nový příliv investic a daní do státní pokladny. [87]

Rok 2016–2017

Roky 2016 vláda Japonska označila Bitcoin a podobné měny za aktivum podobné penězům a následně ho v roce 2017 plně legalizovala.[88] Bitcoin tak získal možnost využití v jedné z největších ekonomik světa, která současně přilákala nové investice a technologie. Průběžně stoupal podíl japonského jenu na realizovaných obchodech s bitcoiny, až do body, kdy se stal japonský jen nejobchodovanějším měnovým párem, ve vztahu krypto a fiat měnou. Následoval americký dolar a korejský won, ve stejném vztahu.[89]

[85] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 63-66
[86] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 63-66
[87] KALINSKÝ, B. *Bitcoin a ti druzí.* 2018, s. 20
[88] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 67
[89] KALINSKÝ, B. *Bitcoin a ti druzí.* 2018, s. 26

Největší norská online banka začala nabízet klientům bitcoinové účty. Postupoval růst obchodníků přijímajících bitcoiny ke kterým se roku 2017 přidal největší český e-shop Alza.[90]

Ve stejném roce došlo k dalšímu halvingu, kdy se opět snížila odměna těžařům o půlku, tedy z 25 bitcoinů za vytěžený blok na 12,5 bitcoinů.[91]

V roce 2016 na ceně 400 USD za 1 BTC nastal postupný růst, který nabral zběsilého tempo po překonání hranice 1000 USD/BTC a s několika průběžnými korekcemi na ceně se vyšplhal až na úroveň 20.000 USD za bitcoin. Přesto však 20x násobek oproti minulosti nebyl nijak ohromující. Rok 2013 přinesl stonásobek vkladu do bitcoinu a v roce 2011 dokonce 172x.[92]

V průhybu roku nastalo i několik problémů. Tím prvním byla ztráta 120.000 bitcoinů burzy Bitfinex, které v této době byla jednou z největších kryptoměnovým burz. Již to však nebyl takový problém, protože burza se zavázala, že všechny ztracené bitcoinu svým uživatelům nahradí, což také později úspěšně splnila. Současně již na trhu existovalo mnoho jiných alternativních burz, které uživatelé mohli využít pro nákup bitcoinů po ztrátě důvěry v Bitfinex. Daleko závaznějším problémem byl problém s počtem transakcí za jednotku času, který byl v počátku bitcoinové sítě omezen tak, aby síť nebylo možné úmyslně zahltit. Tento problém se již vyskytl v minulosti, ale s rostoucím počtem uživatelů vyšel problém více najevo a síť přestávala stíhat. Komunita byla rozpolcena ohledně řešení tohoto problému, přesto nakonec nalezla řešení. Byla provedena změna, která přinesla mírně vyšší propustnost a současně otevírala prostor pro systémové řešení – segwit. Část komunity, která se směnou nesouhlasila, si založila vlastní kryptoměnu s názvem Bitcoin Cash.[93]

Bitcoin vypomohl v roce 2017 některým obyvatelům Venezuely a Zimbabwe, kdy zemi postihl problém s hyperinflací. Někteří obyvatelé opustili zemi díky spoření na letenky v Bitcoinu, který nebyl jako místní měna masivně znehodnocen.[94] Bitcoin byl schopen uchovat hodnotu a nemohl být manipulovatelný místní vládou, současně pomohl i jeho cenový růst v roce 2017.

---

[90] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 67
[91] KALINSKÝ, B. *Bitcoin a ti druzí.* 2018, s. 22
[92] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 67-68
[93] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 68-69
[94] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 67

Rok 2018–2021

V roce 2018 se pád ceny Bitcoinu z původních 20.000 USD zastavil kolem částky 3.300 USD. Postupem času opět Bitcoin nabírat na finanční síle, o čemž svědčil i růst poměru tržní kapitalizace kryptoměnového trhu z jedná třetiny až na 50 %. Růst však zastavil šok z přicházející pandemie a během pouhých pěti dnů se BTC propadl o polovinu své ceny na konečnou hodnotu 4.400 USD/BTC. V krizi se ukázalo, že k Bitcoinu lidé ihned nepřecházejí, je však nutné zmínit, že stejnou situaci zažilo i zlato. Při ústupu pandemie začal pomalý růst ceny i tržní kapitalizace, kdy jeden bitcoin stál 30 tisíc amerických dolarů a tržní kapitalizace Bitcoinu zaujímala 70 %. V roce 2021 se cena bitcoinu vyšplhala až přes hranici 60 tisíc dolarů. Bitcoinu v tomto období pomohly zejména 3 faktory. Prvním byl fakt, že Bitcoin přežil krizi a nezhroutil se na hodnotu blízké nule. Druhým faktorem byl fakt, jakým způsobem byl připravený celý ekosystém Bitcoinu na masivní přísun nových uživatelů, kteří si chtěli své peníze ochránit před přicházející inflací, poznat „peníze budoucnosti“ nebo jen vyzkoušet své štěstí. Nejzásadnějším byl faktor třetí, a to přísun institucionálních investorů, tedy velké investiční fordy a firmy. Fond Grayscale získal investice do 650.000 bitcoinů, což bylo více než 3 % celkové zásoby. Firmy nenakupovaly bitcoiny jen přes investiční fondy, ale také napřímo. Dalším velmi hlasitým jménem byl investor Michael Saylor se společností MicroStrategy, který nakoupil společnosti 91 tisíc bitcoinů. Největší ohlas však přinesl investice nejbohatšího muže planety Elona Muska.[95] [96] Nejprve cena bitcoinu vzrostla o 15 % pouze poté, co si na sociální síti Twitter Musk napsal ke svému jménu popise #bitcoin a přidal k němu logo Bitcoinu. Následně oznámil, že nakoupil do své firmy Tesla bitcoiny v hodnotě 1,5 miliardy amerických dolarů a následovalo rozhodnutí, že firma Tesla bude za své elektrická auta přijímat také bitcoiny, které následně nebude měnit do amerických dolarů. V celku tedy instituce nakoupily do začátku roku 2021 necelých 7 % všech bitcoinů.[97]

[95] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 70-73
[96] Forbes. *Todays's Winners and Losers* [online]. Dostupné z: https://www.forbes.com/real-time-billionaires/#5c0e9a593d78
[97] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 72-73

3.4 Fungování Bitcoinu

„Duoble spend“ problém, také známí jako problém dvojité útraty, je hlavním problémem, který Bitcoin musel překovat.[98]

Dvojitá útrata je typ útoku na bitcoinovou síť, při které je snaha použití stejné Bitcoiny vícekrát. Přesněji tedy využít stejný výstup již existující transakce na více nežli jednom vstupu. Útok je snadné realizovat, pokud příjemce platby nevyžaduje potvrzení příslušné transakce. V tomto případě stačí každému příjemci rozeslat pouze jemu určenou transakci. Čím vyšším je počet potvrzení ze strany příjemce vyžadováno, nežli je transakce uznána, tím těžší je útok uskutečnit. Útočník je v případě tohoto útoku nucen vytěžit alternativní bloky, kterým obětuje svůj výpočetní výkon k útoku, jehož nejistota pro úspěch roste s počtem potvrzeních, které musí svou alternativní větví blockchainu obejít. Tento problém je odstraněný vytvořením blockchainu.[99]

Blockchain funguje v podstatě jako účetní kniha bitcoinových transakcí. Blockchain je veřejně přístupný a sdílený se všemi uživateli bitcoinové sítě, kteří potvrzují transakce stejně, jako je tomu u centrální autority, nicméně v decentralizované podobě, tedy za pomocí rozprostření uživatelů po celém světě. Všichni uživatelné si mohou zobrazit provedené transakce a jejich bližší informace za celou historii fungování bitcoinové sítě, ode dne spuštění až do součásti. Potřeba centrální autority je tedy anulována.[100]

Jak však blockchain přesně funguje? Řetěz bloků, jak je do češtiny překládán blockchain, je v podstatě spojový seznam bloků. *„Spojení je dosaženo obsažením hashe předchozích bloku v datech bloku následujícího. Každý blok má tedy jednoznačně určeného předka s výjimkou prvního bloku, tzv. genesis blok, kde místo hashe předka je 0.“* Předek bloku je jeden. Graf vztahů je tedy strom. K větvení však téměř nedochází. V případě, že ano, dochází k tzv. forku. Jedná se tak v podstatě o jednu dlouhou větev bloků, která vytváří lineární řetěz. Vznikají tak relevantní bloky, které zahrnují provedené transakce a ty jsou považovány za potvrzené. Uzavřené bloky jsou tak již nepřepsatelné a navždy uloženy v historii blockchainu z důvodu, že blockchain pracuje vždy a pouze s nejdelší větví.[101]

---

[98] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 31
[99] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 31
[100] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 31
[101] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 32

Pro přepsaní bloku ve vnitřní části řetězu by bylo zapotřebí přepočítat všechny následující bloky, které by se přepsáním změnily, což by znamenalo, že by se při přepásání nepracovalo s nejdelší větví, nicméně blockchain pracuje jen a pouze s nejdelší větví, tedy přepsání již není možné.[102]

„***Blok*** *je nejvýznamnější datová struktura bitcoinového protokolu. Kóduje množinu transakcí, které svým zahrnutím potvrzuje.“* [103] Jedna transakce v bloku se nazývá transakce generující, prostřednictvím které vznikají nové bitcoiny. Blok, který je možný validovat, musí obsahovat určitou kryptografickou vlastnost, která vyžaduje náročný výpočetní výkon pro její splnění. Úroveň náročnosti je proměnná v čase a umožňuje tak regulace k dosažení stability průměrné rychlosti generování nových bloků a tím i inflaci měny. Nalezením validního bloku je výsledkem vynaložení výpočetní síly při procesu zvaný těžba na koncepční bázi „proof-or-work“.[104]

Generující transakce je speciálním typem transakce, která obsahuje pouze výstupy.[105] Tedy kromě běžných transakcí je v bloku obsažena právě jedna generující transakce, skrze kterou vznikají nové bitcoiny. Generující transakce nemá žádné vstupy a jejím objemem je součet nově vygenerovaných bitcoinů a poplatků za ostatní transakce v bloku. Výstupy neboli bitcoiny generující transakce naleží těžaři, který vytěží tento nový blok. Obsažené bitcoiny ve výstupu generující transakce se poté přesouvají na adresu vítězného těžaře. Generující transakce také může být jediná obsažená transakce v bloku, tak jak tomu bylo na začátku bitcoinové sítě. [106]

Za plynulé fungování bitcoinové sítě může pokládat, když se transakce ukládají do bloků a bloky se za sebou zapojují do blockchainu. V momentu, co je nalezen neboli vytěžen nový blok, je zapojen plynule za blok předchozí a těžaři začínají těžit nový blok. V momentu, co jsou vytěženy dva nebo i více bloků ve stejný či podobný okamžik, je více bloků zapojena za stejný předcházející blok. V tento moment se již nejedná o řetěz bloků, kde jsou všechny bloky za sebou uspořádány. Situace jako tato se čas od času stane, kdy dva či více těžařů

[102] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 32
[103] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 41
[104] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 41
[105] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 49
[106] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 95

vytěží blok a rozešlou ho k validaci ostatním těžařům dříve, nežli jim samotným dorazí informace od těžaře druhého. Jejich vytěžené bloky nejsou stejné a je možné, že obsahují lehce odlišnou množinu nových transakcí, minimálně odměnu za těžbu směřují na jiného těžaře. Tato situace je známá jako fork. Bitcoin následující situaci musí rychle vyřešit, aby zajistil plynulost sítě a současně, aby nedošlo k jiným problémům, jako je například dvojí útrata. V řešení problému je za platný blok považován vždy ten nejdelší, který má blockchain k dispozici. V případě, že oba či více bloků jsou stejně dlouhé, platí ten, u kterého bylo zapotřebí vykonat nejvíce práce při jeho těžbě. Situace forku se tak rychle vyřeší a těžaři pokračují v těžbě pouze za jedním koncem bloků. Druhý konec bloků se v blockchainu nepoužije a stává se tzv. orphan blokem, který zaniká. Při samotném forku se může stát opět stejná situace, že dva těžaři vytěží bloky na dvou koncích ještě dříve, nežli se dozví o samotném forku. Tato situace se vyřeší opět stejnou metody, jako bylo vyřešeno v případě forku. Opět můžeme snadno rozhodnout, který ze dvou vytěžených bloků je delší, či který bylo náročnější vytěžit. Čím delší fork vzniká, tím klesá pravděpodobnost jeho vzniku exponenciálně.

Nyní je nutné specifičtěji vysvětlit jednotlivé procesy bitcoinové sítě.

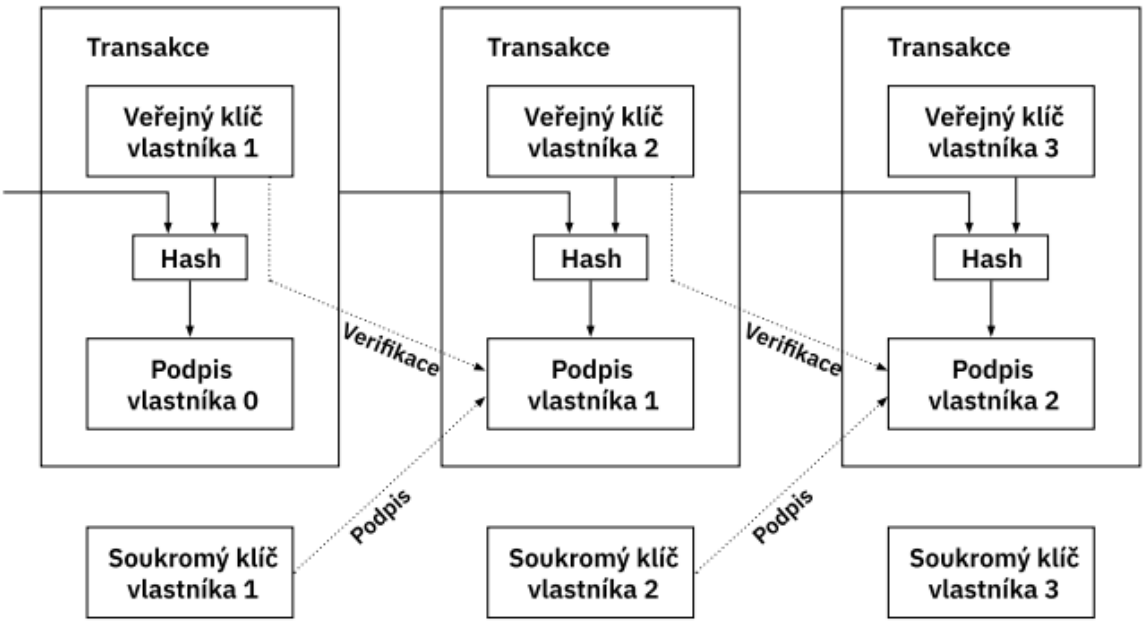
Transakce je prvním konkrétním tématem přímo se týkající fungování bitcoinové sítě.

„Elektronickou minci definujeme jako řetězec digitálních podpisů.“ [107] Převod mincí od jednoho vlastníka na druhého probíhá způsobem, že odesílající uživatel digitálně podepíše hash předchozí transakce a veřejný klíč přijímajícího uživatele sítě. Následně obojí přiloží na konec elektronické mince. Příjemce mincí poté může podpisy potvrdit a tímto se potvrdí řetěz vlastnictví.[108]

Příjemce mincí má potřebu důkazu, že transakce byla právě tou první přijatou, s tímto musí v okamžiku každé transakce většina uzlů sítě souhlasit, jak je zachyceno v obrázku 2. Je tedy eliminován problém „dvojí útraty“.[109]

[107] NAKAMOTO, S. *Bitcoin Whitepaper: A Peer-to-Peer Electronic Cash System.* 2008, s. 3
[108] NAKAMOTO, S. *Bitcoin Whitepaper: A Peer-to-Peer Electronic Cash System.* 2008, s. 3
[109] NAKAMOTO, S. *Bitcoin Whitepaper: A Peer-to-Peer Electronic Cash System.* 2008, s. 3

Obrázek 2 Schéma průběhu transakce



Zdroj: NAKAMOTO, S. Bitcoin Whitepaper: A Peer-to-Peer Electronic Cash System. 2008, s. 3

Proof of work, zkráceně PoW, je překládáno do českého jazyka jako „důkaz o vykonané práci“. Jedná se o náhodný proces, kterým jsou eliminovány hlavní problémy decentralizované sítě, a to absence centrální autority a důvěryhodnost zápisů do blockchainu. Tyto problémy jsou vyřešeny způsobem, že absence centrální autority je nahrazena decentralizovanou sítí, ve které se každý uzel podílí na ověřování provedených transakcí a současně má možnost na zisk odměny, které je získávána výměnou za vstupní náklady na výpočetní techniku a spotřebovanou energii. V neposlední řadě, je zajištěna spravedlivá odměna tomu, kdo první splní požadované podmínky za pomocí hashovací funkce.[110]

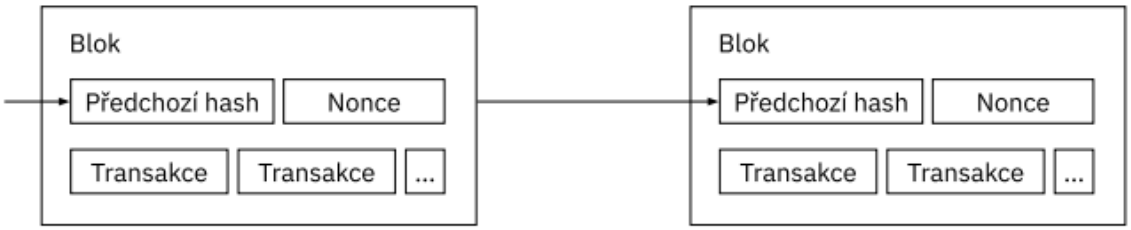
Princip proof of work je tedy založen na generování náhodného čísla, které je odvozeno matematicky od transakcí, které musí odpovídat náhodnému, sítí předem stanovenému rozmezí. Vše tedy funguje na bázi náhody, kdy výpočetní technika generuje náhodná čísla a snaží se najít právě ono číslo, které by jí pomohlo uzavřít blok a získat odměnu. Nalezené číslo musí tedy spadat do cílového rozsahu, který byl předem bitcoinovou sítí stanoven. Číslo musí být matematicky odvozeno z platné množiny transakcí, které musí být zapsány do blockchainu a transakce musí být platné dle pravidel sítě.[111]

[110] PRITZKER, Y. *Vynález jménem Bitcoin.* 2019, s. 28-31
[111] PRITZKER, Y. *Vynález jménem Bitcoin.* 2019, s. 28-31

PoW tedy pokládá za důkaz o vykonané práci náhodný proces, který k nalezení vítězného čísla potřebuje velké množství výpočetních operací, nicméně k potvrzení správnosti řešení stačí pouze jedna operace. To tedy v praxi znamená, že nalezení správného řešení zabírá dlouhou dobu, ale následné ověření správnosti je velmi rychlé. Systém o vykonané práci je z tohoto důvodu asymetrický, je obtížný pro těžaře, ale snadný pro ověřovatele. Důvodem spotřeby energie, tedy peněz při těžbě je i ten, že následně máte zájem o to, aby těžařům vytěžený blok všichni přijali a on tak získal náležitou odměnu. Proces je tedy podložen motivací jednat správně a zapisovat do blockchainu jen platné transakce. Předchází tak případným podvodům či útokům na síť. [112]

Pokus o podvodné jednání by tak na bitcoinové síti znamenal pouze mrháním zdrojů z důvodu odmítnutí podvodných bloků bez jakékoliv odměny za poskytnutý výkon. PoW a tedy i bitcoinová síť je založena na 100 % ověřování a 0 % důvěře.[113] Proces je zobrazen v obrázku 3.

Obrázek 3 Proof of work



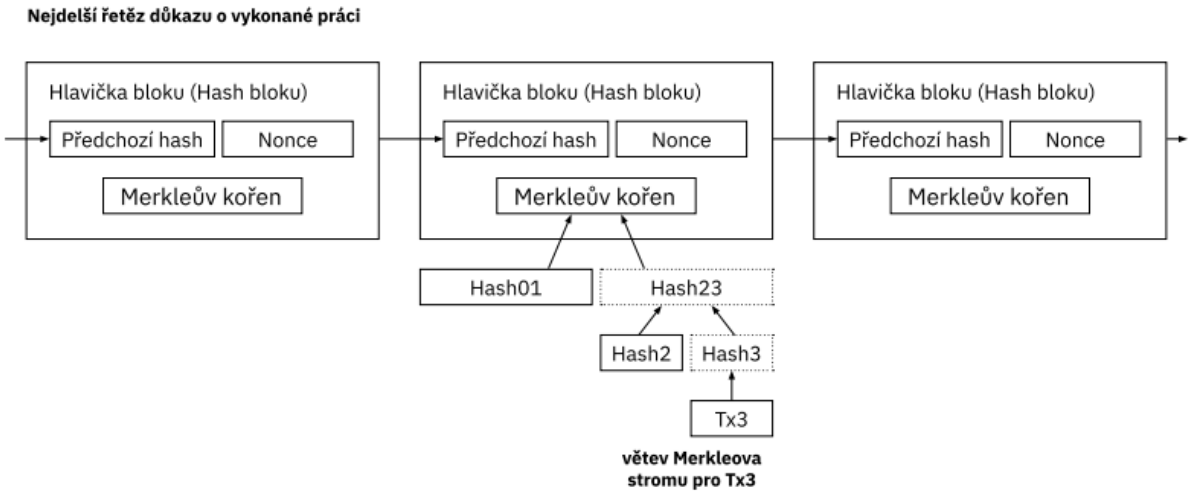
Zdroj: NAKAMOTO, S. Bitcoin Whitepaper: A Peer-to-Peer Electronic Cash System. 2008, s. 4

Distribuce nových mincí do sítě je vyřešena způsobem přidělení motivační odměny pro uzly neboli tvůrce bloků, které jsou tak motivovány síť podporovat. Tímto způsobem je vyřešena absence centrálního orgánu, který by v jiném případě mince vydával. Pro stabilní přírůstek konstantního množství do oběhu je zapotřebí vyložit výpočetní výkon a elektrickou energii. Motivační odměna je také financována za pomocí transakčních poplatků. V moment, co do bitcoinové sítě vstoupí předem stanovené množství mincí, tedy 21 milionu bitcoinů, motivační odměna je zcela financována z transakčních poplatků.[114]

[112] PRITZKER, Y. *Vynález jménem Bitcoin.* 2019, s. 28-31
[113] AMMOUS, S. *The Bitcoin Standard.* 2018, s. 173-175
[114] NAKAMOTO, S. *Bitcoin Whitepaper: A Peer-to-Peer Electronic Cash System.* 2008, s. 5

Ověřování plateb je proces, při kterém: *„Uživatel může platby ověřovat i v případě, že neprovozuje plnohodnotný síťový uzel. Stačí, když uchovává kopie hlaviček bloků z nejdelšího řetězce důkazu o vykonané práci.“* [115] Pro zisk této informace se musí dotazovat okolních uzlů, do doby, kdy má jistotu, že má nejdelší řetěz a následně odvodí kořen Merklova stromu propojením hledané transakce s blokem, který obsahuje časové razítko. Pro uživatele není možné samo ověření transakce, ale musí transakci ověřit v rámci její pozice v řetězci a ujistit se tak, že transakce byla přijata nějakým uzlem. Proces je zachycen v obrázku 4. [116]

Obrázek 4 Průběh ověřování plateb



Zdroj: NAKAMOTO, S. *Bitcoin Whitepaper: A Peer-to-Peer Electronic Cash System.* 2008, s. 7

Slučování a rozdělování částek řeší problém, kdy při převodu mincí se jeví neprakticky evidovat převody jednotlivě a provádět je oddělenými transakcemi. Z tohoto důvodu transakce obsahují více vstupů a výstupů. Většinou se jedná o transakci s jediným vstupem z předchozí transakce nebo o několik vstupů poskládaných z menších částek a maximálně dvou výstupů. [117]

[115] NAKAMOTO, S. *Bitcoin Whitepaper: A Peer-to-Peer Electronic Cash System.* 2008, s. 6
[116] NAKAMOTO, S. *Bitcoin Whitepaper: A Peer-to-Peer Electronic Cash System.* 2008, s. 6-7
[117] NAKAMOTO, S. *Bitcoin Whitepaper: A Peer-to-Peer Electronic Cash System.* 2008, s. 7

Ochrana osobních údajů je problémem, který vzniká u decentralizované sítě. Oproti tradičnímu bankovnímu systému, který zajišťuje určitou míru integrity informací způsobem, že poskytuje přístup k informacím pouze zúčastněným stranám, společně s prověřenou třetí stranou. Model bitcoinové sítě takovéto možnosti nemá, vzhledem k tomu, že musí zveřejňovat všechny transakce. Důvěryhodnost informací zachovává způsobem přerušení toku informaci na jiném místě, tedy, že veřejné klíče zanechá anonymní. Lze tedy vidět, že jeden uživatel posílá určitou částku uživateli druhému, ale již zde nejsou uvedeny žádné informace, které umožní spojit transakci s konkrétními osobami. Pro zachování anonymnosti je doporučeno používat vždy novou dvojici klíčů tak, aby nebylo možné více transakcí spojit s jednotlivým uživatelem. Nicméně s rostoucím množstvím provedených transakcí roste i riziko odhalení uživatele. Toto platí před pověřením procesu KYC. Následně již uživatel poskytl o sobě důvěryhodné informace, které je s provedenými transakcemi snadné propojit.[118]

[118] NAKAMOTO, S. *Bitcoin Whitepaper: A Peer-to-Peer Electronic Cash System.* 2008, s. 7-8

3.5 Těžba Bitcoinu

Těžba bitcoinů je proces, při kterém se hledá další blok pro napojení do blockchainu, za pomocí strojově náročných výpočtů. Pro nalezení validního bloku je třeba splnit podmínku, že jeho hash je nižší nežli určitý cíl. Cílem je brán parametr target, tedy číslo začínající na mnoho nul v numerickém zápise hashe, známé jako nonce. Tento stanovený cíl je odvozen od momentální **úrovně difficulty** neboli obtížnosti, která je změněna každých 2016 bloků. Úroveň difficulty závisí na rychlosti nalezení nových bloků tak, aby byla splněna podmínka, že průměrná rychlost generování nových bloků byla 1 blok za 10 minut a v podstatě určuje, jak náročné je bitcoin vytěžit. V případě, že blok nesplní podmínku na nízký hash, je třeba jeho serializaci upravit.[119]

Při prvotním spuštění sítě se těžba prováděla na procesorech samostatných osobních počítačů, ale se rostoucí obtížností způsobenou nárůstem těžařů se těžba přesunula k využití procesorů v letech 2009-2010. Následovala těžba bitcoinů za pomocí grafických karet v letech 2010-2011, následně k programovatelným hradlovým polím v letech 2011-2012 až k ASIC minerům, na kterých těžba bitcoinů probíhá dodnes. Od roku 2011 se navíc těžba soustřeďuje do těžebních poolů.[120]

I v dnešní době lze bitcoiny stále těžit, ale těžba se s postupem času stává stále více náročná jak z technologické, tak i finanční stránky. V momentu, co bude vytěženo všech 21 milionů bitcoinů, samotné těžba nových bitcoinů zanikne. To se uskuteční přesně v roce 2140. Většina bitcoinů však bude vytěžena již v roce 2033. Nicméně těžaři nebudou vypínat své těžební stroje, ale budou pokračovat v ověřování transakcí, za které budou nadále dostávat odměny financované z transakčních poplatků. [121] [122]

Hash je digitální otisk, jehož vlastností je, že nelze zjistit původní vstup, kromě vyzkoušení všech možností a je využívám v kryptografii.[123]

[119] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 90
[120] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 90
[121] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 38
[122] AMMOUS, S. *The Bitcoin Standard.* 2018, s. 177-179
[123] PRITZKER, Y. *Vynález jménem Bitcoin.* 2019, s. 31-32

Hash rate neboli hashovací rychlost je veličina udávající míru výpočetního uzlu nebo kompletní bitcoinové sítě. Hash rate tedy vypovídá o výpočetní síle zapojené do bitcoinové sítě. Výpočetní výkon je do sítě dodán pomocí těžebních strojů, které nonstop řeší komplexní matematické výpočty hledáním nonce pro uzavření bloku a současně verifikování bitcoinové transakcí. Stroj tak musí provést miliony odhadů pro nalezení nonce za sekundu.[124]

Její jednotkou je h/s, která udává počet spočtených hashů za sekundu. Využívanými jednotkami jsou:

- 1 h/s
- 1 kh/s = 1000 h/s
- 1 Mh/s = 1000 kh/s
- 1 Gh/s = 1000 Mh/s
- 1 Th/s = 1000 Gh/s
- 1 Ph/s = 1000 Th/s
- 1 Eh/s = 1000 Ph/s

Výkon sítě mezi lety 2009-2020 zvýšil z 1 Mh/s na 100 Eh/s, tedy o 14 dekadických řádů.[125]

Hashovací funkce je speciální funkce, do které lze vložit jakákoliv řetězec písmen či jiných znaků a vznikne obsáhlé a náhodné číslo. Vloženo může být například „Hello world“. Výsledek bude:

- 8699136604439246766178316516697330902380718164802471877831352638989 2860994842.

Hashovací funkce využívaná v bitcoinové síti se nazývá SHA-256.[126]

SHA-256 je zkratka pro „Secure Hash Algoritmus“, tedy v českém jazyce „Bezpečný hashovací algoritmus“. Jedná se o kryptografickou funkci, která z libovolně dlouhého vstupu vytváří výstup fixní délky. To tedy znamená, že z transformovaného výstupu je v podstatě nemožné rekonstruovat původní vstup, a stejně tak je nemožné narazit na dvě rozdílné

[124] SoFi Learn. *Bitcoin Hash Rate adn Why It Matters* [online]. Dostupné z: https://www.sofi.com/learn/content/bitcoin-hash-rate/
[125] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 93
[126] PRITZKER, Y. *Vynález jménem Bitcoin.* 2019, s. 31-33

zprávy s totožným výstupem. Číslo 256, které je součástí zkratky, označuje délku výstupu v bitech.[127]

„***Nonce*** *značí v kryptografii číslo, které se používá jako jednorázová hodnota přinášející náhodný element. Takové hodnotě není přisuzován žádný specifický význam, její role spočívá pouze v její libovolnosti a nemožnosti ji odhadnout. Nonce tvoří součást bitcoinového bloku proto, aby bylo možné tuto hodnotu libovolně měnit a zkoušet tak hledat hash hlavičky splňující podmínku pro platný blok.“* [128]

ASIC je označení pro „Application-Specific Integrated Circuit“ což v českém jazyce znamená zákaznický integrovaný obvod. Jedná se o speciální hardwarové zařízení, které slouží výhradně jako těžební zařízení. Tento jednoúčelový stroj je navržen k počítání hashovacích algoritmů SHA-256. Odvádí tak důkaz o provedené práci, který je základem bitcoinové sítě. V současné době představuje jediný efektivní způsob těžby Bitcoinu. Nahradil tak dříve používané grafické karty a klasické procesory v počítačích, které již nemají dostatečný výkon pro těžbu.[129]

3.5.1 Halving

Při procesu těžby vznikají nové bitcoiny, které jsou přisouvány do sítě. Záměrem tvůrce sítě Satoshiho Nakamoty byla vytvoření systém, u, ve kterém nebude docházek ke znehodnocení a proto nechtěl, aby zásoba bitcoinů narůstala donekonečna. Z tohoto důvodu vytvořil časový plán, ve kterém se bitcoiny budou uvolňovat postupně, s rapidním začátkem, který se bude pravidelně zpomalovat.[130]

Při spuštění bitcoinové sítě byla odměna za jeden vytěžený blok 50 bitcoinů. V kódu Bitcoinu je ovšem zabudováno půlení blokové odměny neboli halving, které odměnu za vytěžený blok jednou za přibližně 4 roky sníží o polovinu. Pojem času se v bitcoinové síti počítá na vytěžené bloky nežli na uplynutí určitého času. Vzhledem k tomu, že vytěžení jednoho bloku trvá zhruba 10 minut, vychází časové rozmezí obdobně.[131]

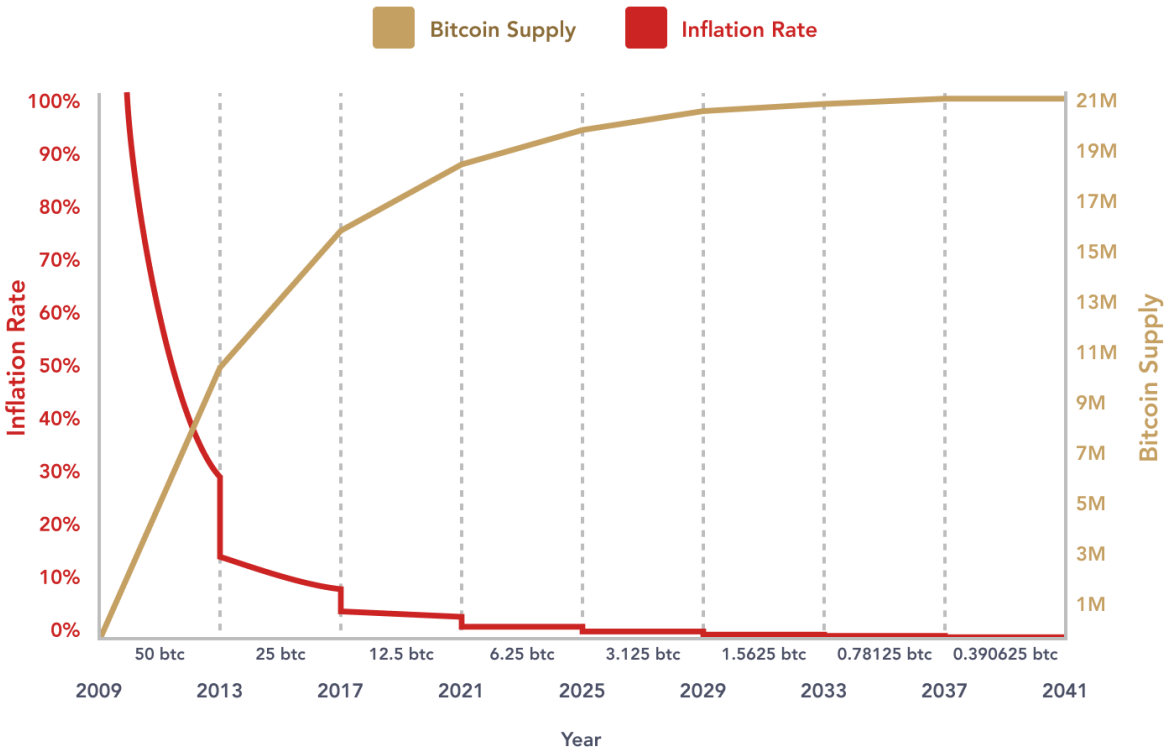
---

[127] PRITZKER, Y. *Vynález jménem Bitcoin.* 2019, s. 111
[128] NAKAMOTO, S. *Bitcoin Whitepaper: A Peer-to-Peer Electronic Cash System.* 2008, s. 13
[129] PRITZKER, Y. *Vynález jménem Bitcoin.* 2019, s. 105
[130] PRITZKER, Y. *Vynález jménem Bitcoin.* 2019, s. 44-45
[131] PRITZKER, Y. *Vynález jménem Bitcoin.* 2019, s. 44-45

Odměna za vytěžený blok byla v roce 2009 50 bitcoinů, v roce 2012 se snížila na 25 bitcoinů, v roce 2016 to již bylo 12,5 bitcoinů a v současné době je odměna na hodnotě 6,25 bitcoinů, kterou stanovil poslední halving v roce 2020. Za následujících 12 let, ve kterých proběhne halving celkem třikrát, bude v oběhu bitcoinové sítě uvolněno více než 99 % bitcoinů. V roce 2140 odměna za vytěžený blok spadne na 0 a těžaři budou odměňováni pouze transakčními poplatky. Online odpočet do dalšího halvingu, který Bitcoin čeká v roce 2014, lze sledovat na internetových stránkách: bitcoinblockhalf.com.[132] [133]

Vývoj uvolňování nových bitcoinů s půlením odměn při každém halvingu v poměru s vývojem celkového množství bitcoinu v oběhu je zachycen na grafu 2.

Graf 2 Vývoj přísunu nových bitcoinů k celkovému množství bitcoinů v oběhu



Zdroj: River Financial [online]. Dostupné z: https://river.com/learn/who-creates-new-bitcoin/

[132] PRITZKER, Y. *Vynález jménem Bitcoin.* 2019, s. 44-45
[133] Bitcoinblockhalf. *Bitcoin Block Reward Halving Countdown* [online]. Dostupné z: https://bitcoinblockhalf.com

3.6 Fundament Bitcoinu a jeho vývoj

Bitcoin se neustále vyvíjí k lepšímu. V decentralizovaném světě Bitcoinu může naprosto každý navrhnout změny fungování sítě a protokolu prostřednictvím tzv. BIP.[134]

BIP zkratka znamenající Bitcoin Improvement Proposal, volně přeloženo do českého jazyka jako návrh vylepšení Bitcoinu, je dokument obsahující návrh na změnu fungování Bitcoinu nebo obsahující důležitou informaci ke vztahu k bitcoinové síti. Zkratka BIP je doprovázena pořadím BIPu, např. BIP 1. BIP běžně obsahuje návrh na přidání nové funkcionality společně s motivací pro její zavedení, přesné specifikace, návrh řešení a analýzu kompatibility.[135]

Tým vývojářů Bitcoin Core o návrhu změn diskutuje v komunitě a případně zavádí změny v softwaru. Součástí diskuze je i hlasování těžařů o změně. Hlasování se provádí za pomocí rezervovaných bitů v hlavičce jimi vytěžených bloků. Po určitou bodu těžaři signalizují připravenost pro přijetí změny, obvykle v posledních 1000 blocích a je vysoká shoda pro přijetí změny v rozmezí obvykle od 75 % do 95 %, dostává se návrh to tzv. „point of no return“. Návrh se poté stává platným a dojde k jeho uzamčení. Následně v určitém časovém rámci dojde k aktivaci změny a síť se začne řídit dle nových pravidel.[136]

Bitcoin Core je referenční implementace klienta pro bitcoinovou síť. Implementace je vyvíjena v jazyce C++ a obsahuje kód k provozu plnohodnotného síťového uzlu, tedy stahuje a validuje celý blockchain.[137]

V bitcoinové síti nikdo nemá možnost přinutit ke změně jiné uživatele, i kdyby se změnou souhlasili všichni ostatní. Bitcoin nemá formu demokracie, ale plné svobody. Kdo s novou změnou nesouhlasí či se mu nelíbí, není nucen přecházen na novou verzi softwaru. Pokud se rozhodne zůstat u starého softwaru beze změny, podstupuje tím risk, že software nebude dostatečně kompatibilní s novou verzí, a právě on zůstane v sítí osamocen, což jde proti smyslu sítě, která je určena pro interakci s ostatními. Užitná hodnota sítě roste kvadraticky s počtem uživatelů sítě. V případě menších změn použití starého softwaru způsobí uživateli jen malý diskomfort, či nemá přístup k novým funkcionalitám. Když se jedná o zásadnější změnu, jako je třeba fundamentální změna bitcoinového protokolu,

[134] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 130
[135] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 130
[136] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 130
[137] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 131

používáním starého softwaru nemusí umožnit užívání bitcoinové sítě. Může dojít i k situaci, kdy vytěžené bloky ve starém softwaru nová verze sítě považuje za nevalidní. Zásadní pravidlo je, že jeho doposud získané peníze před uvedením změny v platnost jsou neohroženy.[138]

Přístup k přijetí změn je však velmi konzervativní. V případě podstatných změn je situace často nepříjemná pro všechny zúčastněné strany. Vývojáři musí dbát na správnost implementace, těžaři se musí na změnu do předu připravit a samotní uživatelé musí změnu přijmout. Někdy ale nastává situace, kdy je změna nezbytná pro vyřešení problému, který s užíváním sítě vychází na povrch. [139]

3.6.1 Fork

K forkům nedochází pouze vlivem náhody v časování sítě, ale i při změně pravidel fungování sítě. V momentu, kdy dojde kde změně protokolu, která přináší novou funkcionalitu Bitcoin a je k ní nutno poupravit datový formát bloku či transakce. Následně již síť může generovat nové, již pozměněné bloky. Přejdou-li všichni těžaři a běžní uživatelé na její novou verzi, síť začne generovat pozměněné bloky v návaznosti na poptávku uživatelů po nové funkcionalitě. V tomto případě již všichni uživatelé sítě novým pozměněným blokům rozumí a nenastává žádný problém.[140]

Existuje však možnost, že někteří uživatelé nejsou ochotni na novou verzi přejít. V některém případě stará verze softwaru považuje bloky za validní, někdy nikoliv. Je očividné, že stará verze softwaru nebude uměl pracovat s funkcionalitou, kterou nabízí verze nová. Neznamená to ale automaticky, že stará verze nové bloky zcela odmítne. Je-li změna navržena jako zpětně kompatibilní, tak stará verze softwaru bude nadále fungovat. Tato možnost je pro uživatele ideální východisko, vzhledem k tomu, že starou verzi mohou nadále používat a pro přechod na novou verzi softwaru se rozhodnou v případě, že chtějí využívat novou funkcionalitu. Této změně se říká softfork. Na novou verzi softwaru musí přejít hlavně těžaři, u kterých je jasné, že bez jejich podpory by nebylo možné novou funkcionalitu využít, vzhledem k tomu, že by nikdo nebyl schopen vygenerovat pozměněné bloky. Z tohoto důvodu mají právě těžaři možnost hlasovat o návrzích změn. Hlasováním se zjistí,

[138] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 130-131
[139] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 131
[140] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 133

zda je o přechod na nový software vůbec zájem a zda má cenu změnu do sítě implementovat. Zejména u podstatných protokolových změn je vyžadována vysoká shoda, častokrát více než 90 %. Je snaha předejít situaci, kdy by někteří těžaři na nový software nebyli ochotní přejít a jejich vytěžené bloky by stále byly validní ve starém softwaru, ale již by nebyly validní v softwaru novém. Tato situace by často tvořila forky a následkem by byl vznik mnoha orphan bloků. To je nežádoucí situace pro těžaře, protože tím přichází o odměnu za poskytnutý výpočetní výkon a raději tak upřednostní přechod na nový software i v případě, že se na výsledku hlasování o novém návrhu změny shodlo pouze devět z deseti těžařů. Změnu tedy nakonec přijmou všichni těžaři.[141]

Nelze však veškeré změny implementovat jako zpětně kompatibilní. Do jaké míry lze změnu zpětně implementovat závisí hlavně na flexibilitě původního protokolu. Dopředné kompatibility je možné dosáhnout prozřetelností při jeho návrhu. [142]

V momentu, kdy je nutné provést změnu, která již není zpětně kompatibilní se starým softwarem, nejedná se již o situaci softforku, ale nastává situace zvaná hardfork. Zásadní odlišností je to, že stará verze softwaru po hardforku považuje nové bloky za nevalidní. Uživatelé, kteří nepřejdou na novou verzi softwaru, nemohou síť nadále využívat. K přechodu na novou verzi softwaru jsou tedy nuceni všichni uživatelé sítě, jak těžaři, tak běžní uživatelé. V případě, že se někteří těžaři a společně s nimi někteří uživatelé (minimálně jeden) rozhodnou, že přechod na novou síť neakceptují a zůstanou užívat síť starou, blockchain bude rozdělen trvalým forkem. Tato situace se nazývá split blockchainu. Spolu s těžaři na staré síti musí zůstat i běžní uživatelé, jinak nemá těžař důvod v síti zůstávat a poskytovat tak výpočetní výkon pro nikoho. Vše záleží na tom, zda bude nadále zájem o využívání staré sítě před změnou.[143]

Po splitu blockchainu vznikají dvě samostatné měny. O svou hodnotu mezi sebou budou u uživatelů vzájemně soupeřit rozdíly svých pravidel, kvalitou svého budoucího vývoje a sílou své komunity, která se rozhodne u sítě zůstat či přejít. Jedná se tedy o decentralizovanou diverzifikaci. Vypořádání mincí, které byly vlastněny před hardforkem uživateli zůstávají. Nová síť se řídí stejnými pravidly a uživatel tak obdrží i pozměněné mince dle nových pravidel sítě nové. V případě, že uživatel drží soukromé klíče od svých kryptoměn na své offline peněžence, má po hardforku 2 druhy mincí. Jednu tak získal zcela

[141] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 133-134
[142] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 133-134
[143] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 134-135

zdarma. Problém nastává v moment, má-li své mince uložené na online peněžence nebo na burze. V tomto případě je závislý na rozhodnutí jejich provozovatelů, zda mu bude přiznáno vlastnictví i mincích druhých. Pravděpodobná je i situace, kdy hodnota mincí po provedeném hardforku klesne a uživatel tak i v součtu obou měn nedosáhne stejného finančního ohodnocení jako, mince před hardforkem. Vše je závislé na reakci trhu.[144]

3.6.2 Škálování

Bitcoin se v průběhu let 2016 a 2017 musel vypořádat s problémem škálování., vzhledem k tomu, že s rostoucí popularitou bitcoinová síť přestávala stíhat zpracovávat objem transakcí.[145]

Škálování je proces přizpůsobení sítě k velkému nárůstu počtu uživatelů.[146]

Základním problémem je fakt, že velikost jednoto bloku, tedy nositele informací o transakcích, je od počátku navržena na velikost maximálně 1 MB = 1 milion bajtů s průměrnou dobou mezi dvěma vytěženými bloky přibližně 10 minut. Při běžné velikosti transakce okolo 0,25 kB tak vychází, že maximální počet transakcí je zhruba sedm za jednu sekundu. V porovnání s klasickými centralizovanými platebními systémy, jako je třeba Visa, 7 transakcí za sekund je extrémně málo. Běžný klasický centralizovaný platební systém zvládá bez problému provést transakcí za sekundu několikanásobné více. Bylo tedy zřejmé, že dřív nebo později se tento problém dostaví a poptávka po transakcích bude větší, nežli činí malá a konstantní nabídka.[147]

Z počátku se jevila nejjednodušší možnost odstranění limitu na velikost bloku. Problémem s tímto řešení však bylo to, že limit na velikost bloku byl do zdrojového kódu zanesen samotným Satoshim Nakamotou. Satosthi tento limit údajně zavedl jako ochranu proti případnému spamovému útoku, který by mohl nastat pár let po spuštění bitcoinové sítě, na tehdy ještě skoro prázdný blockchain. Jeho úmyslem bylo tento limit časem odstranit. Zásadním problémem potencionálního odstranění limitu velikosti bloku je fakt, že pro tento krok by vyžadoval hardfork, kterému se vývojáři snaží vyhnout za každou cenu. O hardfork by se jednalo z důvodu, že by došlo k navýšení velikosti bloků oproti verzi původní. Pokud by se změna vydala opačným směrem a limit by se naopak zpřísňoval, jednalo by se pouze

[144] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 134-136
[145] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 136-137
[146] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 136-137
[147] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 136-137

o softfork a změnu by tam bylo dalo snadnější implementovat. Další složitostí pro tuto změnu by byla dohoda na specifickém novém limitu nebo obecnějšího schématu jeho pozvolném zvětšování či jiném řešení. V tento moment by do procesu rozhodování vstupovalo příliš mnoho osob, které by si museli vybrat z příliš mnoha možností řešení. [148]

Postupem času přicházely první konkrétnější návrhy na změnu škálování Bitcoinu, které se nejvíce lišily mírou konzervativnosti navrhované změny. Přišla myšlenka o přesun malých transakcí mimo blockchain, známé jako „off-chain" mikro platby. Následně přišel nápad na zmenšení transakcí pomocí tagů, známé jako „Flexible Transactions. Toto řešení by ovšem opět vyžadovalo hardfork. Koncem roku 2015 přišel návrh BIP 141 na tzv. segwit.[149]

Více než o systémové řešení škálování Bitcoinu je segwit spíše vylepšení a oprava nedostatků, které bitcoinový protokol dlouhodobě zatěžovaly. Segwit měl na škálování Bitcoinu ihned dva pozitivní dopady. Prvním bylo, že vlivem kvalitní implementace se do bloku vejde o 80 % více transakcí, za předpokladu, že všichni používají segwit. Druhým bylo odstranění maleability transakce, což usnadňuje implementovat tzv. „Lightning Network" pro realizaci mikro plateb mimo hlavní blockchain. LN by bylo možné implementovat i bez segwitu, ale takto se předchází potencionálním nepříjemnostem. Segwit je v podstatě řešení známého systémového problému a „odrazový můstek" pro řešení skutečného problému se škálováním. Hlavní výhodou segwitu bylo nalezení způsobu, jak jej implementovat jako softwork. Pro jeho schválení bylo zapotřebí minimálně 95 % hlasů všech těžařů, která se na začátku setkávala s úspešností v hlasování pouze okolo 30 %.[150]

To se ovšem nelíbilo komunitě běžných uživatelů, kteří návrh seqwitu chtěli přijmout. Nespokojeni byli také s tím, jak dlouho se proces přijetí táhl a že finální slovo mají vždy těžaři. Jsou to nicméně uživatelé, kteří Bitcoinům dávají hodnotu a z této hodnoty poté těžaři profitují. Uživatelská komunita se proto rozhodla předložit UASF.[151]

UASF je zkráceně „User Activated Softfork", přeloženo jako uživatelsky aktivovaný softfork. V tomto návrhu uživatelé, zastupováni zejména představiteli velkých firem, které podnikají nad Bitcoinem, oznámili těžařům, že od 1.8.2017 nebudou akceptovat vytěžené

[148] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 136-137
[149] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 136-138
[150] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 137-138
[151] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 139

bloky nepodporující segwit. Těžaři tedy dostali ultimátum návrh segwitu přijmout, jinak by jejich poskytnutý výpočetní výkon vešel naprázdno a oni tak přišli o své finanční zisky.[152]

V květnu roku 2017 vzešla dohoda NYA, zkrácená verze „New York Agreement", která obsahovala dva hlavní body. Prvním byla aktivace segwitu, druhým bodem bylo zvětšení bloku na 2 MB. Tento návrh se označuje jako Segwit2x, vzhledem ke schválení segwitu a dvojnásobnému zvětšení bloku. Segwit2x, který po aktivaci odmítá bloky nepodporující segwit, v návaznosti na UASF. Na schválení neboli uzamčení návrhu stačila podpora 80 % těžařů. Dohoda získala podporu zejména těžařů z Číny, kde v tehdejší době bylo okolo 80 % veškerého výpočetního výkonu sítě neboli hash ratu.[153]

K naplánovanému harforku o zvětšení bloku, který byl součástí NYA nakonec nedošlo. Podpora uživatelů sítě s postupem času oslabovala a současně byly zjištěny nevyřešené technické problémy koexistence dvou sítí, například „replay protection".[154]

Replay protection je termín označující odolnost sítě po hardforku, tak aby nebylo možné zaměnit transakce sítě s transakcemi sítě původní a naopak. V případě, že síť nemá takovouto odolnost, útočník může zachytit transakci původně určenou jen pro jednu ze sítí a následně ji rozeslat i do sítě druhé. To způsobí nezamyšlený převod mincí na totožnou cílovou adresu i v síti druhé. Tento typ útoku je označován jako tzv. **replay attack**. Pro dosažení odolnosti proti tomuto typu útoku je třeba pozměnit formát transakce.[155]

V podstatě tedy nevznikl software, který by implementoval tuto část Segwit2x a před očekávaným nasazením byl Segwit2x pozastaven. Hardfork Segwit2x se tedy nekonal, namísto toho byla upřednostněna implementace softforku segwit a k UASF tedy nedošlo.

Bitcoin je postaven v decentralizovaném světě, kde si každý může řešit situaci v případě nespokojenosti dle vlastního uvážení. Skupina uživatelů bitcoinové sítě, která byla sdružena kolem čínského výrobce hardwaru pro těžbu bitcoinů Bitman, která byla současně provozovatelem těžebních poolů, vydala v červnu roku 2017 prohlášení o své obavě ohledně hrozby plynoucí z UASF, jehož podpora trvala i po NYA. Společnosti Bitmain tedy přišla s vlastním řešením pojmenovaný UAHF.[156]

---

[152] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 139
[153] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 139-140
[154] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 139-140
[155] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 140
[156] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 141

UAHF je zkráceně „User Activated Harfork“ neboli uživatelsky aktivovaný hardfork. Jednalo se o hardfork, který měnil velikost bloku až na 8 MB, který se k této kapacitě postupně navyšoval až do srpna roku 2019. Hardfork by se aktivoval 12 hodin po případném UASF. Zpočátku se nebránil adopci segwitu a jeho vývoj pokračoval. Výraznou změnou se stala implementace Bitcoin ABC a k ní příslušející síť jménem Bitcoin Cash, ve které byla měna sítě se zkratkou BCH.[157]

Hardfork se uskutečnil dne 1.8.2017, tedy od bloku 478559. Blockchain bitcoinové sítě se poprvé splitnul, tedy blockchain byl rozdělen trvalým forkem na dva blockchainy. Po této události zavládla doba nejistoty. Jedny burzy dávali uživatelům přislib, že obdrží mince obou blockchainů, druhé varovaly své klienty, že potencionální podpora Bitcoin Cash není zaručena a upřednostňovaly řešení volby BTC před splitem.[158]

Po několika týdnech od splitu většina burz implementovala podporu pro BCH jako další měnový pár. Cena BCH se během roku 2017 ustálila zhruba kolem 20% ceny BTC. Na tento projekt následně navázal projekt Bitcoin Gold, který se zaměřil na nižší náročnost těžby užitím slabšího hardwaru, ale jeho cena se pohybovala pouze okolo 10 % ceny BCH, tedy okolo 2 % ceny BTC.[159]

Klasický Bitcoin tedy zůstal tím „pravým“ Bitcoinem, který o existenci Bitcoin Cash neví. Ten se stal odvětveným blockchainem a jeho pravidla se změnila na zpětně nekompatibilním softwarem s tím starým. Stejně tak tomu bylo i v případě Bitcoin Gold.[160]

Postupem času docházelo k výraznému nárůstu dlouhodobě nepotvrzených transakcí a s nimi přicházely i rapidní zvyšování poplatků za transakci v rámci soutěže uživatelů o jejich rychlé potvrzení. Na konci roku 2017 činily poplatky za středně velkou transakci, v přepočtu s tehdejším kurzem, stovky českých korun. Velké transakce stály v řádek desetin bitcoinu. Byla dokonce nalezena transakce přesouvající 25 bitcoinů, která byla zpoplatněna 1 BTC, tehdy okolo 350 tisíc. Kč. Tento fakt činil Bitcoin pro běžné užití v podstatě nepoužitelný. Většina nepotvrzených transakcí tak končila v tzv. mempoolu.[161]

---

[157] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 141
[158] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 141-142
[159] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 141-142
[160] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 143
[161] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 143-144

Mempool je virtuální prostor ve kterém čekají transakce na potvrzení. Každý uzel má svůj vlastní mempool. Na přelomu roku 2017 a 2018 byla velikost kompletního mempoolu v řádek stovek MB. Vzhledem k velikosti jednoho bloku 1 MB i s využitím transakcí se segwitem se jednalo o průměrné čekání na potvrzení transakce v řádu dnů.[162]

Problém se škálováním Bitcoinu tak doposud zůstává v podstatě nevyřešen. Segwit není řešením problému se škálováním, ale jedná se spíše o poklad pro možná řešení. Budoucí řešení můžeme v podstatě rozdělit do dvou hlavních kategorií – on-chain nebo off-chain.[163]

On-chain neboli „uvnitř řetězu (bloků)" je řešení usilující o zapsání všech transakcí do blockchainu. Jedná se o možnost, kterou si zvolil Bitcoin Cash a je zjevné, že se jedná o variantu, která musí vést ke zvětšování velikosti bloků s odvoláním na původní myšlenku Bitcoinu. Vznikající otázkou je, zda bude k dispozici taková technologie, která by v reálném čase byla schopna zpracovat bloky dostatečně velké tak, aby obsáhly všechny probíhající transakce po celém světě. Riziko, které při tomto řešení vzniká, je v decentralizaci sítě, která se součástí původní myšlenky Bitcoinu. Vzhledem k vysokým požadavkům na technologii, vzniká hrozba, že právě tako technologie bude držena v rukou pouze několika „mocných", kteří si tuto technologií budou moci finančně dovolit a pojde tak ke značnému snížení decentralizace sítě.[164]

Off-chain je přístupem, který by zanechával pouze některé transakce na blockchainu. Jednalo by se nejčastěji o velké transakce nebo takové, které nevyžadují rychlé potvrzení. Ostatní běžné mikro platby, jako platby v restauraci či v obchodě by se přesouvali a akumulovali mimo blockchain po nějakou dobu, dokud nebude vyžadováno jejich vypořádání, a to jak transakce průběžné, tak i konečné. V tento moment se o nich dozví hlavní blockchain. V podstatě se jedná o hierarchizaci platebního systému nad hlavním blockchainem, který se stává vrstvou první úrovně. Vrstvou další úrovně může být například Lightning Network.[165]

[162] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 143-144
[163] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 144
[164] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 144
[165] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 144-145

3.6.3 Lightning Network

Lightning Network, zkratka LN, je jedním v současnosti vyvíjeným návrhem off-chainového řešení, který řeší problém škálování. Jedná se o vrstvu druhé úrovně nad Bitcoinem a přináší rychlou realizaci mikro plateb. Do blockchainu se neukládají veškeré informace o mikro platbách, nýbrž jejich agregovaný stav.

LN funguje stylem tak, že se otevře tzv. „Lightning kanál“, do kterého obě strany vloží své mince/peníze. *„Z hlediska Bitcoinu je kanál multisig adresa, se kterou mohou disponovat pouze obě strany současně. Zároveň ale platí, že po nějaké definované době (např. měsíc) si svou část vkladu na tuto adresu mohou strany vzít zpět.“* [166]

Multisig je podmínkou uvolnění BTC z výstupu transakce za využití více podpisů. Jedná se v podstatě o speciální případ kontraktu. V případě multisig transakce se jedná o transakci, která uvolňuje BTC za pomocí multisig podmínky. Nejčastěji je využívám pří řízení přístupu ke kolektivně spravovaným financím.[167]

Jedná se v podstatě o smart kontrakt, který kombinuje podmínku více podpisů, tedy multisig, a časovou podmínku, timelock. Důvodem potřeby časové podmínky je pojištění proti nespolupracují protistraně. Díky tomu nikdo nemůže přijít o své vložené peníze. Lightning Network je tzv. „trustless“. To tedy znamená, že nespoléhá na důvěryhodnost vstupujících stran a použití LN je tedy stejně bezpečné jako použití samotné sítě Bitcoinu, přinejmenším v tomto případě.[168]

Otevřený kanál mezi dvěma uživateli je tedy adresa, na které jsou uloženy peníze obou uživatelů a současně možnost, jak je mohou dostat nazpět v určitém poměru vkladů. Poté, co dojde k otevření kanálu, odpovídá poměr těchto vkladů počátečnímu vkladu obou uživatelů. Při každé uskutečněné platbě dojde k aktualizaci zůstatků v kanálu ve prospěch příjemce a na vrub plátce. Tyto vzájemné platby se tak nemusí ihned vypořádat na blockchainu a současně je tento systém kryptograficky bezpečný. K aktualizaci zůstatků dojde vygenerováním speciálních transakcí, které si obě strany vzájemně vymění, ale nerozesílají je do bitcoinové sítě. Těmto transakcím se říká tzv. **commitment transakce** a v systému ručí, že jednotlivé strany nepřijdou o své zůstatky, pokud by opačná strana přestala komunikovat. Kanál je možné mít otevřen libovolně dlouho a je současně možné ho

[166] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 145
[167] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 145
[168] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 145

kdykoliv uzavřít dle potřeby uživatelů. K této situaci obecně nastává, je-li třeba zapsat poslední stav do blockchainu, například po vyčerpání zůstatku jedné strany nebo v případě, že jedna ze stran nadále nekooperuje. Uzavření kanálu se provede odesláním commitment transakce znárodňující poslední stav kanálu. Do blockchainu se tak zapíší pouze dvě transakce, otevření a uzavření kanálu. Transakce tak probíhající mezi těmito dvěma transakcemi a jsou věcí Lighning Networku.[169]

Jednou z nevýhod LN je fakt, že příjemce platby musí být online, což u klasických on-chane platbách není za potřebí. Platba se jednoduše zapíše do blockchainu a příjemce tak v podstatě nemusí být nijak aktivní. Naopak výhodou LN je rychlost, s kterou realizuje platby, která je omezena jen a pouze rychlostí sítě, navíc transakce jsou v LN mnohem více anonymní nežli při platbách on-chane.[170]

Na hlavním blockchainu je LN k dispozici od roku 2018. Čas tedy ukáže, zda právě LN bude řešením problému se škálováním.[171]

[169] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 145-148
[170] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 147-148
[171] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 149

3.7 Ekonomické základy Bitcoinu

Při pochopení podstaty Bitcoinu, můžeme nalézt kořeny této kryptoměny v souboru ekonomických teorií vydávány pod názvem Rakouská ekonomická škola. Ta vznikla v druhé polovině devatenáctého století zapříčiněním rakouský ekonomů a za základní dílo je považováno dílo autora Carla Mengera „Základy národohospodářské nauky“. V první vlně se ekonom Eugen von Böhn-Bawer zaměřil na analýzu kapitálu s kritikou učení Karla Marxe, jenž v rakouské škole přetrvává do dnes. V druhé vlně se ekonomové Ludwig von Mises a Friedrich Hayek věnovali studiím, které přinesly ekonomické vyvrácení možnosti racionální kalkulace za socialismu, kdy označili roli cen jako nositele informace o vzácnosti a současně praktickou nemožnost nashromáždit všechny potřebné informace centrálním plánováním. Současně se věnovali i teorii peněz, jenž pokládali za tržní prostředek směny, který vznikne z komodit a teorii hospodářského cyklu, ve které upozornili na negativní sliv centrálního bankovnictví a výhodu svobodné soutěže na poli peněz. Vznikla tedy rakouská teorie hospodářského cyklu. Důraz, který se klade na nikým centrálně neřízené spontánní tržní prostředí je značně podobné Bitcoinu a celkově světu kryptoměn. Evropská centrální banka ve své zprávě o virtuálních měnách prohlásila, že teoretické základy Bitcoinu jdou nalézt v Rakouské ekonomické škole.[172]

Některé z děl jsou opravdu podobné hlavní myšlence Bitcoinu, například jedno z děl s názvem „Denacionalizace peněz“ v podstatě popisuje funkci, kterou Bitcoin zastává. Další dílo s názvem „Teorie peněz a úvěru“ je zakončeno slovy: *„Současný neuspokojivý stav peněžních záležitostí je výsledkem socialistické ideologie, jíž jsou naši současníci oddáni, a hospodářských politik, které tato ideologie zplodila. Lidé si stěžují na inflaci, ale zapáleně podporují politiku, která nemůže být prováděna bez inflace. A tak zatímco roní hořké slzy nad nevyhnutelnými dopady inflace, zatvrzele odporují jakémukoliv pokusu snížit vládní výdaje. Reforma měnového systému a návrat k tvrdým penězům předkládají radikální změnu v politické filosofii“*[173]

V myšlenkách děl rakouské školy se samozřejmě nepíše o P2P sítí, digitálních měnách či asymetrické kryptografii, vzhledem k tomu, že se jedná o novodobou technologii. Nutné je však zmínit, že i někteří mladší rakouští ekonomové tvrdí, že Bitcoin nepřežije. Důvodem

[172] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 120-121
[173] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 121

tomu je myšlenka návratu zlata v peněžním systému pro základ hodnoty peněz. Z toho také vznikají otázky, čím je Bitcoin krytý a dochází k častému srovnání se zlatem. Oboje, Bitcoin i zlato, má své zástupce v reálném světě a v ekonomické teorii. Argumenty ve prospěch zlata jsou založeny na faktu, že zlato je a bylo prostředkem směny po tisíce let a současně je jeho výhodou, že ho lidé znají a rozumí mu. Co však hovoří proti zlatu je potřeba centralizace. Doposud nikdo nepřišel s decentralizovaným systémem, ve kterém by svou roli hrálo zlato. Problém centralizace je, že je napadnutelná, zneužitelná a centrum je možné zničit. Bitcoin je však volatilní, jeho cena roste a klesá každý den v řádů procent, která se sice s růstem počtu uživatelů stabilizuje čím dál více, ale pokud je cena nestálá, odrazuje potenciální nové uživatele od vstupu a bez jejich vstupu se cena Bitcoinu nemůže stabilizovat. Zlato má cenu v čase daleko stálejší. [174]

Otázkou tedy zůstává, zda je Bitcoin skutečně penězi či nikoliv. Z právního hlediska lze Bitcoin označit jako peníze velmi snadno, jak již v minulosti bylo provedeno. Ekonomická otázka, zda se skutečně jedná o peníze je však podstatně složitější.[175]

[174] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 120-123
[175] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 120-123

3.8 Bitcoin jako měna

Pokud by Bitcoin měl fungovat jako platidlo, musel by splňovat určitá kritéria. Pro začátek odpadá potřeba centrální autority a síť je zajištěna proti útoku „dvojité útraty využitím blockchainu a vytvořením decentralizované sítě.[176]

Kvalitní měna by měla být dobře dělitelná. Hodnota jednoho bitcoinu, *„psáno s malým „b“ pokud mluvíme o měně v systému Bitcoin označenou zkratkou BTC,“*[177] je ve vztahu k americkému dolaru již příliš vysoká pro běžné užívání. Využívají se tedy hodnoty centibitcoinu (= 0,01 BTC), milibitcoinu (= 0,001 BTC), mikrobitcoinu (= 0,000001 BTC) a nejvyužívanější hodnota známá jako **satoshi** (= 0,00000001 BTC), pojmenovanou podle autora bitcoinové sítě Satoshiho Nakamota.[178]

Měnu je třeba snadno skladovat a jednoduše přenášet. Bitcoin má formu digitální informace a je tedy lehké ho uložit na pevný disk, flashdisk, vytisknout na obyčejný papír, nahrát do telefonu či jiné mobilní zařízení nebo nahrát na specializované servery třetích stran. Přenos Bitcoinu z jedné strany místnosti je stejně snadné jako z jedné strany zeměkoule a druhou, postačí pouze zadat pár pokynů na telefonu či jiném zařízení.[179]

Dalším kritérium je dobrá zaměnitelnost, kterou Bitcoin má. V případě, že si člověk vypůjčí 100 bitcoinů a „jiných“ 100 bitcoinů po čase vrátí, vše bude v pořádku.[180]

Posledním a současně nejkontroverznější vlastností kvalitních peněz je „vnitřní hodnota“. Je nutné nejprve vyvrátit ekonomický mýtus, že bitcoiny jsou „kryty“ elektřinou nebo energií nutnou k jejich vytěžení a podobné. „*Představa, že bez peněžní hodnoty Bitcoinu zůstane alespoň elektřina, která byla vytěžena, je absurdní. Čím jsou tedy bitcoiny kryté? Ničím. Jako u čehokoliv, co je předmětem směny, je i u peněz hodnota dána užitkem, který mu lidé připisují.“*[181] Bitcoin nemá tendenci se vracet na cenu samotné komodity bez peněžní funkce, záleží však na vzácnosti. Bitcoin tedy nemá žádnou „vnitřní hodnotu“ v podobě jiného užitku, nežli je jeho peněžní záměr stejně jako současné peníze. Na rozdíl od současných peněz je však Bitcoin omezený a zafixovaný na maximální hodnotu 21 milionů bitcoinů, úplně přesně 20.999.999,9769 BTC. Je tedy důležité, že Bitcoin má

[176] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 30-32
[177] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 36
[178] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 36
[179] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 37
[180] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 37
[181] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 38

omezené množství, čímž se zajišťuje jeho vzácnost. Neexistuje žádný způsob, jak vytvořit nové bitcoinu po dosažení maximální hodnoty 21 milionů.[182]

Proto, abych se bitcoiny staly penězi, musely by se dle ekonomických teorií stát všeobecně přijímaným prostředkem směny, současně tak být i nejlikvidnějším aktivem. Dále je třeba změna struktury koše zboží a služeb, ve kterých se bitcoiny platí. Porovnáme-li strukturu korunového a bitcoinového spotřebního koše, dostáváme úplně jinou strukturu zboží a služeb. V korunovém spotřebním koši je zhruba 40 % utraceno za náklady na bydlení, 35 % za potraviny a 20 % za energie z měsíčního rozpočtu průměrného Čecha. Bitcoin má k takovému rozpoložení spotřebního koše ještě daleko. V neposlední řadě by se měl Bitcoin zažít běžným lidem pro provádění ekonomických kalkulací. Jestliže víte, že určitý statek stojí 4 BTC a nebudete si muset zpětně přepočítávat, na kolik by statek vyšel například v českých korunách: Bude to tak dalším krokem kupředu pro Bitcoin jako všeobecně přijímaný prostředek směny.[183]

Argument hovořící proti Bitcoinu je omezenost množství. Jedná se o původní argument proti zlatému standardu, který říkal, že zlata je málo.[184]

Zlatý standard je pojem krytí papírových fiat peněz hodnotou zlata. Jedná se tedy o možnost směnit peníze (americký dolar) za dané množství zlata, která se v průběhu 20. století ukázala jako nefunkční z důvodu neschopnosti reagovat na ekonomické následky první světové války s příchodem hospodářské krize. Zlatý standard byl ukončen roku 1971 tehdejším americkým prezidentem R. Nixonem a došlo tak ke zrušení směnitelnosti dolaru za zlato.[185]

Argument o omezenosti množství nedává smysl. Ceny statků se množství zlata přizpůsobí. Bude se jednat stejnou situaci, jako v případě nafukování peněžní zásoby. Je-li peněz více, ceny rostou, pokud je peněz méně, ceny se sníží. V případě zlata se dnes většinou neobchoduje s fyzickou formou, ale pouze se poukázky na zlato. Hypotetická dělitelnost hodnoty je tedy nekonečná, stejně tak v případě Bitcoinu. Teoretickou nevýhodou omezeného množství může být vytvořené deflační prostředí. V tradičním měnovém prostředí banky vytváří více a více peněz, které vypouští do oběhu a tím způsobují inflaci.

[182] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 38-41
[183] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 123-125
[184] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 125-126
[185] KALINSKÝ, B. *Bitcoin a ti druzí.* 2018, s. 7

Tato možnost je u Bitcoinu nemožná. Zásoba bitcoinů je stálá, či dokonce mírně klesající, vezmeme-li v úvahu potencionální ztráty bitcoinů jednotlivými uživateli. Bitcoiny mohou zůstat na zkolabovaných počítačích bez zálohy, ztracených hardwarových zařízeních či zapomenutím hesla. V případě, že poptávka po bitcoinech nebude klesat, jenž se nepředpokládá, cena by tedy měla mírně růst. Pokud se měna zhodnocuje, roste tedy její cena a musí v této závislosti klesat cena všeho ostatního, dochází tak k cenové deflaci. Potencionálním nebezpečím je vznik deflační spirály. Jedná se o modelovou situaci, ve které lidé očekávají růst hodnoty peněz a rozhodnou se peníze spořit, čímž se opět zvedne hodnota peněz, a to následně vede k dalšímu spoření. V případě, že peníze nejsou vnášeny opět do oběhu, podniky přichází o zakázky a jsou nuceny propouštět, což opětovně snižuje koupěschopnou poptávku lidi a vznikající krize se nadále prohlubuje. Tato opodstatnění mají svůj racionální základ. V současnosti by umělé zhodnocování tradičních peněz mohlo vést k ekonomickým problémům. Peníze jsou tvořeny skrze komerční banky v moment, kdy vypůjčí peníze. Nově vytvořené peníze svému klientovi připíší na účet, čímž se nové peníze dostanou do oběhu. Centrální banka tok peněz koriguje nastavením svých úrokových sazeb. Deflace je však přirozeným jevem tržní ekonomiky. Snížení ceny v důsledku konkurenčního boje je pozitivním jevem, nikoliv negativním. Západní svět většinu svých dějin prožil v deflačním prostředí komoditního standardu a velkými hospodářskými problémy si prošel hlavně kvůli znehodnocování peněz. Spoření bitcoinů v důsledku poklesu cen by nemohl vést k nekonečné spirále z důvodu, že do problému vstupují i protichůdné motivace. V případě hromadění bitcoinů bez jejich využívání ke směně by se zvyšovala relativní hodnota jiného prostředku směny, což by zapříčinilo snížení hodnoty bitcoinu. Systém má tak sobě přirozenou regulaci. Fakt, že Bitcoin v porovnání se současnými penězi motivuje lidi ke spoření reflektuje lidskou přirozenost.[186] *„ Vyšší úspory financují investice a umožňují nám žít rok co rok kvalitnější životy. “*[187]

[186] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 123-129
[187] STROUKAL, D.; SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti.* 2021, s. 127

Na základě již získaných informací lze říci, že Bitcoin se nejeví jako ideální volbou pro každodenní využití jako platidlo pro miliardy lidí, i když je toho do jisté části schopný. Jeho největším potenciálem je tak stále vlastnost uschovatele hodnoty. Mohl by tak být ideální kombinací mezi digitálním zlatem a digitální měnou. V tomto je ovšem problém jeho volatilita, která se postupem času zlepšuje. Nicméně, jestli Bitcoinu bude pokračovat v růstu, přiláká více zájemců, což opět podpoří jeho růst a bude tak snižovat svou volatilitu. V momentu, co se růst Bitcoinu zpomalí a jeho cena se ustálí, nebude již lákat investory vyhledávající velké riziko s vysokým zhodnocením a stane se z něj aktivum, které se bude pomalu zhodnocovat, v řádu procent, každý rok.[188]

Nicméně poprvé v historii lidstva existuje komodita, jejíž nabídka je striktně limitovaná. Nezáleží na tom, kolik lidí bude bitcoinovou síť užívat, jakou hodnotu bude bitcoin mít, jak technologicky vyspělé těžební stroje budou použity pro jeho těžbu, vždy bude pouze 21 milionů bitcoinů.[189]

[188] AMMOUS, S. *The Bitcoin Standard.* 2018, s. 183-190
[189] AMMOUS, S. *The Bitcoin Standard.* 2018, s. 197-198

3.9 Potencionální rizika, problémy a mýty Bitcoinu

Bitcoinová síť je vytvořena a zajištěna za pomocí propracovaných výpočtů, díky kterým se stává síť potencionálním útočníkem v podstatě nenapadnutelná.[190]
V klasickém bankovním systému je jeden z hlavních důvodů existence bank důvěra, že banka uložené finance ochrání. Banky proto potřebují velké centrály, mnoho poboček, zabezpečenou a zálohovanou počítačovou infrastrukturu a v neposlední řadě lidi, kteří se o vše budou starat. V případně odcizení využívají pomoc od státu, který má své úředníky, justici a policii. Bitcoin má tento systém zjednodušený na síť počítačů, na kterých běží program a které spolu zároveň komunikují, přičemž komunikace probíhá i s peněženkami a těžaři. Systém je navržen tak, aby nedůvěřoval nikomu. Z tohoto důvodu všichni kontroluji všechny transakce a bloky podle jednotlivých pravidel. Současně se odměňována poctivá práce neboli správný zápis transakcí do bloku. Tedy místo dohledu, zákonů, soudů a smluv jsou využita pravidla kryptografie a teorie her.[191]

Teorie her je soubor oborů, jako je matematika, ekonomie, sociologie a psychologie, která analyzuje proces rozhodování, tedy chování jednotlivých subjektů v okamžik střetu zájmů. Za pomocí matematických výpočtů se snaží nalézt co nejvýhodnější strategii pro jednotlivý subjekt v tomto procesu.[192]

V práci již byl vysvětlen způsob eliminace základního problému dvojité útraty. Nyní je třeba vysvětlit specifičtěji tři konkrétní možnosti dvojitých útrat, jaké rizika přinášejí, jak je možno se proti nim bránit a jaké závěry z toho vyplývají.[193]

Race attack je první možností, která lze využívat pouze v případě, že prodejce přijímá transakce na základě ověření transakce a již nečeká na potvrzení zápisu do bloku. Jedná se například a prodej v obchodě, kde se platí menšími částkami a není z hlediska praktičnosti nechat kupujícího čekat několik minut do doby, kdy bude transakce zapsána do bloku. Útočník v tomto případě může zneužít vyskytlé situace a zaslat jednu transakci na peněženku obchodu a druhou transakci se stejným vstupem na nějakou vlastní adresu do sítě. Zařízení oběti vydá potvrzení útočníkovi transakce, načež se za několik minut do blockchainu zapíše transakce poslána do sítě a satoshi zůstanou majetkem útočníka. Obrana

[190] NAKAMOTO, S. *Bitcoin Whitepaper: A Peer-to-Peer Electronic Cash System.* 2008, s. 8-10
[191] KALINSKÝ, B. *Bitcoin a ti druzí.* 2018, s. 44
[192] Teorie grafů. *Teorie her* [online]. Dostupné z: https://teorie-grafu.cz/vybrane-problemy/teorie-her.php
[193] KALINSKÝ, B. *Bitcoin a ti druzí.* 2018, s. 44

je možná v případě, že obchodník má svůj terminál zabezpečený proti posílání přímých transakcí a přijímá jen transakce ze sítě od důvěryhodných uzlů.[194]

Útok alternativní historií je další možností, jak by bylo možné utratit bitcoiny z jedné adresy vícekrát, které spočívá na nutnosti zapsat transakce do blockchainu. V případě, že útočník chce utratit bitcoin dvakrát a chce je zapsat do blockchainu, je pro něj nutné také najít nonce a dodat síti block se správným hashem.[195]

Útočník pošle jednu transakci do sítě, například do kryptoměnové burzy, a zároveň začne těžit blok, ve kterém by byla transakce odeslána na jím vlastněnou adresu. Pokouší se tímto o fork, tedy o rozštěpení blockchainu. Následně se tedy snaží tajně a úspěšně vytěžit několik bloků po sobě. V poctivé síti doposud jeho transakce obdržela dostatečné množství potvrzení a burza odešle útočníkovi zakoupené bitcoiny. V tento moment útočník pošle do sítě své bloky, ve kterých je transakce poslána na jeho adresu. Musí být s nalezením bloků dostatečně úspěšný tak, aby sít uznala jeho verzi blockchainu za platnou. [196] Zkrácený příklad situace by obsahoval čtyři kroky:

1. odeslání bitcoinů na burzu;
2. směna bitcoinů za dolary a následný výběr USD;
3. následné rozeslání řetězu, který neobsahuje informaci a převodu bitcoinů na burzu;
4. přepsáni historie, díky které útočník stále vlastní původní bitcoiny a současně i dolary, které by vybral z burzy.[197]

V praxi se však jedná o extrémně neefektivní techniku vzhledem k tomu, že transakci lze považovat za potvrzenou v momentu, co obdrží 6 potvrzení. Z toho vyplývá, že k bloku s transakcí by bylo nutné připojit 5 dalších bloků. Kdyby útočník potencionálně disponoval například 4 % celkového výkonu sítě, což by vyžadovalo investice astronomických částek do zařízení a energie, existuje stále poměrně malá šance, že dokáže vytěžit dost bloků a předstihl tak zbytek sítě. Poté má 8 % šanci na první potvrzení, ale už jen 0,002 % na páté potvrzení a v podstatě nulovou šanci na potvrzení šesté. To v reálném světě znamená, že by jen pálil vynaloženou energii bez jakéhokoliv úspěchu, přičemž by mohl vynaložit svou výpočetní sílu a energii na poctivou těžbu, kde by měl garantované zisky.[198]

---

[194] KALINSKÝ, B. *Bitcoin a ti druzí.* 2018, s. 44
[195] KALINSKÝ, B. *Bitcoin a ti druzí.* 2018, s. 44-45
[196] KALINSKÝ, B. *Bitcoin a ti druzí.* 2018, s. 44-45
[197] PRITZKER, Y. *Vynález jménem Bitcoin.* 2019, s. 69
[198] KALINSKÝ, B. *Bitcoin a ti druzí.* 2018, s. 44-45

Útok 51 % je třetí možností rizika. Jedná se o útok, při kterém by útočník musel ovládat 51 % a více výkonu těžby celé sítě. V moment, co by útočník získal více než 51 % těžebního výkonu, roste tím možnost, že by těžit bloky rychleji, nežli by byli schopni těžit ostatní těžaři, možnost blokování transakcí, realizování dvojité útraty a zničení důvěry systému.[199] Útoční by tedy získal moc na zapisováním do „účetní knihy Bitcoinu". Uzly totiž mají povinnost přijmout řetězec s nejtěžším celkovým důkazem o provedené práci a útoční by měl možnost vytvořit ten nejtěžší řetězec. Následující kroky útoku by tedy vypadaly takto:

1. síť by těžila bloky rychlostí 1000 hashů za vteřinu;
2. útoční by nakoupil dostatek těžebního hardwaru a elektřiny, aby mohl vytvořit 2000 hashů za vteřinu;
3. útočník začne vytvářet řetězec dle svých pravidel;
4. řetězec bloků rozešle, a protože těží dvakrát rychleji než ostatní těžaři, řetězec bude obsahovat dvakrát větší množství celkových důkazů o vykonané práci a ostatní uzly ho tak budou muset přijmout.[200]

Z praktického hlediska by byl tento útok extrémně náročné zrealizovat. Lokalizování výpočetní síly by muselo proběhnout v utajení tak, aby se o tom nedozvěděl zbytek sítě. Útočník by musel začít těžit proti druhé části sítě, což by u 51 % výkonu trvalo přibližně 17 hodin. [201] Dalším faktem je, že spotřeba energie Bitcoinu dnes odpovídá jedné středně velké zemi a použít takto velký výkon na útok sítě by bylo extrémně nákladné. Vynaložit takto vysoké náklady za ceny energií, nákup potřebného hardwaru a vše utajit, aby se o tom nedozvěděl zbytek sítě, je prakticky nemožné. [202]

Co však chrání Bitcoin před všemi různými útoky je princip navržení celé bitcoinové sítě, kdy celý zápis transakcí je dostupný všem, kteří mají připojení k internetu po celém světě. Jakékoliv podvodné aktivity jsou tak ihned zaznamenány a jsou asi tak efektivní, jako plýtvání vlastněných zdrojů na prázdno. Bitcoin tedy spoléhá na prostředí, ve kterém jsou

[199] KALINSKÝ, B. *Bitcoin a ti druzí.* 2018, s. 45
[200] PRITZKER, Y. *Vynález jménem Bitcoin.* 2019, s. 68-69
[201] KALINSKÝ, B. *Bitcoin a ti druzí.* 2018, s. 45
[202] PRITZKER, Y. *Vynález jménem Bitcoin.* 2019, s. 68-70

pokusy o podvod daleko dražší, nežli by bylo poctivé získávání odměny za řádné užívání sítě.[203]

Na závěr této tématiky je nutné konstatovat fakt, že samotný Bitcoin jako protokol či peer-to-peer měna fungoval od počátku svého spuštění až do současné doby prakticky bez jakékoliv chyby či problému v otázce bezpečnosti.[204]

[203] AMMOUS, S. *The Bitcoin Standard.* 2018, s. 174-175
[204] AMMOUS, S. *The Bitcoin Standard.* 2018, s. 167

4 Vlastní práce

4.1 Aktuální situace na trhu

Bitcoin se v současně době pohybuje kolem hranice 20.000 USD/BTC, přesněji tedy ke dni 12.3.2023 v kurzu 20.600 USD/BTC. Od začátku roku, kdy se cena pohybovala okolo 16.700 USD/BTC Bitcoin vystoupal až k hranicím ceny 25.000 USD/BTC. Nicméně od této doby se propadl až k cenám okolo 20.000 USD/BTC. Jednalo se tak o přirozený vývoj ceny. Vývoj je zachycen v grafu 3.

Graf 3 Vývoj ceny Bitcoinu v roce 2023

Zdroj: CoinMarketCap. *Bitcoin* [online]. Dostupné z: https://coinmarketcap.com/currencies/bitcoin/

Od svého ATH, tedy svého historického maxima, kdy částka přesáhla v listopadu roku 2021 hranici 69.000 USD/BTC, Bitcoin odepsal 70 % své hodnoty. [205] Od prudkého nárůstu ceny v září roku 2020, kdy započal rychlý nárůst ceny začínající na hodnotě 10.500 USD/BTC, kde se cena pohybovala cena Bitcoinu po Covidové krizi, se Bitcoin dostal v dubnu roku 2021 přes hranici 63.000 USD/BTC. Bitcoinu tak na dosažení této cenovky

[205] CoinGecko. *Ceny kryptoměny od historického maxima (ATH)* [online]. Dostupné z: https://www.coingecko.com/cs/watchlists/all-time-high-crypto

stačilo pouze 7 měsíců. Za nento časový úsek byl Bitcoin schopen zhodnocení o šesti násobek své původní hodnoty.

Tento růst odstartoval zejména vstup institucionální investorů na trh s Bitcoinem. Nejdříve začala společnost MicroStrategy v čele svým výkonným předsedou Michaelem Saylorem [206] silně navyšovat svou expozici do Bitcoinu [207]. Společnost MicroStrategy následovala společnost Tesla, která nejdříve začala Bitcoin přijímat jako formu úhrady za své elektrické automobily a následně se rozhodla do něj sama investovat.[208] Další velkou pozitivní novinkou bylo rozhodnutí státu El Salvador přijmul Bitcoin za svou oficiální měnu.[209] Růst ceny Bitcoinu také podpořil nárůst peněžní zásoby USD v vnesený do oběhu ekonomiky Spojených států amerických. Vypouštění většího množství peněžní zásoby do oběhu byla reakce na pandemickou krizi a taktika, jak zabránit ekonomické krizi.[210]

Následně nastal pád ceny, kdy je Bitcoin dostal v červenci roku 2021 těsně nad hranici 31.000 USD/BTC. Došlo k ochlazení trhu, který byl způsobil zejména FUD z Číny, jejíž vláda se rozhlodla zakázat těžbu, trading, obchodování s Bitcoinem a současně také jakékoliv zaměstnání vztahující se k Bitcoinu a kryptoměnám. [211]

Po ustálení trhu nastal opětovný růst ceny, který se za pouhý měsíc zastavil těsně pod hranicí 50.000 USD/BTC, následovaný propadem k hranicím ceny 42.000 USD/BTC a opětovný nárůstem na nové ATH, tedy úroveň převyšující hodnotu 69.000 USD/BTC. Na tuto hodnotu cena vystoupala zejména v reakci na pozitivní zprávu o rozhodnutí americké Komise pro cenné papíry, která schválila spuštění prvního amerického veřejně

---

[206] Michael. *Michael J. Saylor* [online]. Dostupné z: https://www.michael.com/
[207] Kurzy.cz. *Institucionální investoři nezpomalují s nákupy Bitcoinu, kolik ho vlastní?* [online]. Dostupné z: https://www.kurzy.cz/zpravy/607834-institucionalni-investori-nezpomaluji-s-nakupy-bitcoinu-kolik-ho-vlastni/
[208] BBC. *Elon Musk's Tesla sells most of its Bitcoin holding* [online]. Dostupné z: https://www.bbc.com/news/business-62246367
[209] Business Today. *One year since El Salvador announced Bitcoin adoption plans! Shat's te latest?* [online]. Dostupné z: https://www.businesstoday.in/crypto/story/one-year-since-el-salvador-announced-bitcoin-adoption-plans-whats-the-latest-336443-2022-06-06
[210] USA Today [online]. Dostupné z: https://eu.usatoday.com/in-depth/money/2020/05/12/coronavirushow-u-s-printing-dollars-save-economy-during-crisis-fed/3038117001/
[211] Worldcoin. *All you need to know about China's crypto ban* [online]. Dostupné z: https://worldcoin.org/articles/china-crypto-ban

obchodovaného fondu ETF vázaného na Bitcoin.[212] Toto ETF zhřizovala společnosti ProShares s označením BITO.[213]

Následoval však pozvolný propad k cenám mezi 40.000 USD/BTC a 50.000 USD/BTC. Jednalo se zejména o přirozené ochlazení trhu po předešlých rychlých cenových růstech a novém ATM, současně mnoho investorů odprodávalo své bitcoiny a tím vybírali své zisky. Mezi touto úrovní Bitcoin cca 4 měsíce osciloval a nastal další pád ceny, nejdříve na hranici 30.000 USD/BTC a následně k bodu 20.000 USD/BTC. Okolo tohoto bodového cenu Bitcoin pokračuje oscilovat již od června roku 2022. Cenový vývoj je zobrazen v grafu 4. Nejdříve se Bitcoin cenově v tomto období dostal až k hranici 15.000 BTC/USD.

Graf 4 Vývoj ceny Bitcoinu

Zdroj: CoinMarketCap. *Bitcoin* [online]. Dostupné z: https://coinmarketcap.com/currencies/bitcoin/

Velký propad ceny způsobil zejména obecně nepříznivý vývoj trhu. Přicházející ekonomická a energetická krize, která byla zapříčiněná dohrou pandemické krize a válkou

[212] Živě. *Bitcoin na rekordní ceně. K novému ATH jej vyhnalo klíčové rozhodnutí americké Komise pro cenné papíry* [online]. Dostupné z: https://www.zive.cz/clanky/bitcoin-na-rekordni-cene-k-novemu-ath-jej-vyhnalo-klicove-rozhodnuti-americke-komise-pro-cenne-papiry/sc-3-a-212946/default.aspx

[213] ProShares. *BITO Bitcoin Strategy ETF* [online]. Dostupné z: https://www.proshares.com/our-etfs/strategic/bito

na Ukrajině způsobenou Ruskou agresí [214], způsobila nejen propad ceny Bitcoinu, ale negativně ovlivnila i ostatní trhy. Například celý akciový trh.[215]

Jindy stabilní ETF akciového trhu, s pěti sty největšími společnostmi amerického trhu, index S&P 500 se propadl od začátku roku 2022 již 17,25 %, jak je znázorněno v grafu 5.[216]

Graf 5 Vývoj ceny indexu S&P 500

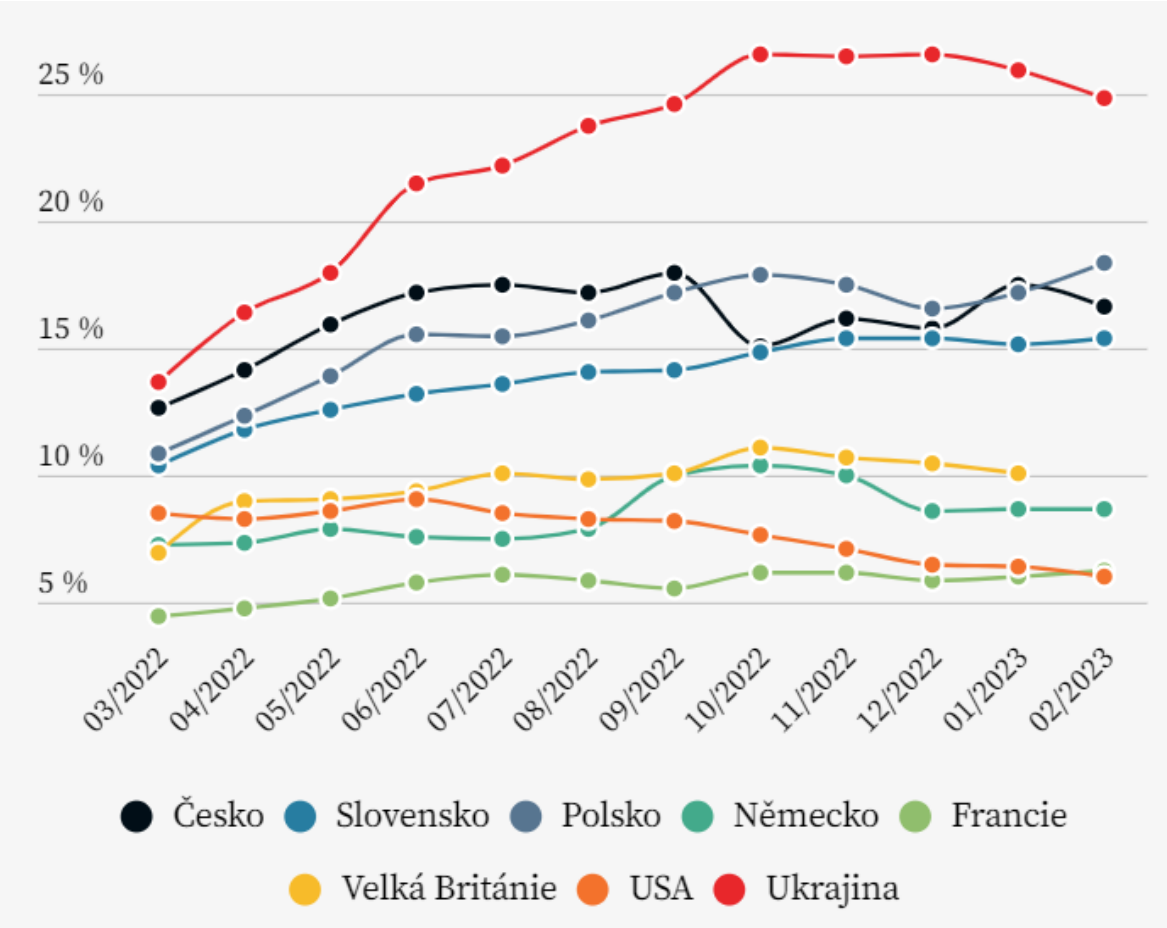
Zdroj: Finex. *S&P500* [online]. Dostupné z: https://finex.cz/index/standard-and-poors-500/

Bitcoin je však oproti indexu akciového trhu daleko více volatilní. Současná situace jasně ukázala, že Bitcoin ještě není tzv. pákou proti inflaci. Na tuto skutečnost je Bitcoin stále příliš volatilní. Vzhledem k tomu, že světovou ekonomiku v roce 2023 postihl problém vysoké inflace, která byla způsobena zejména negativním vývojem světové ekonomiky.

Inflace v lednu roku 2023 v USA pohybovala kolem 6,4 %, v Německu 8,7 % a v České republice 17,5 %. Vývoj je zachycen v grafu 6.[217]

[214] iDnes. *Zlato kvůli válce na Ukrajině značně posiluje. Kryptoměny začínají krvácet* [online]. Dostupné z: https://www.idnes.cz/ekonomika/zahranicni/zlato-bitcoin-investice-riziko-pokles-cena-ukrajina.A220224_094020 _eko-zahranicni_jla
[215] e15. *Mapa inflace* [online]. Dostupné z: https://www.e15.cz/inflace-v-cr-a-ve-svete-ceny-graf
[216] Finex. *Akciový index S&P500* [online]. Dostupné z: https://finex.cz/index/standard-and-poors-500/
[217] e15. *Mapa inflace* [online]. Dostupné z: https://www.e15.cz/inflace-v-cr-a-ve-svete-ceny-graf

Graf 6 Vývoj inflace v Česku a dalších vybraných státech



Zdroj: e15. *Inflace* [online]. Dostupné z: https://www.e15.cz/inflace-v-cr-a-ve-svete-ceny-graf

Samotný kryptoměnový trh zasáhl několik negativní okamžiků, které výrazně srazily ceny Bitcoin směrem dolů. Koncem roku 2022 vyhlásily bankrot 3 velkých společnosti, které byly přímo spojeny s Bitcoinovým a kryptoměnovým trhem. První společností, kterou postihl tento osud, byla v září roku 2022 společnost Celsius Network, která fungovala na způsob virtuální banky či krypto banky Na účet bylo možné vložit vlastněné kryptoměny, za které byl poskytnut úrok v řádu několika procent. U Bitcoinu se jednalo o úročení okolo 10 % p. a. Současně bylo možné si po zástavě Bitcoinu či jiných kryptoměn vypůjčit finanční prostředky. Zastavené finanční prostředky složily jako zástavní kolaterál. Nicméně se s propadem ceny Bitcoinu dostala společnost do finančních problémů. V červnu roku 2022 zastavila uživatelům možnost výběru vložených bitcoinů. Firma má v současné době závazky vůči uživatelům 4,72 mld. CZK a není jisté kdy a zda vůbec bude schopna

uživatelům uložené bitcoiny a jiné kryptoměny vrátit, minimálně tomu budou předcházet dlouhé soudní řízení.[218]

Stejný osud postihl i společnost BlockFi, která byla v podstatě pouze větší kryptoměnovou bankou, než byla společnost Celsius Network, fungovala však na stejný způsob. Krach BlockFi měl nicméně daleko větší dopad, vzhledem k tomu, že nevyplacené kryptoměny uživatelů se odhadují v hodnotě až 10 mld. USD.[219]

Největší zprávou s největším rozsahem škod byla novinka ohledně krachu 3. největší kryptoměnové burzy FTX. Po vyhlášení krachu burze chybělo okolo 9,4 mld USD, na vyplacení uložených finanční prostředků uživatelů burzy. Tito uživatele tak své finanční prostředky s velkou pravděpodobností již nikdy nezískají zpět. Po dalším průzkumu došlo k zjištění, že krab burzy nezpůsobila jen nepříznivá situace trhu či špatné vedení společnosti, ale hlavně nezákonné zacházení s finančními prostředky uživatelů. CEO burzy FTX je v současné době souzen a hrozí mu desítky let ve vězení. Tato informace samozřejmě přinesla soustu negativní pozornosti na celý kryptoměnový trh, i když na burze byly obchodovaný v daleko větším objemu altcoiny, nežli samotný Bitcoin. Následně se do ohrožení dostaly další velké burzy jako Kraken, Crypto.com a další burzy či společnosti spojené s Bitcoinem. Společnosti musely ujišťovat své klienty, že jejich vložené prostředky jsou zabezpečené a nedojde k jejich ztrátě. Všechny tyto negativní zprávy způsobily prodat Bitcoinu až k úrovni ceny 15.000 USD/BTC.[220] [221]

Veškeré tyto skutečnosti tak výrazným způsobem upozornily na propagované moto Bitcoinové komunity: „Not your keys, not your coins“, tedy NYKNYC. Jedná se o velmi důležité rozhodnutí, jak a kam budou bitcoiny uloženy a zda k nim bude mít uživatel stále své primární klíče. V momentu, co soukromý klíč od svých bitcoinů majitel propůjčí někomu jinému, již nemá nad svými prostředky plnou kontrolu. Tuto skutečnost si musí Bitcoinový investoři uvědomit a vždy nést v paměti.

---

[218] e15. *Hořký konec kryptobanky. Uvízly v ní tisíce Čechů, ukazují dokumenty* [online]. Dostupné z: https://www.e15.cz/kryptomeny/horky-konec-kryptobanky-uvizly-v-ni-tisice-cechu-ukazuji-dokumenty-1394177

[219] e15.*Další oběť pádu burzy FTX. Půjčovna kryptoměn BlockFi vyhlásila bankrot* [online]. Dostupné z: https://www.e15.cz/kryptomeny/dalsi-obet-padu-burzy-ftx-pujcovna-kryptomen-blockfi-vyhlasila-bankrot-1395177

[220] e15. *Pád kryptoburzy. Po krachu FTX se smráká i nad Crypto.com a BlockFi* [online]. Dostupné z: https://www.e15.cz/kryptomeny/pad-kryptoburz-po-krachu-ftx-se-smraka-i-nad-crypto-com-a-blockfi-1394927

[221] e15. *Kryptoměnová burza FTX přišla o licenci pro působení v EU, v USA vyhlásila bankrot* [online]. Dostupné z: https://www.e15.cz/kryptomeny/kryptomenova-burza-ftx-prisla-o-licenci-pro-pusobeni-v-eu-v-usa-vyhlasila-bankrot-1394819

V případě tržní kapitalizace se jedná o obdobný případ jako samotná cena Bitcoinu, vzhledem k tomu, že tržní kapitalizace Bitcoinu se počítá vynásobením aktuálním množstvím vytěžených bitcoinů a aktuální cenou za jeden BTC. V moment pádu ceny Bitcoinu se z trhu v podstatě se odlívají finanční prostředky. To způsobí pád ceny a pokles celkové tržní kapitalizace Bitcoinu.

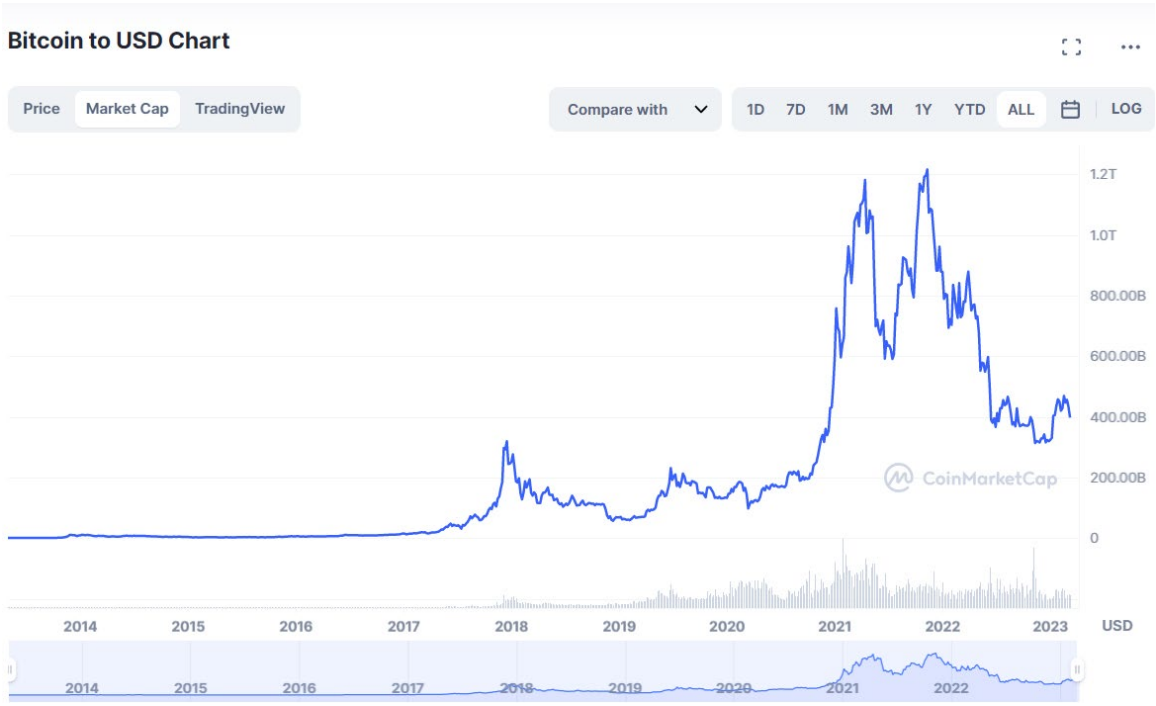
Tržní kapitalizace se pohybovala na začátku roku 2023 kolem 318 mld. USD, s denním objemem tržeb okolo 10 mld. USD. V půlce ledna roku 2023 došlo k posílení tržní kapitalizace až nad bod 400 mld. USD s výraznějším denním objemem pres 40 mld. USD. Vysoký růst ceny, který je podpořen vysokým denním objemem zrealizovaných transakcí bývá pozitivní indikátorem, že trh se rozhodl podpořit růst ceny a nebude se jednat pouze o výstřel ceny s následným poklesem. Pozvolným tempem rostla tržní kapitalizace až k hranicím 450 mld. USD. Po překonání této hranice následoval propad celkové tržní kapitalizace až k hodnotám 414 mld. USD. Následně se tržní kapitalizace dostala koncem února roku 2023 přes hranici 480 mld. USD. Tento bod byl lokálním maximem dosavadního roku 2023 a následoval propad k hranici 380 mld. USD. V současné době se tržní kapitalizace pohybuje okolo bodu 400 mld. USD s denním objemem tržeb oscilující kolem hodnoty 40 mld. USD. Vývoj tržní kapitalizace v neukončeném roce 2023 je zachycen v grafu 7.

V bodě své nejvyšší tržní kapitalizace přesahoval celý trh Bitcoinu hodnotu 1,27 bil. USD. Na této hodnotě se ocitl v září roku 2021. Se začínajícím „bull runem“ v září roku 2021, kdy se tržní kapitalizace pohybovala pod hranicí 200 mld. USD, bylo do Bitcoinu zainvestováno přes 1 bil. USD za pouhý rok. Doposud nejvyšší denní objem tržeb atakoval hranici 100 mld. USD při tržní kapitalizaci necelých 1 bil. USD. Vývoj tržní kapitalizace je zachycen v následujícím grafu 8. Růsty a propady tržní kapitalizace byly zapříčiněny stejnými či obdobnými důvody jako růst a propad ceny Bitcoinu. Tyto důvodu byly v této kapitolo již popsány.

Graf 7 Vývoj tržní kapitalizace Bitcoinu v roce 2023

Zdroj: CoinMarketCap. *Bitcoin* [online]. Dostupné z: https://coinmarketcap.com/currencies/bitcoin/

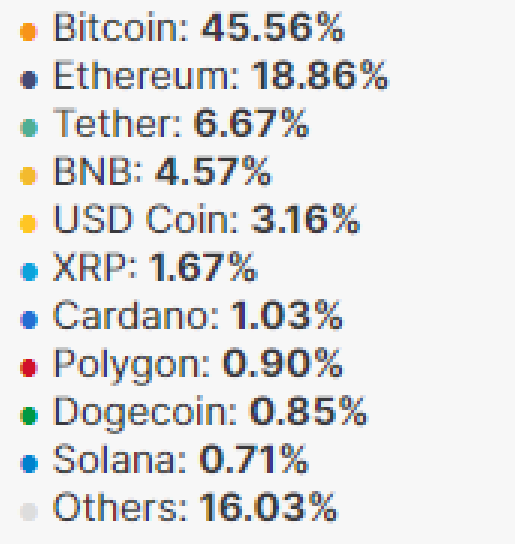
Graf 8 Vývoj tržní kapitalizace Bitcoinu



Zdroj: CoinMarketCap. *Bitcoin* [online]. Dostupné z: https://coinmarketcap.com/currencies/bitcoin/

V současné době je v oběhu, vytěženo přes 19.300.000 bitcoinů z 21.000.000 bitcoinů možných. [222] Současná odměna za vytěžený blok je 6,25 BTC a následný halving nastane přesně 29. dubna 2024 v 14:23:47.[223] Bitcoin zaujímá přes 45 % celkové tržní kapitalizace kryptoměnového trhu. Procentuální rozložení kryptoměnového trhu je zobrazeno v obrázku 5.

Obrázek 5 Poměr tržní kapitalizace kryptoměnového trhu

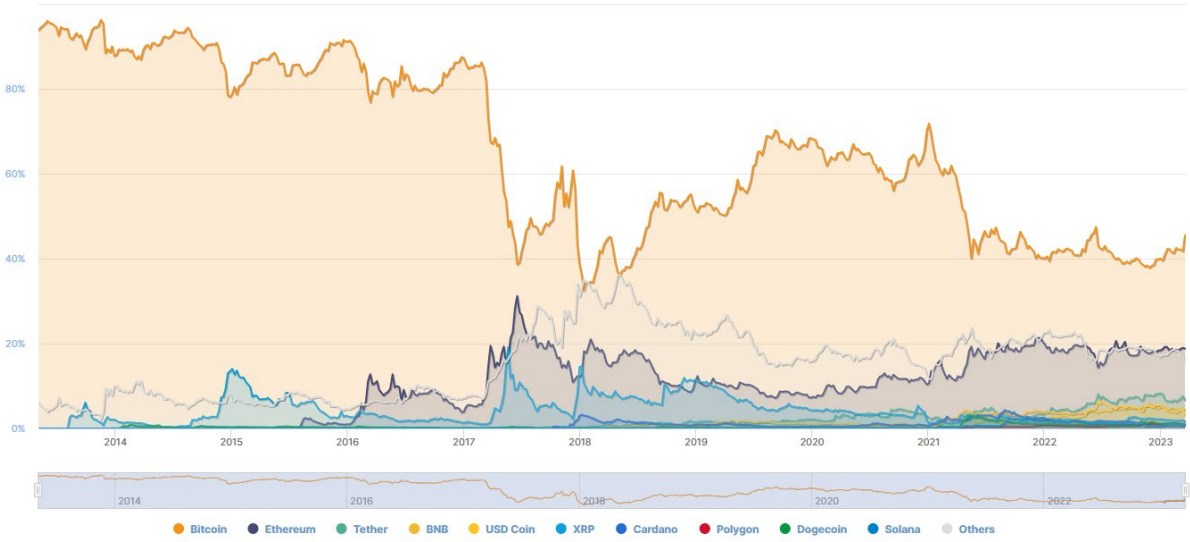


Zdroj: CoinMarketCap. [online]. Dostupné z: https://coinmarketcap.com/charts/

Bitcoin dominance kryptoměnového trhu se pohybovala od roku 2014 do roku 2017 okolo 90 %, s nejnižším bodem 78 % a nejvyšším bodem 96 %. Začátkem roku 2017 se jeho dominance propadla až k pouhým 32 %, což byla nejnižší hodnota od počátku Bitcoinu. Od této doby se Bitcoin dostal nejvýše na 71 % dominanci a v současné době je nad hranicí 45 % zastoupení kryptoměnového trhu. Vývoj dominance Bitcoinu na kryptoměnovém trhu je zachycen v grafu 9.

[222] CoinMarketCap. *Bitcoin* [online]. Dostupné z: https://coinmarketcap.com/currencies/bitcoin/
[223] Bitcoin Block Half. *Bitcoin Block Reward Halving Countdown* [online]. Dostupné z: https://www.bitcoinblockhalf.com/

Graf 9 Vývoj dominance Bitcoinu na kryptoměnovém trhu



Zdroj: CoinMarketCap. [online]. Dostupné z: https://coinmarketcap.com/charts/

Bitcoin tak prokázal svou vysokou volatilitu. Cena snadno reaguje rychlým růstem ceny na pozitivní zprávy, ale ještě rychleji propadem až o desítky procent v krátkém časovém úseku v reakci na FUD a jiné negativní zprávy. Investora tak dokáže vývoj ceny při nově zveřejné zprávě snadno zaskočit a nastává fáze, ve které spousta méně zkušených investorů začně reagovat na základě emocí a začíná prodávat ve ztrátě, či nakupovat pod vlivem FOMO.

Obdobným způsobem jako cena BTC se vyvíjí i jeho tržní kapitalizace. Jeho dominance na kryptoměnovém trhu stále ještě není na hodnotách, kterých se dříve nacházela, nicméně pozvolně roste.

4.2 Nákup Bitcoinu

V dnešní době existuje mnoho míst, kde je možné Bitcoin zakoupit či směnit. Bitcoiny je možné pořídit přímým způsobem prostřednictvím bitcoinových burz, směnáren, P2P portálů, kryptoměnových bankomatů [224] či nepřímým způsobem například přes aplikace PayPal, Revolut či prostřednictvím různých brokerů, kteří nabízejí bitcoinové deriváty.[225]

Rozdíl mezi přímým a nepřímým způsobem nákupu je v samotném vlastnictví Bitcoinu. V případě přímého nákupu získáte od Bitcoinu veřejný i soukromý klíč a Bitcoin je tak plně ve vašem vlastnictví. Na rozdíl od nepřímého nákupu, kdy od Bitcoinu nevlastníte soukromé klíče, které tak zůstávají v držení prodávajícího a není možné tak bitcoiny přesouvat. Jedná se o jednodušší variantu nákupu nicméně bitcoiny jsou v podstatě pronajímané. Tento přístup tak jde i proti principu decentralizace a porušuje bitcoinové heslo „Not your keys, not your coins“. Tato varianta je tak vhodná spíše pro méně technicky zdatného investora za podstoupení rizika nevlastnění soukromého klíče. Jednoznačně preferovaná varianta je tak varianta přímého nákupu, se kterou se v této práci bude pokračovat. Existují však různé druhy a typy nákupních prostředích, které jsou vysvětleny a zanalyzovány v následujících podkapitolách.[226]

Velkou výhodou investice do Bitcoinu je to, že existuje možnost ho nejen zakoupit online odkudkoliv, ale je možné ho, na rozdíl od akciového trhu, zakoupit 24 hodin denně, 7 dní v týdnu.[227]

Bitcoin je v této práci považován za dlouhodobou investici s předpokládanou dobou držení minimálně 5 let. Z tohoto důvodu se práce nezabývá tradingem.

---

[224] Kurzy. *Burzy a směnárny kryptoměn* [online]. Dostupné z: https://www.kurzy.cz/kryptomeny/burzy-smenarny

[225] e15. *Kryptoměny* [online]. Dostupné z: https://www.e15.cz/bitcoin-wiki?fbclid=IwAR25qrgD3BD293H1nVis4MfxVxpV6U6tHDSAQTWLxh1klK0xzyZqRyX06UM#penezenka_btc

[226] e15. *Kryptoměny* [online]. Dostupné z: https://www.e15.cz/bitcoin-wiki?fbclid=IwAR25qrgD3BD293H1nVis4MfxVxpV6U6tHDSAQTWLxh1klK0xzyZqRyX06UM#penezenka_btc

[227] Kurzy. *Burzy a směnárny kryptoměn* [online]. Dostupné z: https://www.kurzy.cz/kryptomeny/burzy-smenarny

4.2.1 Nákupní prostředí

Centralizované burzy

Nákup prostřednictví burzy se dnes řadí k nejběžnějšímu nákupnímu prostředí, využívané investory do Bitcoinu. Existují proto desítky kryptoměnových burz, které se od sebe odlišují svou velikostí, uživatelskou přívětivostí, nabízenými produkty, směnným kurzem a dalšími poplatky. Je proto důležité vybrat důvěryhodnou burzu, která současně nabízí nejlepší podmínky. Již se několikrát v minulosti stalo, že kryptoměnová burza zkrachovala a uživatelé přišli o část, či dokonce všechny své vložené finanční prostředky. Naposledy se tak stalo v roce 2022, kdy došlo k, již zmíněnému krachu burzy FTX, třetí největší burzu současnosti.[228]

Kryptoměnové burzy jsou v podstatě tržiště, na kterém se provádí obchody měnových párů, tedy nákup či prodej Bitcoinu ve směnném kurzu k americkému dolaru, euru, české koruně či jiné kryptoměně, označovanou za altcoin. Jedná se tedy o místo, kde probíhá obchod mezi dvěma osobami, přičemž jeden chce Bitcoin nakoupit a druhý jej prodat. Burza slouží v tomto procesu jako prostředník, přes kterého je možné transakci uskutečnit a současně eliminuje nutnost přímé směny mezi 2 osobami.[229]

Směnný kurz je cena za nákup či prodej Bitcoinu ve vztahu k jiné měně. Cena je tvořena protnutím bodu poptávky a bodu nabídky, jedná se tedy o cenu tržní. Cena se v podstatě pohybuje na úrovní, za kolik jsou uživatelé ochotní zobchodovat měnový pár. Cena se neustále vyvíjí a je velmi flexibilní, vzhledem k velkému množství transakcí, které probíhají v řádech milisekund.[230]

Burza si za své služby účtuje poplatky, které ovlivní finální cenu směnného kurzu měnového páru. Mezi tyto poplatky se řadí:

- procentuální poplatek = procentuální část z provedené transakce (obvykle do 1 %);
- pevný poplatek = pevná částka za provedení transakce (např. 1 EUR);
- kombinovaný poplatek = kombinace procentuálního a pevného poplatku za provedení transakce;

[228] Finex. *Kryptoměnové burzy* [online]. Dostupné z: https://finex.cz/rubrika/kryptomeny/burzy/
[229] Finex. *Kryptoměnové burzy* [online]. Dostupné z: https://finex.cz/rubrika/kryptomeny/burzy/
[230] Finex. *Kryptoměnové burzy* [online]. Dostupné z: https://finex.cz/rubrika/kryptomeny/burzy/

- poplatek za vklad prostředků = procenta z vložené částky (nejběžnější u vlaku přes platební kartu, lze eliminovat vkladem přes SEPA platbu, která je zdarma);
- poplatek za výběr prostředků = částka odečtená z vybíraného množství (současně pokrývá poplatek síti za zapsání transakce do Blockchainu);[231]
- spread = rozdíl mezi nákupní a prodejní cenou, který je určován volatilitou a likviditou předmětu směny a jedná se v podstatě o skrytý poplatek burze. [232]

Poplatky se mohou různě lišit v závislosti na frekvenci a objemu provedených transakcích. Poplatky je možné snížit na určitých burzách prostřednictvím využití tokenu burzy při provádění transakcí. Například u burzy Binance je možné poplatky snížit o 25 % při využití tokenu BNB, tedy token Binance sítě, při uskutečnění transakce.[233]

Pro možnost provedení obchodu na burze, je nutné projít autorizací a ověřením klienta. Tento proces se nazývaný KYC aneb „Know your customer“. Pro ověření je žádoucí oskenovat průkaz totožnosti, například občanský nebo řidičský průkaz a doložit dokument s celým jménem a adresou trvalého pobytu, třeba výpis z bankovního účtu. U některých burz existují výjimky možnosti nákupu i bez provedení KYC, jedná se však o limitní částky pohybující se obvykle do 25.000 CZK.[234]

Při výběhu vhodné burzy pro nákup Bitcoinu je nutné zohlednit několik základních faktorů:

- je umožněno na burze obchodovat občanům České republiky z legislativních důvodů;
- důvěryhodnost burzy = burza, která má dobrou pověst a velké množství uživatelů působí obecně důvěryhodněji nežli malá burza s malým počtem uživatelů, dalším ukazatelem může být i objem provedených transakcí;
- zabezpečení burzy = je třeba brát ohled na bezpečnost, tak, aby se burza byla schopna ubránit potencionálnímu hackerskému útoku a podobným situacím, burza by proto měla mít alespoň dvoufázové zabezpečení při přihlášení uživatele na účet či při provádění transakcí se zůstatky na uživatelském učtu;

[231] Finex. *Kryptoměnové burzy* [online]. Dostupné z: https://finex.cz/rubrika/kryptomeny/burzy/
[232] Finex. *Co je to spread?* [online]. Dostupné z: https://finex.cz/co-je-to-spread/
[233] Finex. *Kryptoměnové burzy* [online]. Dostupné z: https://finex.cz/rubrika/kryptomeny/burzy/
[234] Finex. *Kryptoměnové burzy* [online]. Dostupné z: https://finex.cz/rubrika/kryptomeny/burzy/

- možnosti vkladu prostředků = tedy jedná-li se o zahraniční burzu se sídlem v Evropě a je-li možné využít bezplatné SEPA platby.

Vždy je nutné mít na paměti, že jakákoliv provedená chyba v procesu jakékoliv transakce s Bitcoinem povede k nenávratné ztrátě bitcoinů, které byli do transakce zapojeny. Poté již neexistuje žádný způsob, jak ztracené bitcoiny obnovit. Tato chyba se může stát i při výběru té nejlepší burzy, odpovědnost v tomto případě nese vždy uživatel. Většina burz již implementovala různé ochranné kontroly, které by těmto ztrátám měly pomoci zabránit.[235]

Mezi nejznámější a největší kryptoměnové burzy v současné době patří: Binance, Coinbase, Coinmate, Kraken, Bitstamp, Gemini, Bitfinex, Crypto.com, KuCoin a mnoho dalších. Pro finální analýzy nákupního prostředí budou zařazeny dle splnění základních kritérií a na základě jejich velikosti, dobré pověsti a obecné popularitě burzy Binance, Coinbase a Coinmate. [236] [237]

Binance je největší a nejvyužívanější kryptoměnou burzou současnosti. Své popularitě vděčí zejména ohromnému množství obchodovaných altcoinů. Tato práce však uvažuje pouze o investici do kryptoměny Bitcoin, proto je toto kritérium to výběr burzy irelevantní. I tak se jedná o vhodnou burzu pro nákup Bitcoinu.

Celkový proces využívání burzy Binance začíná založení účtu a ověření KYC. Binance je také populární díky nízkým poplatkům, které byly nyní dokonce sníženy na nulu pro transakce v měnovém páru BTC/EUR. Burza disponuje prostředím v mnoha jazycích, včetně jazyka českého. Současně lze využívat prostřednictvím mobilní aplikace. Prostředí lze považovat za relativně přívětivé, které nabízí velké množství funkcí. K dispozici je i funkce automatické investice metodou DCA. Platforma je však spíše vhodnější pro zkušenější uživatele. Nákup Bitcoinu je možné provést v měnovém páru s USD a EUR. Tyto měny lze díky SEPA platbě vložit na burzu zcela zdarma. Bohužel českou korunu doposud burza nepodporuje. Burza se současně pyšní dobrou pověstí. Od svého vzniku v roce 2017 burza čelila mnoha hackerským útokům, přičemž jediný úspěšný byl v roce 2019, kdy se hackerům podařilo odcizit přibližně 7.000 bitcoinů, nicméně všechny poškozené uživatele

[235] Finex. *Kryptoměnové burzy* [online]. Dostupné z: https://finex.cz/rubrika/kryptomeny/burzy/
[236] Finex. *Kryptoměnové burzy* [online]. Dostupné z: https://finex.cz/rubrika/kryptomeny/burzy/
[237] CoinMarketCap. *Top Cryptocurrency Spot Exchanges* [online]. Dostupné z: https://coinmarketcap.com/rankings/exchanges/

burza plně kompenzovala. Kromě klasického nákupního prostředí burzy Binance také nabízí jednodušší prostředí směnárny, které však díky jednoduššímu užívání požaduje vyšší poplatky nežli na burze. V případě využití burzy Binance je vhodné současně využít služby společnosti Revolut, kde je možné si směnit EUR za CZK bez poplatků za nejvýhodnější směnný kurz a za pomocí SEPA platby následně prostředky bezplatně vložit na burzu.

Výhody:

- největší kryptoměnová burza;
- nulové poplatky BTC/EUR za transakci;
- velké obliba uživatelů a kladně recenze;
- dobrá pověst bezpečnosti (2FA);
- mobilní aplikace;
- velké množství nabízených služeb a měn;
- vklad zdarma SEPA platbou.

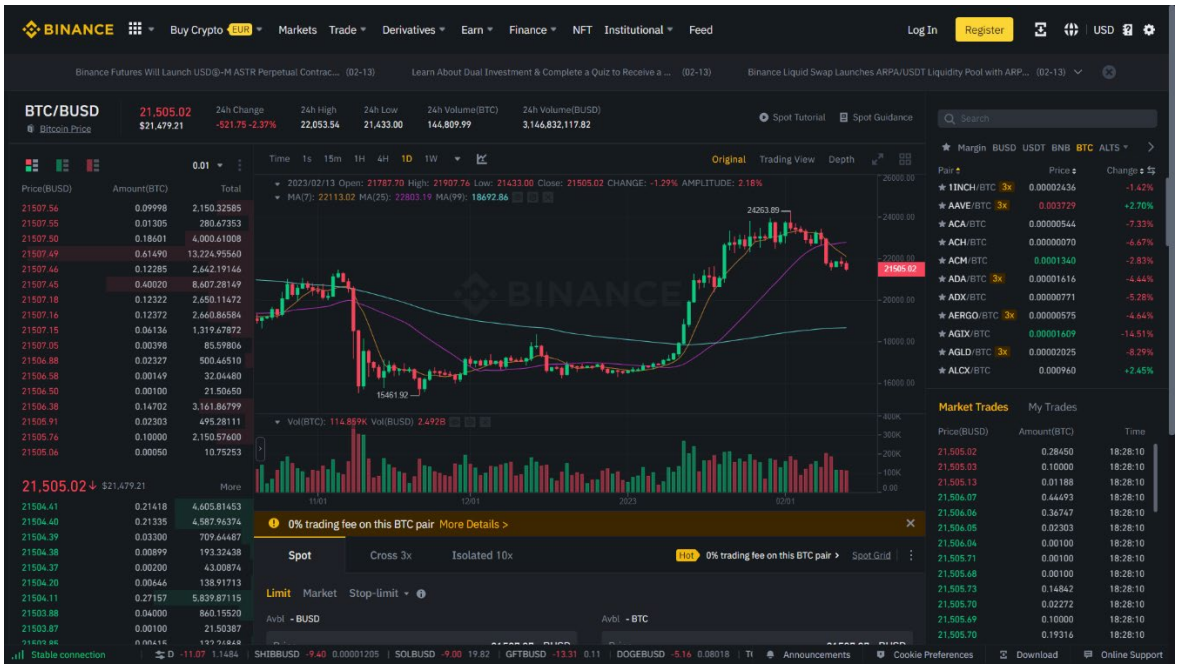
Nevýhody:

- prostředí vhodnější pro zkušenější uživatele;
- ověření KYC při nákupu nad 25.000 CZK;
- složitý kontakt zákaznické podpory;
- není možnost nákupu ve CZK. [238] [239]

Prostředí burzy je zobrazeno v obrázku 6.

[238] Finex. *Recenze burzy Binance* [online]. Dostupné z: https://finex.cz/recenze/binance/
[239] Binance. *Binance* [online]. Dostupné z: https://www.binance.com/en

Obrázek 6 Prostředí burzy Binance



Zdroj: Binance. [online]. Dostupné z: https://www.binance.com/en

Coinbase je jednou z nejpopulárnější kryptoměnových burz. Novinkou roku 2023 je sloučení předešlých dvou platforem Coinbase a Coinbase Pro, přičemž Coinbase byla směnárna s vyššími poplatky a Coinbase Pro byla burza. Nyní je vše sloučeno do jedné platformy a mezi směnárnou a burzou lze přecházet. Účet je třeba podrobit KYC ověření a následně je možná obchodovat s nízkými poplatky ve výši 0,5 % z provedené transakce. Tento poplatek se vyšším objemem snižuje. Vklady a výběry jsou následně osvobozeny od poplatků burze, kromě samozřejmého poplatku těžařům za zapsání transakce, jenž je automaticky odečten z vybírané částky. Na burze je možné nakupovat BTC ve směnném kurzu k EUR. Nákup ve CZK není možný. Burza disponuje velmi přívětivým uživatelským prostředím, současně tak dostatečným množstvím funkcí. Coinbase má velmi dobrou pověst. Od svého založení v roce 2015 neměla burza žádné významné problémy. Současně burza využívá 2FA při přihlášení do uživatelského účtu. V případě nákupu na burze Coinbase je doporučené také využít služby společnosti Revolut, kde je možné směnit EUR za CZK bez poplatků za nejvýhodnější směnný kurz a následně je vložit na burzu zcela zdarma prostřednictvím SEPA platby.

Výhody:

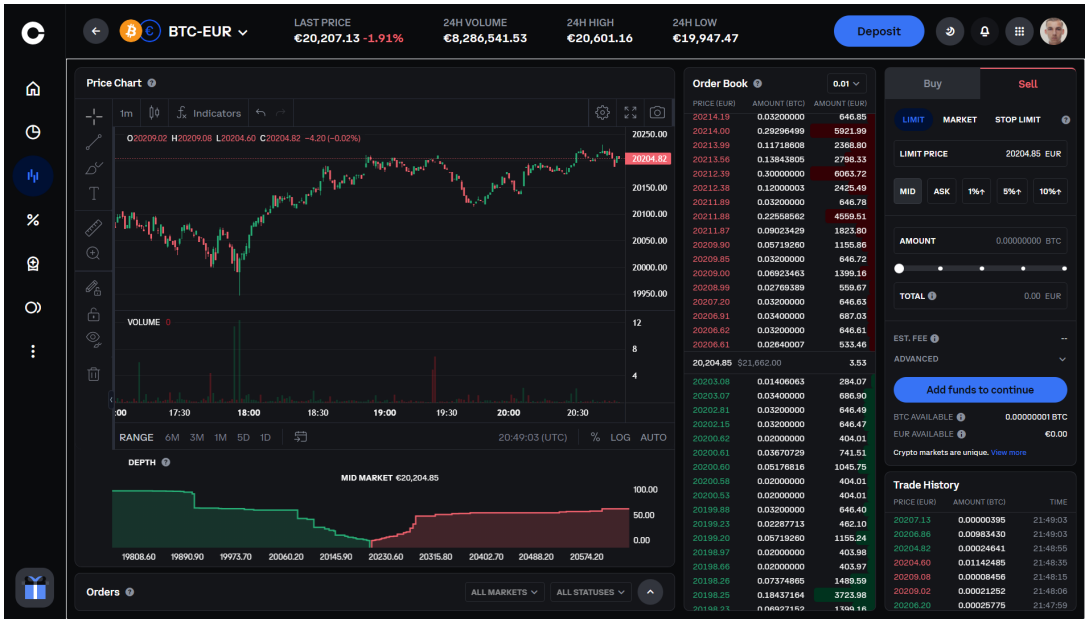
- nízké poplatky;
- velké obliba uživatelů a kladné recenze;
- dobrá pověst celkové bezpečnosti burzy (2FA);
- mobilní aplikace;
- uživatelsky přívětivé prostředí;
- vklad finančních prostředků zdarma prostřednictvím SEPA platby.

Nevýhody:

- ověření KYC;
- nepodporovaná měna CZK;
- prostředí není dostupné v českém jazyce;
- prostředí burzy je složitější pro začátečníky;
- špatná zákaznická podpora.[240] [241]

Prostředí burzy je zobrazeno v obrázku 7.

Obrázek 7 Prostření burzy Coinbase



Zdroj: Coinbase. [online]. Dostupné z: https://www.coinbase.com/advanced-trade/

[240] Finex. *Recenze nurzy burzy Coinbase Pro* [online]. Dostupné z: https://finex.cz/recenze/coinbase-pro/
[241] Coinbase. *Home* [online]. Dostupné z: https://www.coinbase.com/home

Coinmate je poslední z vybraných burz pro srovnávací analýzu, současně se jedná jedinou českou burzou v tomto výběru, která byla založena již v roce 2014 a má velmi dobrou pověst mezi uživateli. Při zakládání účtu je nejdříve nutné projít ověřením KYC a následně je možné si nastavit 2FA. Hlavní výhodou burzy je možnost vkládat a následně nakupovat BTC za české koruny. Současně je však možné nakupovat BTC za eura. Burza má příjemné uživatelské prostředí, které však nabízí méně funkcí či měn nežli konkurenční burzy, pro tuto práci jsou však tyto funkce nepodstatné. Obecně je burza vhodná zejména pro české uživatele, vzhledem k výhodám plynoucím pro transakce v české koruně, vklady, výběry, prostředí v českém jazyce a zákaznické podpoře v českém jazyce. Další výhody jsou nízké poplatky a nízké spready ceny.

Výhody:

- optimální pro české uživatele;
- platforma v českém jazyce;
- obchodování v CZK;
- nízké poplatky a spready;
- jednoduchá platforma;
- dobrá zákaznické podpora v českém jazyce;
- pokročilá směnárna s nízkými poplatky a spready ceny.

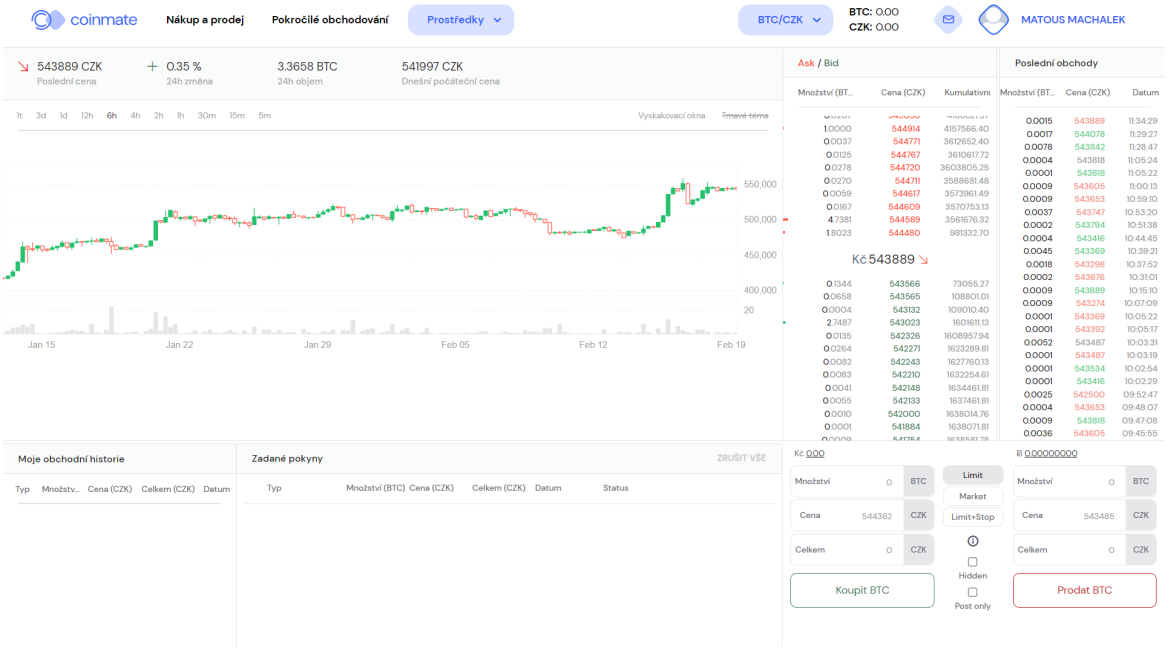
Nevýhody:

- absence mobilní aplikace;
- KYC.[242] [243]

Prostředí burzy je zobrazeno v obrázku 8.

[242] Finex. *Coinmate* [online]. Dostupné z: https://finex.cz/recenze/coinmate//
[243] Coinmate. *Home* [online]. Dostupné z: https://coinmate.io/cs

Obrázek 8 Prostření burzy Coinmate



Zdroj: Coinmate. [online]. Dostupné z: https://coinmate.io/pages/secured/trade.page

Směnárny

Kryptoměnové směnárny umožňují proces nákupu a prodeje Bitcoinu, který je vhodný pro méně zkušené uživatele. Oproti burze se jedná o jednoduší prostředí, jenž je za cenu vyšších poplatků za využití služeb. Většina z velkých burz, jako jsou Binace, Coinbase či Coinmate také nabízí platformu směnárny. Jedná se tedy o platformu, kde je možné směnit Fiat měny na bitcoiny a naopak. Nákupní cena a cena prodejní se vždy bude lišit, díky vyššímu spready ceny. Právě spread cen je hlavní nevýhodou směnáren oproti burzám, na které se obchoduje za cenu tržní. Obecně platí, že poplatky a procenta spreadu nejsou na směnárnách malé, obvykle se pohybují v řádech jednotek procent. Směnárna je oproti burze pouze prostředníkem vykonávajícím objednávky uživatelům na trhu burzy. Centralizované krypto burzy mají často daleko větší a robustnější finanční základnu, nežli mají směnárny. Vklady bankovním převodem bývají také zdarma, stejně tak výběr, samozřejmostí je úhrada poplatku těžařům v případě výběru Bitcoinu, bez kterého by se transakce do Blockchainu nezapsala a nebyla by tak potvrzena. [244]

[244] Finex. *Kryptoměnové směnárny* [online]. Dostupné z: https://finex.cz/rubrika/kryptomeny/krypto-smenarny/

V dnešní době existuje velké množství směnáren, které je možno pro transakce Bitcoinu využít. Mezi hlavní kryptoměnové směnárny patří: Anycoin, Simplecoin, Change Invest, Coin Bank či Finex.cz. Jako nejvhodnější směnárnu pro českého uživatele na základně českého původu a reputace byla pro potřeby této práce vybrána směnárna Anycoin.[245]

Anycoin je česká kryptoměnová směnárna, která nabízí nákup a prodej Bitcoinu s nižšími poplatky na poměry směnárny. Na směnárně Anycoin je možné nakoupit kryptoměnu Bitcoin bez registrace až do výše 25.000 CZK. Bitcoin je možné zakoupit v měnovém páru s eurem nebo českou korunou. Směna Bitcoinu za jiné altcoiny na směnárně provést nelze. Směnárna poskytuje rychlé, přehledné a jednoduché prostředí v českém jazyce. K dispozici je také mobilní aplikace. Vklad finanční prostředků lze provést zdarma, pouze však prostřednictvím bankovního převodu. Výběry jsou také zdarma, nepočítá-li se poplatek těžařům za zapsání transakce, který však k přednastaveným rychlostem zapsání transakce může být vyšší. Hlavní nevýhodou směnárny je však spread nákupní a prodejní ceny, který se pohybuje kolem 3 %, tedy 1,5 % na každou stranu od středové ceny. I tak se však jedná na poměry směnáren o nižší spread ceny. Například na směnárnách SimpleCoin se pohybuje spread do výše 6 % a u směnárny CoinBank 4,5 %. Směnárna oproti největším burzám nedisponuje velkým množstvím funkcí, avšak všechny potřebné jsou k dispozici. Anycoin získal od svého založení v roce 2019 dobrou pověst. Za tuto dobu také nikdy neměla bezpečnostní problémy a umožňuje 2FA při přihlášení na již zaregistrovaný. Alarmující však je, že v případě obnovy hesla, je možné ho provést tento proces pouze prostřednictví emailu. Jiné směnárny a burzy vyžadují v procesu obnovy hesla i kód zaslaný na telefonní číslo, což zvyšuje bezpečnost procesu a směnárna Anycoin tak v zabezpečení tohoto zaostává. Zákaznickou podporu je však možné kontaktovat v českém jazyce prostřednictvím e-mailu či telefonu.

[245] Finex. *Kryptoměnové směnárny* [online]. Dostupné z: https://finex.cz/rubrika/kryptomeny/krypto-smenarny/

Výhody:

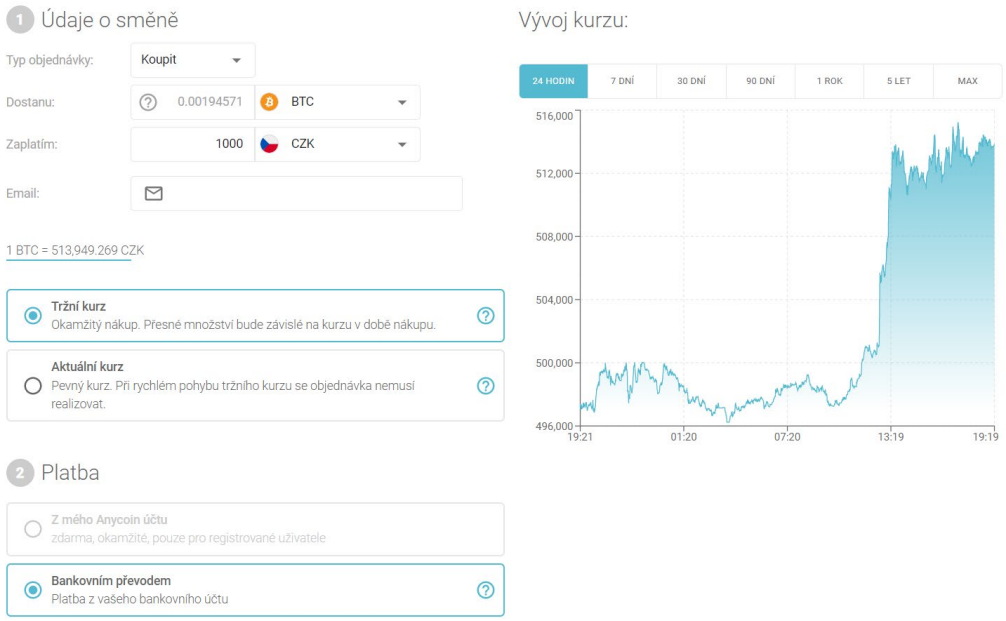
- možný nákup bez registrace;
- funkce automatického nákupu;
- transakce v CZK;
- jednoduché prostředí v českém jazyce;
- nákup bez ověření KYC do 25.000 CZK;
- mobilní aplikace;
- kvalitní zákaznická podpora v české jazyce.

Nevýhody:

- vysoké poplatky;
- vyšší spread cen;
- nižší bezpečnost způsobena jednofaktorovým ověřením v procesu obnovy hesla.[246]

Prostředí burzy je zobrazeno v obrázku 9.

Obrázek 9 Prostření směnárny Anycoin



Zdroj: Anycoin. [online]. Dostupné z: https://www.anycoin.cz/exchange

[246] Finex. *Kryptoměnová směnárna Anycoin* [online]. Dostupné z: https://finex.cz/recenze/anycoin/

Decentralizované burzy

V současné době pro nákupy a prodeje BTC dominují centralizované kryptoměnové burzy neboli CEX. Jejich hlavní nevýhodou je již zmíněná centralizace, které jde proti podstatě decentralizované měny Bitcoin. Je totiž nutné prostředky pro směnu držet na zákaznických účtech vedených u daných burz. Pokud chce uživatel nakupovat Bitcoin bez ověření KYC a současně mít vždy ve vlastnictví své soukromé klíče, nabízí se mu alternativní cesta v podobě decentralizované burzy, zkráceně DEX, které fungují na způsob peer-to-peer portálů.[247]

Decentralizované burzy mají zcela odlišný princip, nežli mají burzy centralizované. Na DEX neexistuje prostředník mezi dvěma protistranami, jedná se tedy o čistý peer-to-peer obchod. Prostředky jsou plně ve vlastnictví uživatelů a ti si tak sami ručí za bezpečnost svých soukromých klíčů svých kryptoměnových peněženek. Díky tomu se transakce uskutečňují přímo na blockchainu.[248]

Mezi hlavní výhody decentralizovaných kryptoměnových burz patří anonymita a svoboda uživatelů, pro které je nežádoucí podstupovat ověřovací proces KYC. Nejsou nuceni tak dokládat zdroj a původ svých finančních prostředků. Zde však vzniká otázka ohledně AML, která je částečně eliminována transparentností blockchainu, kam je i tak každá transakce zapsána a snadno dohledatelná a propojitelná s ostatnímu provedenými transakcemi a účty. DEX navazuje na hlavní myšlenku kryptoměn, a to je decentralizace finančního systému.[249]

I přes tyto výhody DEX mají spoustu nevýhod, které tak jsou v podstatě poplatkem za decentralizovanost. Jednou z nich je zajisté horší uživatelské přívětivost a složitost uživatelského prostředí. Vzhledem k absenci prostředníka, na DEX není k dispozici zákaznická podpora. Zmnohonásobuje se tak riziko ztráty prostředků pro méně zkušené uživatele. Pokud se v procesu transakce něco pokazí, vzhledem k faktu, že je nutné držet prostředky na vlastních peněženkách a při transakci protistrana narazí na hackera či podvodníka, který se zmocní prostředků protistrany, není možné se na někoho obrátit. Další nevýhody jsou zajisté nižší likvidita, nežli je u CEX. Běžností jsou i několikanásobně vyšší

[247] Finex. *Decentralizované burzy* [online]. Dostupné z: https://finex.cz/rubrika/kryptomeny/decentralizovane-burzy/?ac=decentralizova&sc=autocomplete
[248] Finex. *Decentralizované burzy* [online]. Dostupné z: https://finex.cz/rubrika/kryptomeny/decentralizovane-burzy/?ac=decentralizova&sc=autocomplete
[249] Finex. *Decentralizované burzy* [online]. Dostupné z: https://finex.cz/rubrika/kryptomeny/decentralizovane-burzy/?ac=decentralizova&sc=autocomplete

poplatky za provedené transakce, které jsou navýšeny zejména z toho důvodu, že se pracuje přímo na blockchainu. Obvyklý bývá i větší spread ceny od běžné ceny. Poplatek za anonymitu je ten vysoký a DEX rozhodně není vhodné pro méně zkušené uživatele.[250]

V současné době je možné vybírat ze stovek až tisíců decentralizovaných kryptoměnových burz. Mezi hlavní patří 1icnh, PancakeSwap, SushiSwap, Uniswap, Bisq a mnoho dalších. Většina z nich je však přizpůsobená zejména pro transakce altcoinů. Pro obchod s Bitcoinem je nejvhodnější decentralizované P2P burza Bisq, která je z důvodu přizpůsobení uživatelského prostředí pro obchody s Bitcoinem zařazena do srovnávací analýzy.[251]

Bisq je decentralizovanou peer-to-peer kryptoměnovou burzou, na které uživatelé sami drží své soukromé klíče a vystupují v relativní anonymitě. Bisq se tedy drží filozofie Bitcoinu a převádí zodpovědnost za své finanční prostředky do rukou svých uživatelů. Platí zde známé pravidlo „Not your keys, not your coins“. Díky neexistence třetí strany není vyžadováno ověření KYC/AML, jenž o uživateli nezvratně poskytuje velké množství soukromých dat, jako je jméno, bydliště, fotografie, adresa a další. I přes to, že centralizované burzy kladou velký důraz na zabezpečení a ochranu těchto dat, již v minulosti nastalo několik situací, kdy došlo k úniku těchto citlivých informací.[252]

Burza Bisq funguje na způsob tržiště, na kterém mají uživatelé možnost vytvořit vlastní nabídku na nákup či prodej Bitcoinu a Bisq tyto uživatele pouze vzájemně propojí. Obchody jsou umožněny díky smart kontraktům, na které dva spolu obchodující uživatelé zasílají zálohu pro zajištění bezpečností a uskutečnění transakce a následně obchodované bitcoiny. Tento postup zajišťuje bezpečnost transakce. Celý projekt burzy je open-source a komunikace na burze mezi kupujícím a prodávajícím probíhá přes šifrovaný chat, který umožňuje zachovat skrytou identitu uživatelů.[253]

Při založení účtu se současně vytvoří non-custodial peněženka, které uživateli dává plnou kontrolu od svých veřejných i soukromých klíčů a současně plnou kontrolu nad svou

[250] Finex. *Decentralizované burzy* [online]. Dostupné z: https://finex.cz/rubrika/kryptomeny/decentralizovane-burzy/?ac=decentralizova&sc=autocomplete
[251] Finex. *Decentralizované burzy* [online]. Dostupné z: https://finex.cz/rubrika/kryptomeny/decentralizovane-burzy/?ac=decentralizova&sc=autocomplete
[252] Finex. *Decentralizovaná P2P burza Bisq* [online]. Dostupné z: https://finex.cz/recenze/bisq/
[253] Finex. *Decentralizovaná P2P burza Bisq* [online]. Dostupné z: https://finex.cz/recenze/bisq/

peněženkou a uloženými prostředky [254], od které je třeba si bezpečně uložit seed. Vklady je možné provést prostřednictvím klasické SEPA platby, přes peněženku Revolut. Existuje je možnost za obchod zaplatit v hotovosti na osobním setkání, které je možné domluvit přes šifrovaný chat. Jak již bylo zmíněno, před uzavřením obchodu je nutné vlastnit nějaké bitcoiny/satoshi tak, aby bylo možné je v průběhu obchodu použít jako zálohu, jenž bude uzamčena před uzavřením transakce. Obvykle se jedná o 15–40 % z obchodované částky. Záloha se uzamkne na multisig adresu a zajistí se tak bezpečnost transakce. Následně dojde k dočasnému odhalení bankovní identity druhé strany, pro možnost odeslání finančních prostředku prodávajícímu a zakoupené bitcoiny kupujícímu. Po potvrzení úspěšné transakce z obou stran se odemkne poskytnutá záloha, která je následovně vrácena, jak kupujícímu, tak i prodávajícímu. Pro zaručení celkové bezpečnosti jsou zavedeny obchodní limity. Z počátku je uživatel omezen na transakce do 0,01 BTC. S postupem času roste uživateli kredibilita a tím se mu umožní provádět transakce s vyššími limity, a to až do výše 0,25 BTC. Minimalizuje se tím možnost různých podvodů a AML problémů. Za prováděné transakce je však nutné si připlatit. Vzhledem tomu, že poplatky za transakci navrženou protějším uživatelem začínající na 0,01 % z provedené transakce a stoupají až do řádu jednotek %. Vyšším nákladům na nákup déle přispívá vyšší spread ceny a poplatky těžařů za zápis každé transakci do blockchainu. To vše je bráno jako cena za anonymitu.[255]

Výhody:

- anonymita a absence KYC;
- plná kontrola a vlastnictví soukromých klíčů.

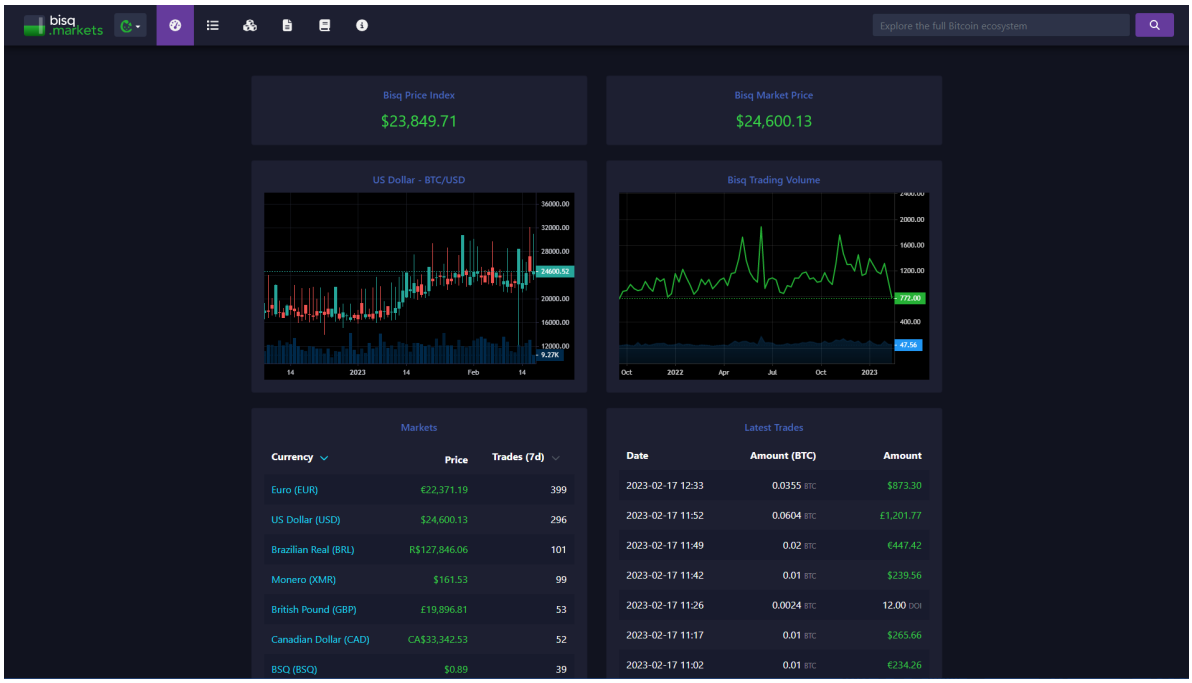
Nevýhody:

- vysoké poplatky;
- prostředí pouze v anglickém jazyce;
- absence mobilní aplikace;
- složitější prostředí vhodné pro zkušené uživatele.[256] [257]

[254] Ledger. *Non-Custodial Wallet* [online]. Dostupné z: https://www.ledger.com/academy/glossary/non-custodial-wallet
[255] Finex. *Decentralizovaná P2P burza Bisq* [online]. Dostupné z: https://finex.cz/recenze/bisq/
[256] Finex. *Decentralizovaná P2P burza Bisq* [online]. Dostupné z: https://finex.cz/recenze/bisq/
[257] Bisq. *The Bisq DAO* [online]. Dostupné z: https://bisq.network/dao/

Prostředí směnárny je zobrazeno v obrázku 10.

Obrázek 10 Prostření směnárny Bisq



Zdroj: Bisq [online]. Dostupné z: https://bisq.markets/

Bitcoinové bankomaty

Bitcoiny je možné zakoupit také „offline“. Pro tyto účely se dají využít bitcoinové bankomaty/ATM známé takové pod pojmem „bitcoinmaty“. Bankomaty jsou spíše automatizované směnárny, vzhledem k tomu, že s bankou nemají nic společného. Existují dva typy bitcoinmatů a to jednosměrné, které bitcoiny pouze prodávají a obousměrné, na kterých je možno Bitcoin nakoupit i prodat. Pro nákup je dostačující mít k dispozici kryptoměnovou peněženku, či je možné si nechat soukromý klíč vytisknout na papír. Nakoupit bez ověřovacího procesu KYC je umožněno do výše 25.000 CZK za den, po překročení je vyžadována registrace. Nákup probíhá v českých korunách, přičemž se do bitcoinmatu vkládá hotovost. Po vložení hotovosti se naskenuje kód peněženky, na který má bitcoinový AMR bitcoiny odeslat a ty jsou následně několika minut přijaty a potvrzeny na zadané adrese. Prodej funguje obdobným způsobem, pouze v opačném směru. Poplatky za provedení transakce jsou však vysoké, okolo 100 CZK za provedenou transakci či ve vyšších řádech % z provedené transakce. Častý nákup o malých částkách tak není vhodné provádět právě přes bitcoinmat a je rozhodně výhodnější přejít na jinou formu online nákupu, zde

bude možné získat daleko více Bitcoinu za stejnou investovanou částku. Nejen po celém světě, ale i v České republice je dnes k nalezení velké množství bitcoinmatů.

Výhody:

- anonymita a absence ověřovacího procesu KYC;
- rychlost provedených transakcí;
- jednoduchost.

Nevýhody:

- offline obchod, který je možný provést na vybraném bitcoinmatu;
- vysoké poplatky za transakci;
- vysoké spready cen.[258] [259]

Ukázkou Bitcoinového ATM je obrázek 11.

Obrázek 11 Bitcoinový ATM

Zdroj: Tuesday. *Bitcoin a další kryptoměny* [online]. Dostupné z: https://www.tuesday.cz/akce/bitcoiny/

[258] Finex. *Jak nakoupit nebo prodat bitcoin v automatu* [online]. Dostupné z: https://finex.cz/jak-nakoupit-nebo-prodat-bitcoin-v-automatu/
[259] imore. *Bitcoinový bankomat: Jak funguje a jak jej používat?* [online]. Dostupné z: https://www.imore.cz/post/14512-bitcoinovy-bankomat-jak-funguje-a-jak-jej-pouzivat

4.2.2 Analýza nákupního prostředí

Pro účely této práce je provedena srovnávací analýza nákupního prostředí pro výběr finálního prostředí nákupu a následnou práci s vybraným prostředím. Do srovnávací analýzy byly na základně předchozích zjištěných informací zahrnuty:

- 3 centralizované burzy = Binace, Coinbase, Coinmate;
- 1 směnárna = Anycoin;
- 1 decentralizovaná burza/P2P směnárna = Bisq;
- 1 obecný bitcoinový bankomat.

Tyto nákupní prostředí jsou srovnány na základě několika vybraných kritérií. Kritéria byla vybrána na základě důležitosti a relevantnosti z doposud získaných informací a zajistí tak výběr nevhodnějšího nákupního prostředí pro účely této práce a současně zajistí výběr nákupního prostředí s nejvýhodnějšími podmínkami pro nákup Bitcoinu. Mezi podstatná kritéria byla zařazena kritéria:

- druh;
- možnost transakce přes webové stránky;
- možnost transakce přes mobilní aplikaci;
- přítomnost ověřovacího procesu KYC;
- možnost transakce v CZK;
- možnost transakce v EUR;
- výše poplatku za vlak;
- výše poplatku při výběru bitcoinu v BTC;
- výše poplatku za provedení transakce v % z transakce;
- výše minimálního obchodu;
- hodnocení uživatelského prostředí na hodnoticí škále 0 do 10 (0 = nejhorší, 10 = nejlepší);
- hodnocení náročnosti použití na hodnoticí škále od 0 do 10 (0 = nejhorší, 10 = nejlepší);
- hodnocení bezpečnosti na hodnoticí škále od 0 do 10 (0 = nejhorší, 10 = nejlepší).

Následně výsledkům byly přiděleny váhy důležitosti od 0 do 10 (0 = nejhorší, 10 = nejlepší) na základě důležitosti kritéria pro rozhodovací proces výběru nejvhodnějšího a

nejvýhodnějšího nákupního prostředí pro účely této práce. Nákupy přes PayPal, Revolut či různé brokery, které nabízejí bitcoinové deriváty nebyly do srovnávací analýzy zahrnuty z důvodu absence možnosti výběru zakoupených bitcoinů, tedy absencí vlastnictví soukromých klíčů. Všechna kritéria byla zanesena do tabulky 1.

Tabulka 1 Analýza srovnání nákupního prostředí – základní data

Název	druh	webová stránka	mobilní aplikace	KYC	transakce v CZK	transakce v EUR	poplatek za vlak	poplatek za výběr (v BTC)	poplatek za transakci (v %)	minimální obchod	uživatelské prostředí (1-10)	náročnost použití (1-10)	bezpečnost
Binace	burza	ANO	ANO	ANO	NE	ANO	Zdarma	0,0004	0	0,0001 BTC	6	5	8
Coinbase	burza	ANO	ANO	ANO	NE	ANO	Zdarma	0	0,5	0,0001 BTC	7	6	10
Coinmate	burza	ANO	NE	ANO	ANO	ANO	Zdarma	7E-05	0,35	50 CZK	9	7	9
Anycoin	směnárna	ANO	ANO	od 25.000 CZK	ANO	ANO	Zdarma	0	1,5	0,0001 BTC	9	9	6
Bisq	P2P směnárna	ANO	NE	NE	ANO	ANO	Zdarma	0	0,5	dle nabídky	7	3	3
Bitcoinmat	AMT	NE	NE	NE	ANO	NE	Zdarma	100 CZK	8	100 CZK	9	9	6

Zdroj: Vlastní zpracování

Jednotlivá kritéria byla vyhodnocena a došlo k přidělení bodů na hodnoticí škále od 0 do 10, které je zachyceno v tabulce 2.

Tabulka 2 Analýza srovnání nákupního prostředí – přidělení bodů

Název	webová stránka	mobilní aplikace	KYC	transakce v CZK	transakce v EUR	poplatek za vlak	poplatek za výběr (v BTC)	poplatek za transakci (v %)	minimální obchod (1-10)	uživatelské prostředí (1-10)	náročnost použití (1-10)	bezpečnost
Binace	1	1	0	0	1	1	2	10	6	6	5	8
Coinbase	1	1	0	0	1	1	5	5	6	7	6	10
Coinmate	1	0	0	1	1	1	3	7	4	9	7	9
Anycoin	1	1	1	1	1	1	5	1	6	8	9	6
Bisq	1	0	2	1	1	1	5	5	2	7	3	3
Bitcoinmat	0	0	2	1	0	1	1	0	1	7	8	5
body	0-10	0-10	0-10	0-10	0-10	0-10	0-10	0-10	0-10	0-10	0-10	0-10

Zdroj: Vlastní zpracování

Následně výsledným hodnotám byly přiděleny váhy důležitosti v rozhodovacím procesu, které jsou zobrazeny v tabulce 3.

Tabulka 3 Analýza srovnání nákupního prostředí – výsledné hodnocení

Název	webová stránka	mobilní aplikace	KYC	transakce v CZK	transakce v EUR	poplatek za vlak	poplatek za výběr (v BTC)	poplatek za transakci (v %)	minimální obchod (1-10)	uživatelské prostředí (1-10)	náročnost použití (1-10)	bezpečnost	výsledek
Binace	3	2	0	0	5	3	10	70	24	48	40	72	277
Coinbase	3	2	0	0	5	3	25	35	24	56	48	90	291
Coinmate	3	0	0	8	5	3	15	49	16	72	56	81	308
Anycoin	3	2	6	8	5	3	25	7	24	64	72	54	273
Bisq	3	0	12	8	5	3	25	35	8	56	24	27	206
Bitcoinmat	0	0	12	8	0	3	5	0	4	56	64	45	197
váha (0-10)	3	2	6	8	5	3	5	7	4	8	8	9	

Zdroj: Vlastní zpracování

Z vyhodnocení provedené analýzy vzešel výsledek, který vybral centralizovanou kryptoměnovou burzy Coinmate jako nejvhodnější a nejvýhodnější nákupní prostředí pro účely této práce. Burza Coinmate získala nejvyšší počet bodů o celkoví výši 308 bodů, jak je zachyceno v tabulce 3. Na druhém místě se umístila burza Coinbase, na třetím místě burza Binance. Celkově se tedy centralizované burzy ukázaly pro nákup bitcoinů jako ideální variantou, zejména díky jednoduchosti použití, nízkým poplatků a dobré bezpečnosti. Pozici čtvrtého místa obsadila kryptoměnová směnárna Anycoin, která pracuje na obdobný způsob jako centralizované burzy, jen je díky jednoduššímu prostředí nutné si připlatit za vyšší poplatky při provedené transakci. Páté místo obsadila peer-to-peer směnárna Bisq, která je díky nižší uživatelské přívětivosti a vyšší poplatkům vhodná zejména pro zkušené uživatele bitcoinové sítě, kteří jsou si ochotni za zachování anonymity připlatit. Poslední místo obsadil bitcoinmat, který má podobné výhody anonymity jako decentralizované burzy ovšem s lehčím uživatelským prostředím, nicméně je nutné počítat s nejvyššími poplatky ze všech nákupních prostředích, které byly součástí analýzy.

Pro nákup Bitcoinu je tedy, na základně provedení srovnávací analýzy nákupního prostředí a následného vyhodnocení této analýzy, vybrána centralizovaná kryptoměnová burza českého původu Coinmate, se kterou se bude dále v práci pracovat.

4.2.3 Aktivní nákup

Vyhodnocení srovnávací analýzy nákupního prostředí ukázalo centralizovanou kryptoměnovou burzu Coinmate jako nejvhodnější pro nákup Bitcoinu.

Pro možnosti nákupu na burze Coinmate je zapotřebí se nejdříve se registrovat za pomocí e-mailu, na který bude zaslán potvrzovací e-mail, přes který se následně aktivuje účet a verifikuje. Poté je možné se do účtu za pomocí stejných přihlašovacích údajů přihlásit. Pro plnou aktivaci účtu je nutné zadat základní informace – typ účtu, adresa, telefonní číslo, které je za pomocí SMS zprávy ověřeno. V následujícím kroku je třeba nahrát průkaz totožnosti, přičemž dojde za pomocí QR kódu k přesměrování na mobilní telefon, který disponuje kamerou pro pořízení fotografie. Průkaz totožnosti, například občanský průkaz, řidičský průkaz či cestovní pas, je třeba vyfotit z obou stran. Po nahrání průkazu je potřeba pořídit fotografii obličeje pro dostoupení ověřovacího procesu KYC. Následuje nahrání druhého typu dokladu totožnosti, který bude současně odlišný od předešlého, který byl použit v předchozím kroku. Dokument je nutné vyfotit a nahrát opět z obou stran. Po

automatické kontrole totožnosti a je nutné vyčkat na odsouhlasení manuální kontroly totožnosti, kterou verifikuje zaměstnanec burzy. Tato kontrola obvykle trvá několik minut. Dále je třeba vyplnit investiční dotazník, který obsahuje otázky:

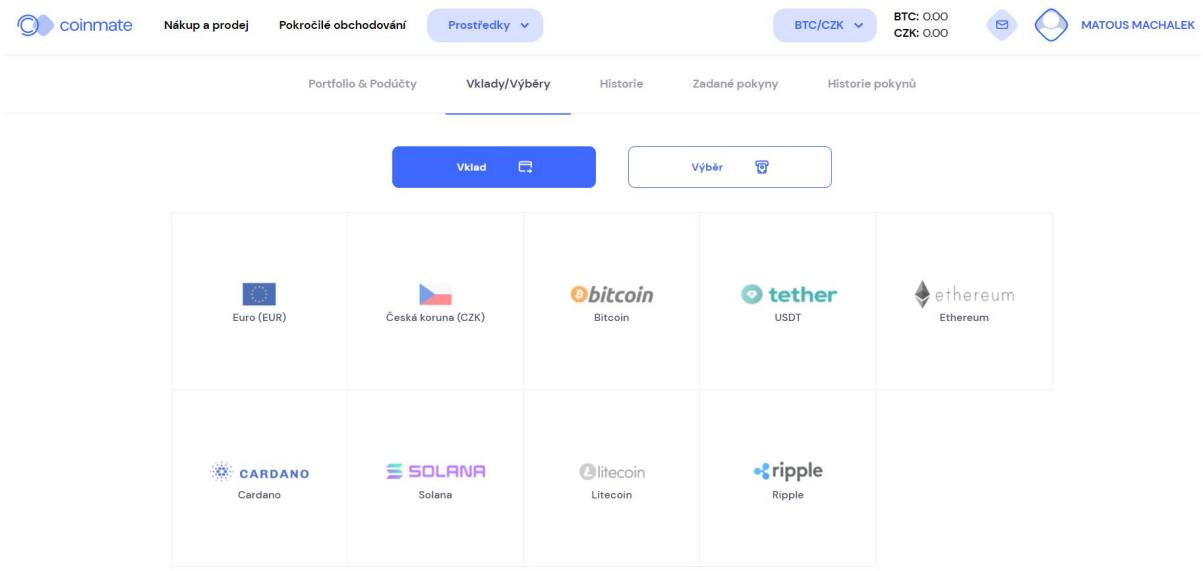
- Jakým způsobem budete využívat obchodní účet?
- Jaké jsou zdroje vámi vkládaných prostředků?
- Jaké jsou vaše zkušenosti s investováním?
- Jste politicky exponovaná osoba?
- Máte občanství USA?

Nyní je účet plně aktivovaný a je možné přejít k nákupu Bitcoinu. Ještě před prvním nákupem je doporučeno aktivovat dvoufázový způsob ověřování za pomocí aplikace Google Authenticator, jenž generuje náhodné šestimístné kódy, které jsou následně použity pro potvrzení prováděné akce na uživatelském účtu. Do aplikace Google Authenticator je uživatel opět přesměrován za pomocí QR kódu. Aplikace se následně spáruje opět za pomocí QR kódu a vygenerovaný kód je následně zapotřebí pro ověření uživatelského účtu na burze Coinmate. Náhodný kód z aplikace Google Authenticator se aktualizuje každých 30 vteřin. Druhé ověření probíhá za pomocí SMS či emailové zprávy. Pro zabezpečené přihlášení je také možné spárovat účet na burze s účtem z hardwarové peněženky Trezor, přičemž přihlašování na burzu bude probíhat za pomocí zařízení Trezor a PIN kódu, více v kapitole Uložení Bitcoinu.[260]

Pro první nákup Bitcoinu je nutné nejdříve vložit na účet finanční prostředky. Rychlý nákup přes debetní či kreditní kartu není doporučen, vzhledem k poplatku 1,9 % z provedené transakce u Visa karty a 2,9 % z provedené transakce u Mastercard karty. Pro účely této práce se postupuje s variantou vkladu finančních prostředků v české koruně za pomocí bankovního převodu s denním limitem vkladu 25.000 CZK a současně měsíčním limitem vkladů 500.000 CZK. V průběhu tohoto procesu je zapotřebí vybrat výši vkladu, výběr banky, provést přihlášení do bankovního účtu a dokončit platbu. Po potvrzení platby se obvykle finanční prostředky připíší do několika vteřin. Prostředí burzy Coinmate pro vlak je zobrazeno v obrázku 12.

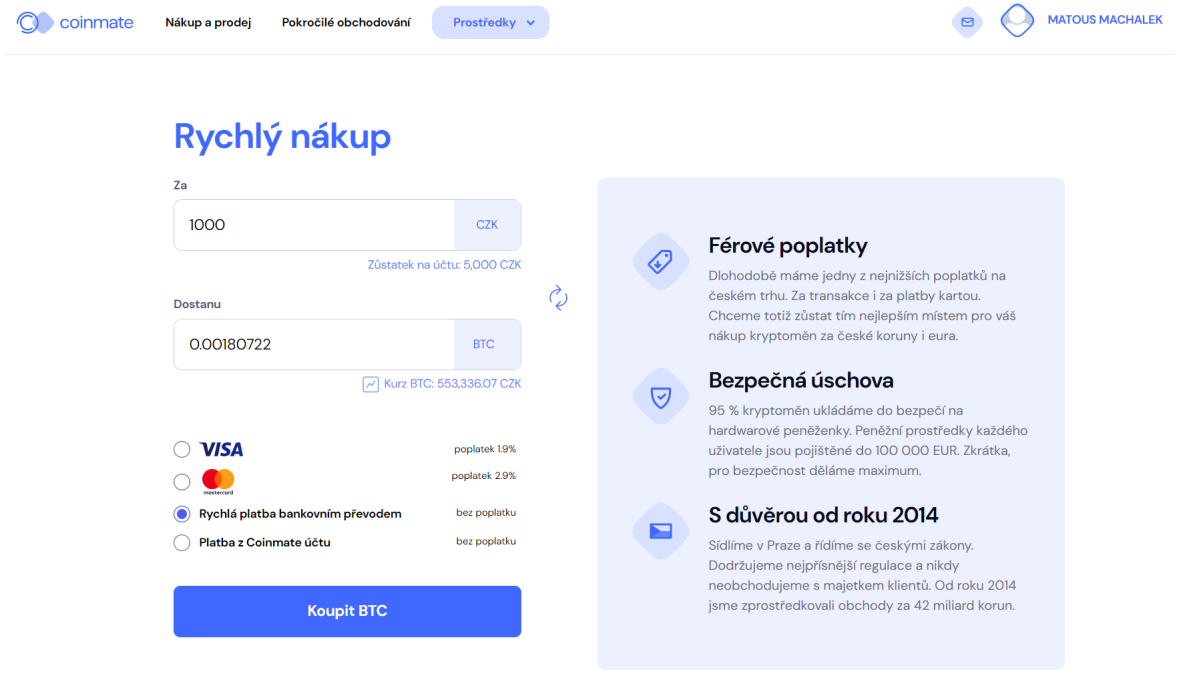
[260] Coinmate. *Home* [online]. Dostupné z: https://coinmate.io/cs

Obrázek 12 Vklad finanční prostředků na burzu Coinmate



Zdroj: Coinmate. [online]. Dostupné z: https://coinmate.io/

Obrázek 13 Rychlý nákup na burze Coinmate



Zdroj: Coinmate. [online]. Dostupné z: https://coinmate.io/

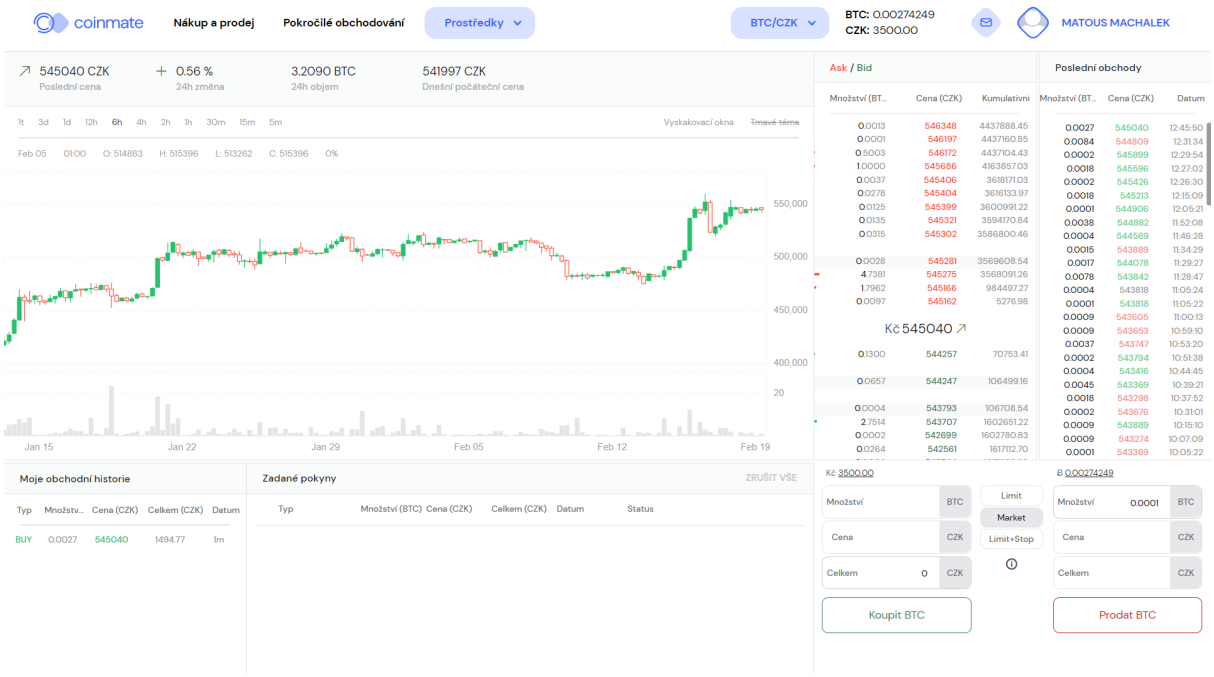
Pro nákup je možné využít sekci „Rychlý nákup“, při kterém dojde k instantnímu nákupu Bitcoinu za předem zvolenou částku v CZK při aktuálním směnném kurzu prostřednictvím platební karty, bankovního převodu či zůstatku na účtu. Prostředí rychlého nákupu na burze Coinmate je zobrazeno na obrázku 13. [261]

Výhodnějším nákupem je nákup v sekci „Pokročilé obchodování“. Zde je možné nakupovat či prodávat třemi způsoby:

- **Market order** – nákupní příkaz za aktuální tržní cenu
- **Limit order** – nákupní příkaz nastavený na uskutečnění při předem určené ceně
- **Limit + stop order** – nákupní přikaz nastavený na minimální ziskovou částku nebo maximální ztrátovou částku

Prostřední pokročilého obchodování je zobrazeno na obrázku 14.

Obrázek 14 Pokročilé obchodování na burze Coinmate



Zdroj: Coinmate. [online]. Dostupné z: https://coinmate.io/

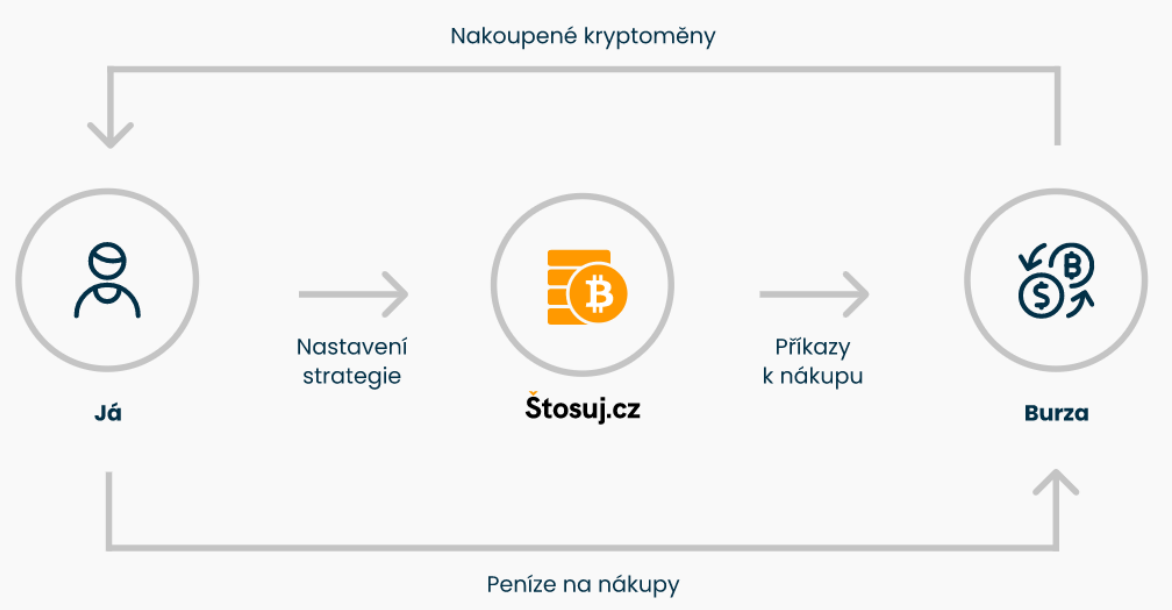
[261] Coinmate. *Home* [online]. Dostupné z: https://coinmate.io/cs

4.2.4 Pasivní nákup

Kromě aktivního nákupu, kdy je za potřebí se přihlásit do účtu burzy a provést nákup za pomocí market orderu či pravidelně nastavovat jednotlivé limit či limit stop ordery, je možné využitím „obchodních robotů“ nastavit automatické nákupu a využít tak benefity DCA metody nákupu. Některé burzy či směnárny tyto funkce přímo nabízejí ve svém prostředí, nicméně pro potřeby této práce bude využito služeb Štosuj.cz.

Štosuj.cz je český projekt, který vznikl pro automatizaci nákupní strategie DCA. Služba funguje jako samostatný nástroj, se kterým se burza pouze propojí. Finanční prostředky tak zůstávají jen na burze a služba tak pouze zajišťuje pravidelné nákupy dle provedeného nastavení. Proces je zachycen v obrázku 15.

Obrázek 15 Nákupní proces Štosuj.cz



Zdroj: Štosuj.cz [online]. Dostupné z: https://stosuj.cz/

Pro registraci je zapotřebí uvést emailovou adresu, zvolit heslo, jazyk, ve kterém bude prostředí používáno a odsouhlasit obchodní podmínky. Následně je potřeba potvrdit emailovou adresu a je možné se do účtu přihlásit. Jako první po přihlášení je nutné vytvořit propojení s burzou či směnárnou. V této práci bude Štosuj.cz propojeno s kryptoměnou burzou Coinmate, která byla vybrána na základně srovnávací analýzy nákupního prostředí.

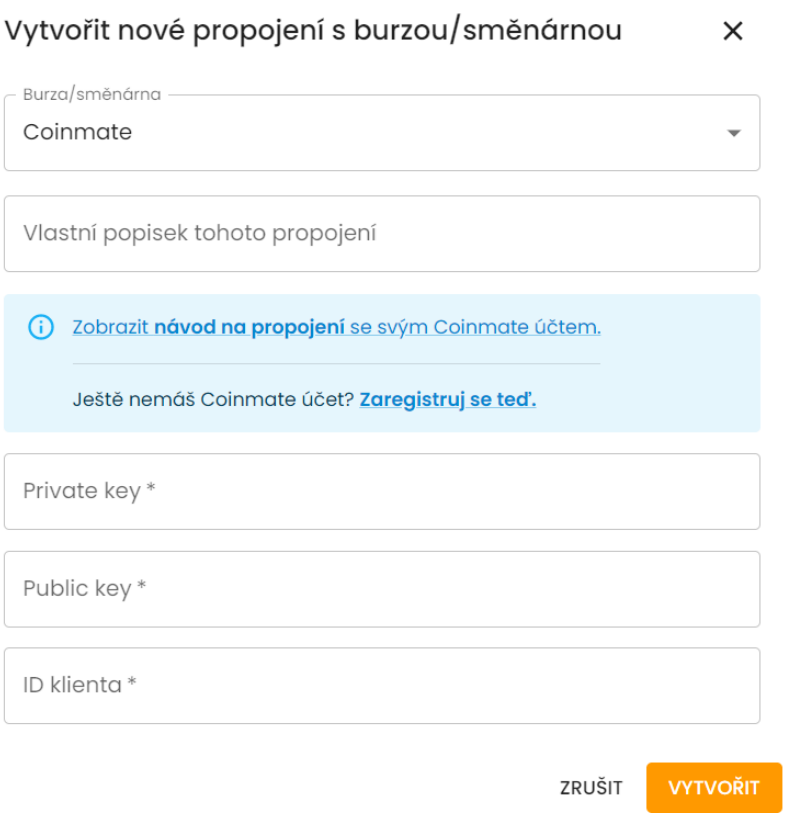
Po zvoleni burzy je potřebné zadat soukromý a veřejný klíč, společně s ID klienta. Co získání těchto informací je třeba se přihlásit do prostředí burzy Coinmate, v horním rohu

vstoupit do sekce uživatelského profilu a pokračovat do sekce „API“. Zde je nutné provést následující kroky:

1. označit pole „Povolit pro obchodování“;
2. ponechat pole „Povolit pro výběry“ neoznačené;
3. libovolně si pojmenovat pole „štítek“;
4. do pole „Omezit přístup na IP adresu“ vyplnit „46.28.110.125“, což je IP adresa serveru štosuj.cz
5. pokračovat přes pole „Generovat nový klíč“;
6. nyní z aplikace Google Authenticator vložit vygenerovaný kód;
7. následně se vygeneruje soukromý klíč, veřejný klíč a ID klienta, jenž je nutné zapsat do prostředí Štosuj.cz a celý proces dokončit přes polem „vytvořit“.[262]

Prostředí propojení Štosuj s burzou je zachyceno v obrázku 16.

Obrázek 16 Propojení Štosuj s burzou



Zdroj: Štosuj.cz [online]. Dostupné z: https://stosuj.cz/

[262] Štosuj.cz. *Můj přehled* [online]. Dostupné z: https://stosuj.cz/dashboard

Nyní je již možné nastavit automatické nákupy a využít tak benefitů metody DCA. Pro úspěšné provedení nákupů je nutné mít na účtu Coinmate vložené finanční prostředky, které zle vložit na burzu Coinmate i přímo z prostředí Štosuj.cz. Prostředky budou stále uloženy pouze na účtu burzy.

Vytvoření pravidelného nákupu lze provézt z prostředí „Můj přehled“ přes pole „Přidat první pravidelný nákup“. Nyní je třeba vybrat burzu Coinmate, měnový pár BTC/CZK, je možné si přidat nepovinný popisek nákupního příkazu, a zvolit cílovou částku spoření. Následně je možné zvolit frekvenci nákupů na 1x za týden kde lze zvolit i určitý den v týdnu, kdy má být nákupní příkaz proveden nebo nákup 1x měsíčně. Tyto frekvence nákupů jsou k dispozici pro neplacenou verzi učtu, v případě placené verze je možné frekvenci nákupů zvýšit a současně získat přístup k rozšířeným funkcím. Pro nákup je možné zvolit dvě možnosti, a to market order či limit order.

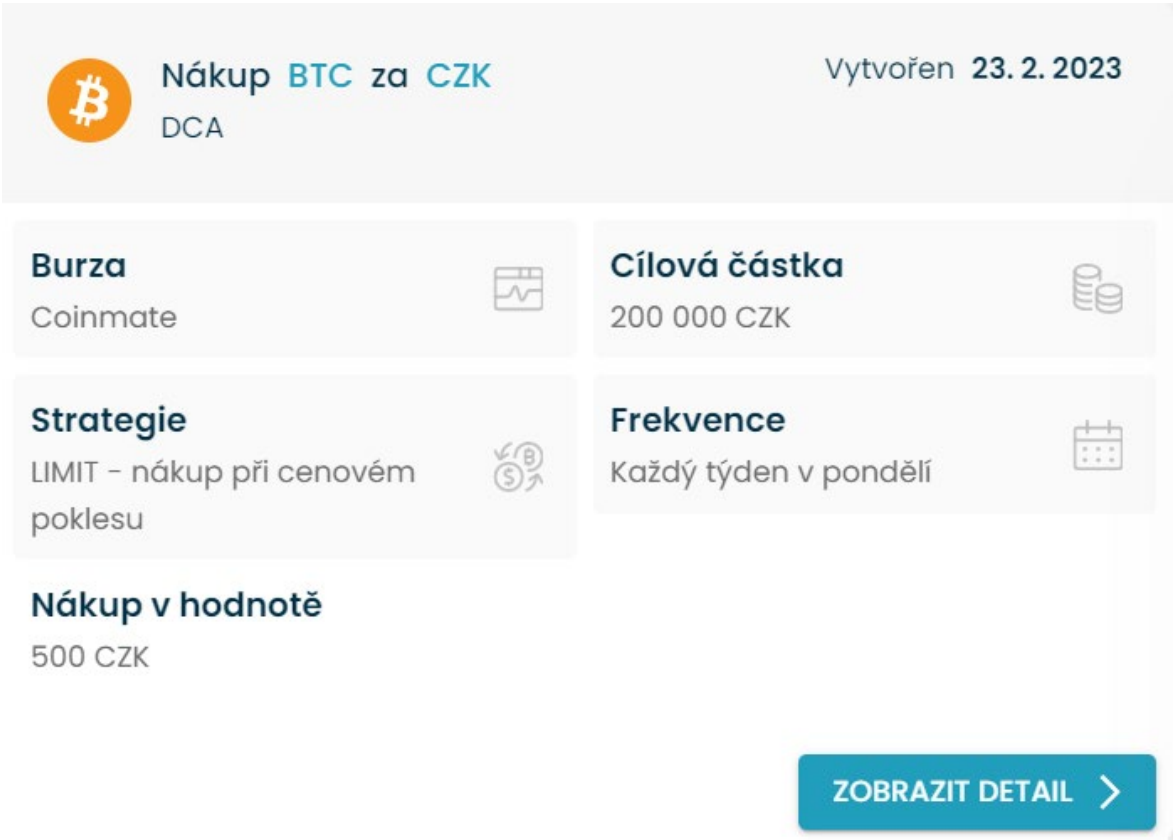
Market order je nákup za aktuální cenu. V momentu, co bude příkaz nastaven na nákup 1x za týden v pondělí, což je obecně den, kdy finanční trhy bývají cenově nejníže [263], nákup se uskuteční za aktuální cenu mezi 8 až 10 hodinou ranní. Bude se takto nakupovat každý týden v pondělí mezi 8:00-10:00 za předem nastavenou cenu, např. 500 CZK/týden.

Limit order je pokročilejší nákupní příkaz. Při tomto nákupní příkazu je možné nastavit nákup při poklesu ceny, například nákup za 500 CZK/týden při poklesu ceny BTC o 10 %. Po zadání příkazu dojde k tomu, že každé pondělí se nastaví nákupní příkaz ve vztahu k aktuální ceně a po celý týden bude příkaz čekat, zda cena klesne o nastavených 10 %. V případě, že ano, při první poklesu ceny o 10 % se uskuteční nastavený nákup. V případě, že cena za celý týden nepoklesne o předem stanovených 10 %, na konci týdne se uskuteční nákupní příkaz za aktuální cenu a následně se automaticky vytvoří nový nákupní příkaz na stejný způsob pro následující týden. [264]

Přehled nákupních orderů v prostředí Štosuj.cz je zachyceno v obrázku 17.

[263]Roklen24. *Nejhorší den a měsíc pro trhy?* [online]. Dostupné z: https://roklen24.cz/nejhorsi-den-a-mesic-pro-trhy-pozor-na-pondeli-a-zari/
[264] Štosuj.cz. *Můj přehled* [online]. Dostupné z: https://stosuj.cz/dashboard

Obrázek 17 Přehled nákupních příkazů Štosuj.cz



Zdroj: Štosuj.cz [online]. Dostupné z: https://stosuj.cz/

Minimální nákup je dle podmínek burzy Coinmate 0,0001 BTC. Za provedení nákupu přes market order si burza Coinmate účtuje poplatek ve výši 1,5 % z provedené transakce. V rámci limitní orderu je účtován poplatek ve výši 0,3 % z provedené. Market order přes burzu Coinmate je oproti jiným burzám vyšší. Například u burzy Coinbase je za market order účtován poplatek z 0,4 % z provedené transakce a v případě Binance je poplatek výši 0,1 % z provedené transakce. Nákup přes market order je tak u burzy méně výhodný v porovnání s ostatními nabízenými burzami. Naopak je však nutné brát v potaz, že u burzy Coinmate nedochází k nákladům za směnu měnového páru EUR/CZK, které vznikají díky spreadu směnného kurzu přes peněženku Revolut.

4.3 Těžba Bitcoinu

Přesto, že těžba Bitcoinu v dnešní době již není tak dostupná, jako tomu bývalo v minulých letech, kdy bylo možné Bitcoin těžit na běžném CPU stolního počítače, grafické kartě či obdobného způsobu. V dnešní době je již nutné pro těžbu Bitcoinu využitím jen a pouze specializovaný ASIC miner.

Otázkou je, zda v dnešní době existují způsoby, jak investovat do těžby Bitcoinu a profitabilně Bitcoin těžit. Princip těžby a její nepostradatelnost pro bitcoinovou síť byla vysvětlena v teoretické části práce.

Rostoucí počet těžařů v sítí pomáhá bezpečnosti a stabilnosti sítě. Pro samotné těžaře to má však opačný efekt. Více těžařů znamená, že odměna je rozdělována mezi více subjektů a tím je samozřejmě odměna nižší. Současně rostoucí obtížnost znamená, že je zapotřebí vynaložit větší výpočetní sílu, což se odráží na větší požadavcích na technologickou náročnost strojů, což vyžaduje vyšší investici a menší profitabilitu. Současné energetická krize započatá v roce 2022 nadále profitabilitu rapidně snižuje, z důvodů potřeby vynaložit větší náklady na pokrytí spotřebované energie. Důležitým faktorem v tématu profitability těžby Bitcoinu je tak i přístup k levné a bezpečné elektrické energii. Profitabilita těžby ve však nejvíce závislá na aktuální ceně Bitcoinu. V případě vysoké ceny je samozřejmé, že těžba se stává více profitabilní, nežli je při ceně nízké. V obdobích poklesu ceny se často těžba Bitcoinu stává neprofitabilní, tedy přidělené odměna za poskytnutý výpočetní výkon nepokryje vynaložené náklady na spotřebovanou energii. V tomto případě lidé často pokračují s těžbou, vytěžené bitcoiny neprodávají s důvěrou v opětovný růst ceny.[265]

Pro zjištění, zda je investice do těžby Bitcoinu v dnešní době profitabilní a do jaké míry, bude v práci popsán postup investice do těžby Bitcoinu s následnou kalkulací profitability v roce 2023.

[265] Kriptomat. *Jak funguje těžení kryptoměn* [online]. Dostupné z: https://kriptomat.io/cs/kryptomeny/co-je-to-tezba-kryptomen/

Nákup hardwarového vybavení je prvním krokem pro investici do těžby Bitcoinu. V současné době je nutné zakoupit těžební stroj nazývaný ASIC miner, který je specializovaný typ přístroje provádějící pouze specifické typy výpočetních operací. ASIC miner řeší kryptografické úlohy na algoritmu SHA-256 a specializuje se pouze a jen na nalezení nonce, díky kterému získá odměnu za uzavření bloku v podobě bitcoinů. Jedná se však o velmi hlučný a teplo produkující stroj, který není vhodný do běžné domácnosti.[266]

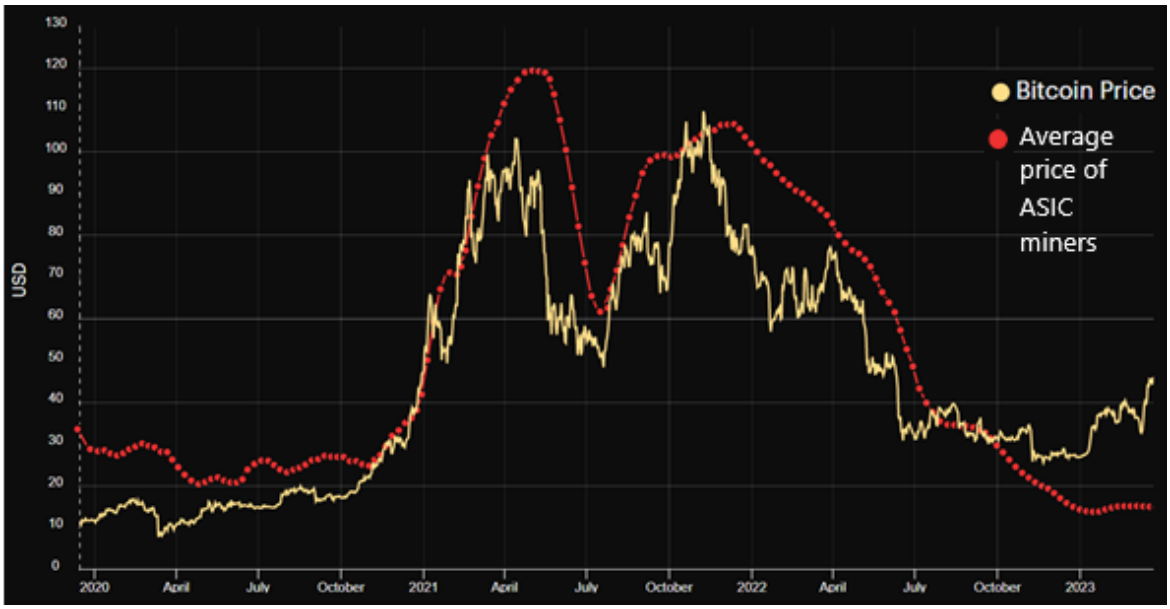
Při nákupu ASIC mineru je nutno zvážit několik faktorů:

- cena/výše investované částky;
- dostupnost;
- výkonnost;
- spotřeba elektrické energie;
- hlučnost a produkce tepla.[267]

Faktory by měly být řešeny i v tomto pořadí. Nejdříve je nutno vědět, kolik je možné na těžební stroj vynaložit finanční prostředků. Cena se odvíjí od výkonnosti, která je udávána v Th za sekundu. V současné době se vzhledem k úrovni difficulty minimální výpočetní síla pohybuje okolo 100 Th/s, vhodné jsou však stroje výkonnější. Dnes se většina ASIC minerů výkonnostně pohybuje od 96 Th/s do 255 Th/s. Pořizovací cena za jeden stroj se aktuálně pohybují od úrovně 2.000 USD až do 7.000 USD, tedy cca od 45.000 CZK do 155.000 CZK. Cena se dále odvíjí od aktuální ceny BTC. V momentu, kdy roste cena Bitcoinu, roste i cena těžebního stroje, který splňuje aktuální technické parametry. Růst a pád ceny těžebního hardwaru k ceně Bitcoinu je zachycen v grafu 10, který vypovídá o tom, že ASIC minery, které dříve stávaly kolem 10.000 USD za kus se v dnešní době pohybují kolem 3.000 USD za stroj.

[266] Finex. *Jak se těží bitcoin? Co je těžba bitcoinu a jak funguje?* [online]. Dostupné z: https://finex.cz/jak-se-tezi-bitcoin-co-je-to-tezba-bitcoinu-a-jak-funguje/
[267] Finex. *Jak se těží bitcoin? Co je těžba bitcoinu a jak funguje?* [online]. Dostupné z: https://finex.cz/jak-se-tezi-bitcoin-co-je-to-tezba-bitcoinu-a-jak-funguje/

Graf 10 Vývoj ceny ASIC minerů k ceně Bitcoinu



Zdroj: Hashrate Index. *ASIC Index data* [online]. Dostupné z: https://data.hashrateindex.com/asic-index-data

V rámci dostupnosti se situace výrazně zlepšila. Při vyšších cenách Bitcoinu v „bull runu“ mezi rokem 2021 a 2022 byly ASIC minery téměř nedostupné. Ty, které stále byly k dispozici, byly za velmi vysoké cenovky. Těžební stroje bylo možné pořídit pouze od přeprodávajících společností, nikoliv přímo od výrobce, který těžební stroje běžně prodával. Tímto vznikal velký problém důvěry, vzhledem k tomu, že za stroje bylo často vyžadováno zaplatit přímo v Bitcoinu a spousta kupujících se tak setkala s podvodnými praktikami. Nyní je možné stroje zakoupit přímo od výrobce či od důvěryhodných prodejců za zlomkové ceny ceny.

Spotřeba elektrické energie se pohybuje přibližně od 19 W/Th u ASIC minérů, které jsou efektivnější v rámci spotřeby elektrické energie na vyprodukovaný Th výpočetního výkonu až do 35 W/Th u méně efektivních těžebních strojů. Celková spotřeba těžební stroje se tak pohybuje od 3.000 W do 5.500 W.

Velkým faktorem v otázce těžby Bitcoinu v prostředí domova je hlučnost. Ta si často vyžaduje uložení stroje do skladovacích prostorů domu, odhlučněných místností či těžbě z domova zamezuje. Obvykle se jedná o hlučnost začínající na hodnotách od 45 dB, která roste až k hodnotě 85 dB. Hlasitost způsobují silné chladicí ventilátory, které odvádí teplo vzniklé z provozuj stroje, přesněji z čipových desek, které pracují 24 hodin denně. Těžební stroj se tedy pracuje každý den 24 hodin, proto je nutné s konstantní hlučností a přísunem

tepla počítat. Dnes již začínají vznikat stroje, které odvádí teplo na základě vodního chlazení, u kterých tak problém hlučnosti a přebytečného tepla významně klesl.

Za použití srovnání výkonnosti ASIC minerů, které je zachyceno v obrázku 18 s využitím doposud získaných informací, bude v této práci postupováno pro investici do těžby Bitcoinu s ASIC minerem názvem Antminer S19j Pro+ od výrobce Bitmain. Tento ASIC miner je v současné době dostupný k pořízení. Antminer S19j Pro+ byl vydán v prosinci roku 2022, jedná se tedy o jeden z nejnovějším modelů a nehrozí tak jeho technologická zastaralost. S výkonností 122 TH/s se jedná o dostatečně výkonný stroj pro potřeby domácí těžby Bitcoinu, se celkovou spotřebou 3355W a efektivností 27,5 spotřebovaných W na vyprodukovaný TH výpočetního výkonu. Denní příjem stroje je vyčíslen na 8,4 USD za den při aktuální cenách Bitcoinu pohybujících se okolo úrovně 25.000 USD/BTC. Srovnání výkonnosti ASIC minerů z obrázku 18 vypovídá o denní profitabilitě 3,6 USD/den, nicméně tato hodnota se musí dále propočítat dle aktuální ceny elektrické energie na území České republiky.[268]

Obrázek 18 Srovnání výkonnosti ASIC minerů

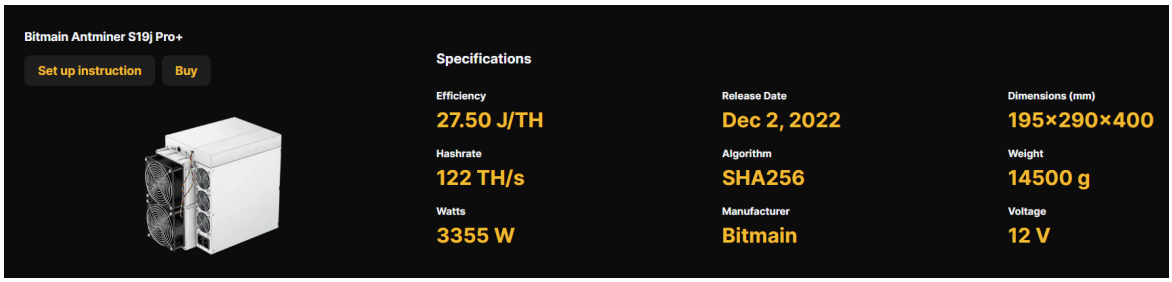
#	Model	Release Date	Hashrate	Watts	Efficiency	Daily Revenue	Daily Profit	Operating Margin
1	Antminer S19j Pro+ SHA256	Dec 2022	122 TH/s	3355 W	27.5 W/TH	$8.4/day	$3.6/day	42.4%
2	Whatsminer M50S+ SHA256	Dec 2022	136 TH/s	3264 W	24.0 W/TH	$9.4/day	$4.7/day	49.8%
3	Avalon A1366 SHA256	Oct 2022	130 TH/s	3250 W	25.0 W/TH	$9.0/day	$4.3/day	47.7%
4	Avalon A1346 SHA256	Oct 2022	110 TH/s	3300 W	30.0 W/TH	$7.6/day	$2.8/day	37.2%
5	Antminer Ka3 SHA256	Sep 2022	166 TH/s	3154 W	19.0 W/TH	$11.4/day	$6.9/day	60.2%
6	Antminer T19 Hydro SHA256	Jun 2022	145 TH/s	5438 W	37.5 W/TH	$10.0/day	$2.2/day	21.5%
7	Whatsminer M50S SHA256	Apr 2022	126 TH/s	3276 W	26.0 W/TH	$8.7/day	$4.0/day	45.6%
8	Whatsminer M53 SHA256	Apr 2022	226 TH/s	6554 W	29.0 W/TH	$15.6/day	$6.1/day	39.3%
9	Whatsminer M50 SHA256	Apr 2022	114 TH/s	3306 W	29.0 W/TH	$7.8/day	$3.1/day	39.3%
10	Avalonminer 1266 SHA256	Apr 2022	100 TH/s	3500 W	35.0 W/TH	$6.9/day	$1.8/day	26.8%

Zdroj: Hashrate Index. *Rigs* [online]. Dostupné z: https://hashrateindex.com/rigs

[268] Hashrate Index. *ASIC Rigs* [online]. Dostupné z: https://hashrateindex.com/rigs

ASIC miner Antminer S19j Pro+ je možné pořídit na vyžádání přímo od výrobce Bitmain z Číny za 2.379 USD bez DPH, cla a dopravy[269] nebo od prodejce z Evropy za 3.386 EUR včetně DPH a cla. Specifikace ASIC mineru Antminer S19j Pro+ je zobrazeno v obrázku 19. [270]

Obrázek 19 Specifikace parametrů ASIC mineru Antminer S19j Pro+



Zdroj: Hashrate Index [online]. Dostupné z: https://hashrateindex.com/rigs/bitmain-antminer-s19jpro+

Zakoupený ASIC miner se pro zahájení těžby musí zapojit do elektrické energie, při kterém je doporučeno používat ochranu přepětí v podobě zapojení těžebního stroje do elektrické zásuvky skrze zásuvky přepěťové ochrany. Ta v případě přepětí elektrického proudu ochrání ASIC miner před poškozením komponentů stroje. ASIC miner je následně nutné připojit k internetu za pomocí ethernetového kabelu. Následně bude možné připojit ASIC miner k těžebnímu poolu, kterému se poskytne výpočetní výkon a za kterou se dle výše poskytnutého výpočetního výkonu v TH/s získává poměrová odměna, která je pravidelně odesílána na předem nastavenou peněženku.[271] ASIC mineru obvykle trvá několik hodin od spuštění, nežli se dostane do maximálního výkonu.

Přehled těžební poolů dle jejich procentuální zastoupení na celkové těžbě Bitcoinu je zobrazen v grafu 11. Na výběr je tedy v dnešní době z více jak 15 hlavních těžebních poolů. Jednotlivé těžební pooly se liší podmínkami pro těžaře, jako je například výše poplatků v % ze získané odměny či frekventovanost vyplácení odměn.

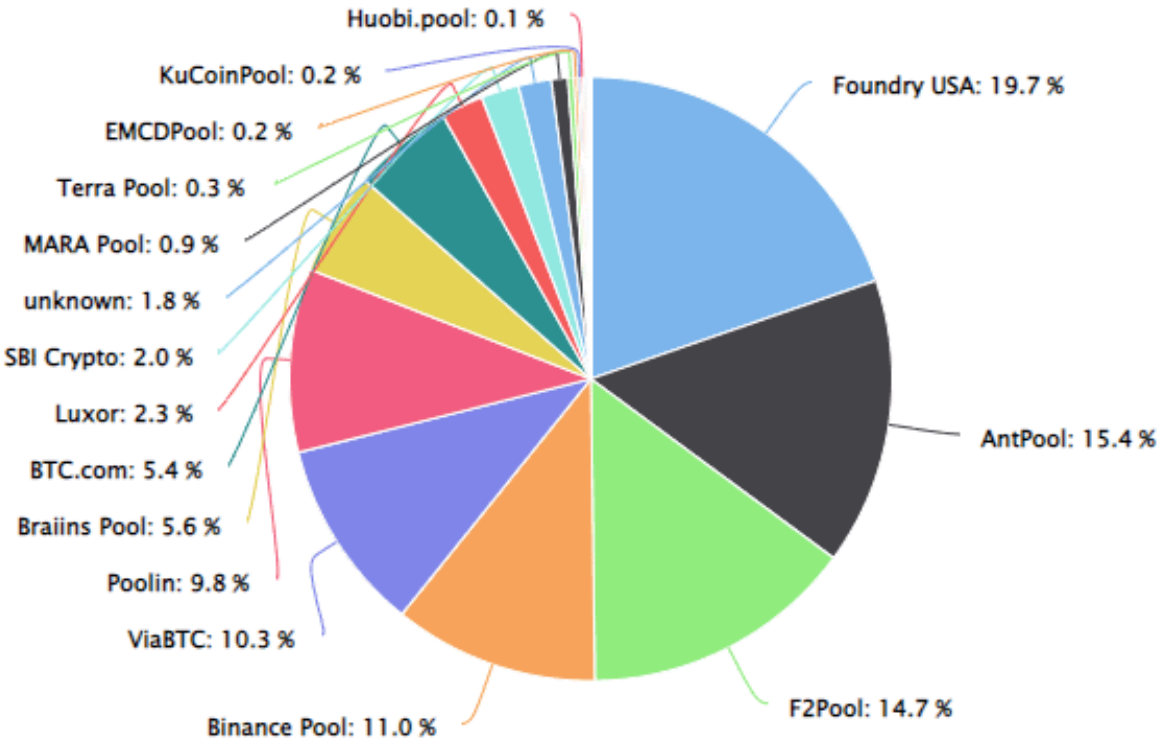
Bez připojení na těžební pool již v dnešní době není možné těžit. I přesto, že je specializovaný ASIC miner výkonným strojem, v případě, že by nebyl připojen do těžebního

[269] Bitmain. *Bitcoin miner S19J Pro+* [online]. Dostupné z: https://shop.bitmain.com/product/detail?pid=00020230108213609854b369SGwI0654
[270] Antminer Distribution Europe. *Antminer S19J Pro+* [online]. Dostupné z: https://www.antminerdistribution.com/antminer-s19j-pro-2/
[271] Finex. *Jak se těží bitcoin? Co je těžba bitcoinu a jak funguje?* [online]. Dostupné z: https://finex.cz/jak-se-tezi-bitcoin-co-je-to-tezba-bitcoinu-a-jak-funguje/

poolu, soutěžil by se všemi ostatními pooly o to, kdo dřív uzavře blok a získá odměnu za jeho uzavření v podobě bitcoinů. Pravděpodobnost, že by tento scénář nastal je tak minimální.

Nežli se v práci přistoupí k samotnému výběru nejhodnějšího těžebního poolu, je nutné zjistit, zda je těžba vůbec profitabilní a zda se tak vyplatí v investici do těžby Bitcoinu postupovat.

Graf 11 Přehled těžebních poolů dle velikost



Zdroj: Finex. *Těžba* [online]. Dostupné z: https://finex.cz/rubrika/kryptomeny/tezba/

Úroveň hash rate je velký faktorem v otázka profitability těžby. Vzhledem k tomu, že úroveň hash rate vypovídá a výši zapojené výpočetní síty do bitcoinové sítě pro těžbu Bitcoinu a validaci transakcí, znamená tak pro těžaře v podstatě výši konkurence. V případě zvýšení výpočetního výkonu zapojeného do sítě se úroveň hash rate se zvýší, vzhledem k tomu, že jednotlivé bloky nemohou být vytěženy jinak rychleji. Standardní doba mezi jednotlivými vytěženými bloky 10 minut, která je nastavena pro bitcoinovou síť, musí být

zachována. Pro zajištění této rovnováhy se na základně úrovně hash rate stanoví úroveň diffuculty. Hash rate tak v podstatě nepřímo ovlivňuje profitabilitu těžby.[272]

Tato úroveň ve se i přes pokles ceny pohybuje na nejvyšších úrovních, tedy okolo 350 EH/s. Vývoj úrovně hash rate je za posledních 5 let je zachycen v grafu 12.

Graf 12 Vývoj úrovně hash rate

Zdroj: YCharts. *Těžba*[online]. Dostupné z: https://ycharts.com/indicators/bitcoin_network_hash_rate

Úroveň difficulty je tedy dalším faktorem, který poznamenal profitabilitu těžby Bitcoinu. Úroveň difficulty je hodnota, která vykazuje, jak náročná je těžba Bitcoinu, tedy jak těžké je získat odměnu v podobě bitcoinů. Vyšší úrovně difficulty tedy obvykle znamenají nižší odměnu za poskytnutý výpočetní výkon do bitcoinové sítě. Co je však pozitivní pro běžného uživatele sítě je to, že s růstem úrovně hash rate a úrovně difficulty roste i celková bezpečnost sítě.[273]

Z grafu 13, ve kterém je zachycen vývoj úrovně difficulty k ceně Bitcoinu je zřetelné, že úroveň difficulty neustále roste i přes stagnaci či pokles ceny Bitcoinu. Mezi současnými hodnotami a hodnotami mezi roky 2021 a 2022 je tak nyní markantní rozdíl.

Cena elektrické energie je další důležitým faktorem při investici do těžby Bitcoinu, vzhledem k velké spotřebě elektrické energie těžebním strojem. Vzhledem k energetické krizi v roce 2022-2023 ceny elektrické energie drasticky vzrostly. V grafu 14 je zachycen vývoj průměrné ceny elektrické energie pro domácnosti v České republice v měrné jednotce kWh za CZK.

---

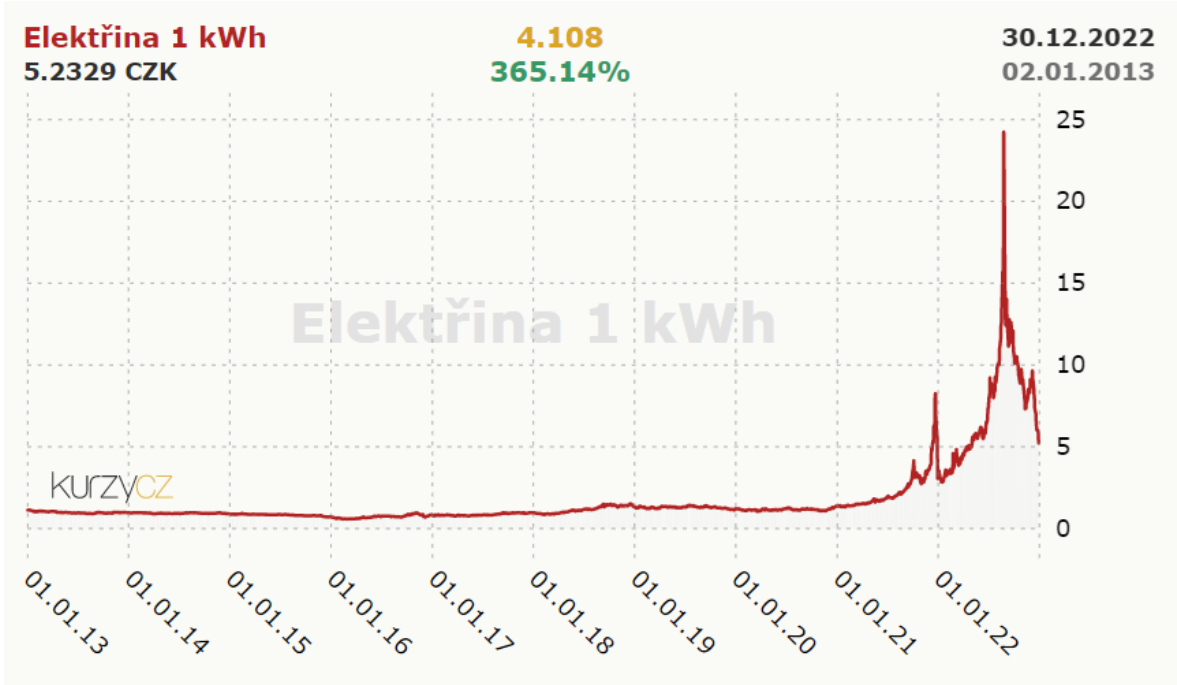
[272] SoFi Learn. *Bitcoin Hash Rate adn Why It Matters* [online]. Dostupné z: https://www.sofi.com/learn/content/bitcoin-hash-rate/

[273] Money Control [online]. Dostupné z: https://www.moneycontrol.com/europe/?url=https://www.moneycontrol.com/news/business/cryptocurrency/mining-and-hash-rate-difficulty-at-all-time-high-amid-bitcoin-slump-9100341.html

Graf 13 Vývoj úrovně difficulty k ceně Bitcoinu

Zdroj: Hashrate Index. [online]. Dostupné z: https://data.hashrateindex.com/chart/bitcoin-price-and-difficulty

Graf 14 Vývoj ceny elektřiny



Zdroj: Kurzy.cz [online]. Dostupné z: https://www.kurzy.cz/komodity/cena-elektriny-graf-vyvoje-ceny/

Vzhledem k cenám z předchozích 10 let kdy se cena 1 kWh pohybovala v průměru kolem 1 české koruny[274] s nárůsty ceny, kdy v roce 2023 se cena 1 kWh pohybuje okolo 5,8 CZK došlo k velkému zásahu pro těžbu Bitcoinu.[275] Po provedení přepočtu ceny 1 kWh z CZK na USD, že dne směnného kurzu ČNB ze dne 1.1.2023, který činil 1 USD = 22,616 by 5,8 CZK vycházelo na 0,2565 USD [276].

Pro výpočet výnosnosti tak bude použit 1 kWh = 0,26 USD. Při ceně BTC = 22.923 USD by profitabilita těžby byla v roční ztrátě 4.289,03 USD, bez započtení ceny pořízení vybraného ASIC mineru. ASIC miner by denně vytěžit bitcoiny v hodnotě 9,02 USD, nicméně by k tomu spotřeboval elektrickou energii v hodnotě 20,94 USD. Vývoj profitability těžby ASIC mineru Antminer S19j Pro+ je zachycena v grafu 15.

Graf 15 Vývoj profitability ASIC mineru Antminer S19j Pro+

Period	/day	/month	/year
Income	$9.02	$270.64	$3,247.64
Electricity	-$20.94	-$628.06	-$7,536.67
Profit	-$11.91	-$357.42	-$4,289.03

Zdroj: ASIC Miner value [online]. Dostupné z: https://www.asicminervalue.com/miners/bitmain/antminer-s19j-pro-122th

[274] Kurzy.cz. *Elektřina* [online]. Dostupné z: https://www.kurzy.cz/komodity/cena-elektriny-graf-vyvoje-ceny/1kWh-czk-1-rok?dat_field=01.01.2013&dat_field2=01.01.2023/
[275] E-on. *Kolik stojí kWh energie* [online]. Dostupné z: https://www.eon.cz/radce/zelena-energie/ceny-energie/kolik-stoji-kwh-energie/
[276] ČNB. *Kurzy devizového trhu* [online]. Dostupné z: https://www.cnb.cz/cs/financni-trhy/devizovy-trh/kurzy-devizoveho-trhu/kurzy-devizoveho-trhu/index.html?date=01.01.2023

Pro to, aby se těžba stala aspoň neztrátová, je nutné mít přístup k elektrické energii v cena okolo 0,11 USD/kWh nebo by musela cena Bitcoinu výrazně vzrůst. Rok 2023 s vysokými cenami elektrické energie a nízkou cenou ve vztahu k nejvyšší ceně Bitcoinu tak těžbě Bitcoinu nenahrává. I z tohoto důvodu jsou ceny těžebního hardwaru nižší, něž-li byly v předešlých letech. Těžba se tak běžnému uživateli v současné době nevyplatí. Musel by mít přístup k levné energii či například potřeboval zužitkovat přebytečnou elektrickou energii například ze solárních panelů. V tomto případě by se samostatná domácí těžba k nižším pořizovacím nákladům ASIC mineru vyplatila a uživatel by se mohl rozhodnout, zda do těžby je ochoten zainvestovat dle vlastního výpočtu ROI.

Nadále je třeba vzít v potaz další faktory, které by v budoucnu mohly těžbu Bitcoinu ovlivnit. Jednou z nich může být potencionální regulace, které se již v některých státech světa uplatnily, jako byla například Čína a mohly by dojít i do České republiky, i když uskutečnění tohoto scénáře není nijak pravděpodobné. Dalším faktorem může být potenciální vývoj a příchod nových těžebních ASIC minérů na trh, které by mohli být efektivnější a výkonnější nežli ty současné a navýšily by tak úroveň hash rate i úroveň difficulty. Současné úrovně hash ratu i difficulty se pohybují na značně vysoké úrovni, stejně tak i technická úroveň těžebních strojů. Z tohoto důvodu se drastický nárůst neočekává.[277] V neposlední řadě je jistý příchod halvingu, který sníží odměnu za vytěžený blok z 6,25 BTC na 3,125 BTC. Ten nastane přesně 29. dubna 2024 v 14:23:47.[278] Avšak s vyšším užíváním sítě rostou i příjmy z těžby Bitcoinu, díky tomu, že více uživatelů přináší do oběhu více bitcoinů v rámci zaplacených poplatků za transakce. S novým „bull runem“ tak může tato hodnota výrazně vzrůst.

Vzhledem k tomu, že investice do těžby Bitcoinu byla vyhodnocena jako neprofitabilní, nebude v této práci nadále k zahrnut výpočet ROI a nebude popsán proces výběru a následného připojení ASIC mineru do těžebního poolu.

[277] Hashrate Index. *10 Bitcoin Mining Predictions for 2023* [online]. Dostupné z: https://hashrateindex.com/blog/10-bitcoin-mining-predictions-for-2023/
[278] Bitcoin Block Half. *Bitcoin Block Reward Halving Countdown* [online]. Dostupné z: https://www.bitcoinblockhalf.com/

I přes to, že v současné době „domácí“ či individuální těžba není profitabilní, nemusí tomu tak být na dlouho a situace se může rychle obrátit. Pokles cen energií ve spojení s růstem ceny Bitcoinu mohou rychle situaci otočit a těžba se stane opět profitabilní. Je možné očekávat, že s růstem profitability těžby Bitcoinu porostou i ceny těžebních strojů. Je však nutné mít na paměti, že největší profitabilita se dostaví s místě, pro které jsou externí podmínky pro těžbu Bitcoinu nejvhodnější. České prostředí nikdy nebude nejvýhodnějším prostředím pro těžbu. Jsou státy, zejména v Asii, kde těžební stroje jsou dostupnější, za nižší pořizovací cenu, vzhledem k tomu, že se často ve stejné lokalitě vyrábí. Není tak nutné hradit náklady na dopravu, clo, daně a ceny elektrické energie jsou několikanásobně nižší. Existují i těžební místa v blízké vzdálenosti od elektrických elektráren, které spotřebovávají přebytečnou energii a mají ji tak v podstatě zadarmo.

Existuje však i jiný způsob, jak nepřímo investovat do těžby Bitcoinu prostřednictvím investice do těžební farmy, kde je možné si stroj pronajmout. Tyto farmy jsou umístěny v místě dosahu nízké ceny elektrické energie a často v chladných oblastech, aby nebylo zapotřebí využívat velké množství energie na samotné chlazení strojů při těžbě, díky tomu, že ASIC minery vždy pracují na maximální výkon. Tímto značně zvyšují svoji profitabilitu. Je tak možné si v podstatě pronajmout výpočetní výkon a nechat ji zasílat poníženou odměnu z těžby.[279]

V současné době se však těžba Bitcoinu není pro fyzickou osobu v domácím prostředí ČR profitabilní, proto se v této práci nebude nadále v investici do těžby Bitcoinu pokračovat.

[279] Kriptomat. *Jak funguje těžení kryptoměn* [online]. Dostupné z: https://kriptomat.io/cs/kryptomeny/co-je-to-tezba-kryptomen/

4.4 Uložení Bitcoinu

Jak již bylo v této práci zmíněno, nakoupené bitcoiny či satoshi není rozumné nechávat uložené na účtu burzy. V případě, že by se došlo k jakýmkoliv problémům burzy, uložené finanční prostředky se dostanou do rizika ztráty, vzhledem k tomu, že do momentu výběru prostředků je burza vlastníkem soukromých klíčů od nakoupeného bitcoinů. Nicméně není nutné vybírat své prostředky po každém menším nákupu, vzhledem k poplatku za výběr aneb poplatku těžaři za zapsání transakce do blockchainu. Jednotlivé výběry malých částek by se tak prodražily. Je tedy vhodné si stanovit určitou částku, při jejíž překročení budou bitcoiny/satoshi vybrány.

Vybíraný bitcoin je však třeba někam uložit. Od tohoto existují peněženky, kterých existuje v dnešní době několik typů:

- **mobilní peněženka** – klíč, adresy a ostatní funkce jsou spravovány v aplikace v chytrém telefonu nebo tabletu;
- **desktop peněženka** – klíč a adresy spravuje stolní počítač či notebook pomocí programu;
- **webová peněženka** – klíče a adresy jsou pod správy třetí strany na svých serverech, ke kterým se uživatel připojí za pomocí počítačového prohlížeče, či prohlížeče v telefonu nebo tabletu;
- **hardwarová peněženka** – specializované zařízení, které v momentu správy připojuje k počítači, uchovává klíče a potvrzuje transakce;
- **papírová peněženka** – soukromé a veřejné klíče jsou společně vytištěny na papír;
- **full node/bitcoinový klient** – na počítači je spuštěn klient, počítač vystupuje jako uzel bitcoinové sítě a současně slouží jako peněženka.[280]

Peněženky se mohou dělit na full client či light client. V případě full clinet peněženky dochází k práci s full node, tedy celým záznamem blockchainu. Oproti tomu light client peněženky pracují pouze s nejnutnější, maximálně zredukovanou verzí blockchainu a dochází tak k úschově pouze hlaviček bloků, tzv. SPV uzel, což je uzel pro zjednodušené ověřování plateb.

[280] KALINSKÝ, B. *Bitcoin a ti druzí.* 2018, s. 79-80

Nejčastějším dělením je však rozdělení na hot storage a cold storage nebo také označováno jako hot wallet a cold wallet. V případě hot storage se jedná o peněženku, která je připojena k internetu. V rámci bezpečnosti se jedná a více rizikovou variantu, vzhledem k tomu, že online připojení peněženky může znamenat vzdálený útok, jako je prolomení hesla, využití chyb peněženek či jiný typ online útoku. Jedná se tak zejména a různé softwarové peněženky, například mobilní či desktop peněženka. Cold storage je oproti tomu zařízení, které uchovává veškeré klíče off-line, tedy bez připojení k internetu. Riziko na ztrátu uložených finanční prostředků se tak omezuje zejména na ztrátu či fyzické poškození zařízení. Do této kategorie spadají zejména hardwarové peněženky, ale může se jednat například i o peněženku v papírové podobě.[281]

Pro postup této práce bude využita hardwarová peněženka Trezor. Vzhledem k investičnímu záměru této práce a většímu objemu investovaných finančních prostředků je nutné mít investované prostředky dostatečně zabezpečeny. Hardwarová peněženka je v současně dostupný variant peněženek pro uložení Bitcoinu jednoznačně nejbezpečnější. Nejvhodnější variantou hardwarové peněženky je dle aktuálního trhu varianta Trezor Model One, které je open-source hardwarovou peněženkou od české společnosti SatoshiLabs, jenž byla vůbec první hardwarovou peněženkou na světě. Tato peněženka je možná zakoupit za pořizovací cenu 1.694 CZK přímo na stránkách Trezor.io a jedná se tak o levnější variantu hardwarové peněženky společnosti Trezor, které je díky plné podpoře Bitcoinu vhodnou variantou.

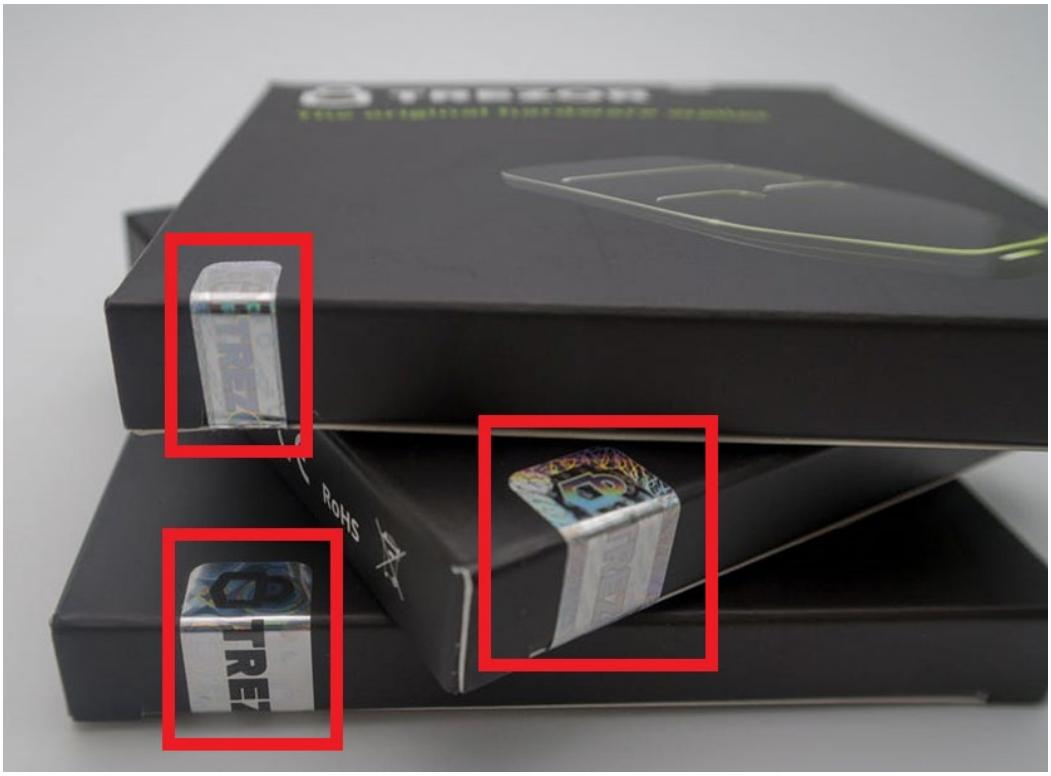
Po zakoupení peněženky Trezor je nutné postupovat dle jednotlivých kroků pro nastavení Trezoru.[282]

Nastavení Trezoru:

1. Po zakoupení zařízení je v jako první nutné zkontrolovat neporušenost balení, které je zajištěno za pomocí holografické nálepky, která nesmí být porušena. Ta zaručuje, že zařízení doposud nebylo použito nikým jiným a je tak garantována plná bezpečnost, jak je vyznačeno na obrázku 20.

[281] KALINSKÝ, B. *Bitcoin a ti druzí.* 2018, s. 79-80
[282] Trezor. *Trezor Model One* [online]. Dostupné z: https://trezor.io/trezor-model-one

Obrázek 20 Neporušená holografická nálepka Trezoru



Zdroj: Trezor [online]. Dostupné z: https://blog.trezor.io/trezor-one-tamper-evident-packaging-f98d3f63569d

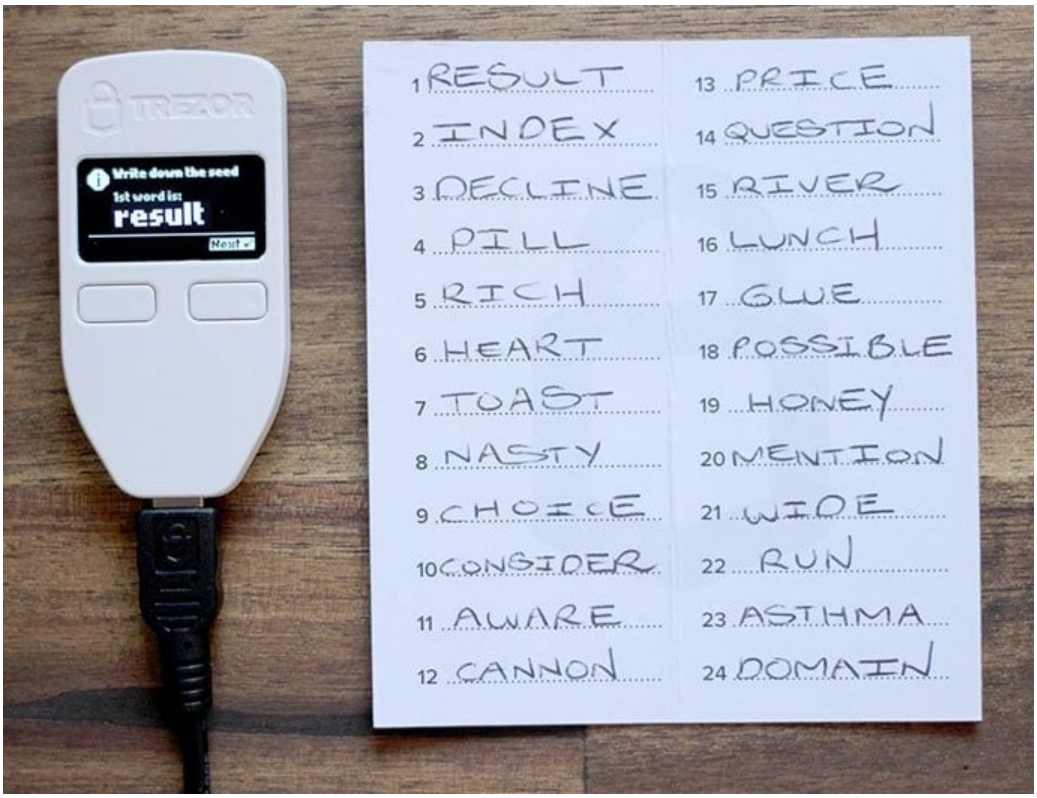
2. V následujícím kroku je zařízení nutné připojit k počítači za pomocí USB kabelu, který je součást zakoupeného balení. Zařízení na obrazovce odkazuje na stánku trezor.io/start pro první nastavení Trezoru. Zde je nutné vybrat variantu Trezoru One.
3. Pro komunikaci se softwarem Trezor využívá program Trezor Bridge, který je nabídnut k automatickému stažení. Pro dokončení je nutné vybrat operační program počítače a výběr potvrdit. Po dokončení instalace je uživatel vyzván k odpojení a opětovnému zapojení zařízení.
4. Nyní je možné postupovat v nastavení rozhraní buď to na webovém prohlížeči nebo za využití desktopové aplikaci Trezor Suite. V případě, že se bude pokračovat s prostředí aplikace Trezor Suite, aplikaci je nutné stáhnout a nainstalovat.
5. V následujícím kroku je nutné stáhnout a nainstalovat firmware. K této instalaci zařízení uživatele přímo navede. Důvodem této instalace je, že nový Trezor se

vždy prodává s resetovaným firmwarem. Následuje opětovné odpojení a zapojení zařízení pro dokončení tohoto kroku.

6. V dalším kroku je z nabízené možnosti nutné vybrat variantu nového nařízení, vzhledem k tomu, že jde o prvotní nastavení nového zařízení. Varianta obnovy starého zařízení, která je uživateli také nabízena, je možnost pro obnovení ztraceného nebo poničeného zařízení.
7. Pokračuje se v zabezpečení zařízení za pomocí vytvoření seedu. Jedná se o nejdůležitější krok, který vyžaduje největší pozornost. Seed funguje jako záloha peněženky v případě ztráty či zničení zařízení. Seed bude vygenerovaný systémem ve formě 24 náhodných anglických slov, u kterých je důležité jejich pořadí. Vzhledem k tomu, že seedem je možné získat přístup k uloženým bitcoinům, je nutné dodržovat několik pravidel:
   - seed se nikdy nesmí fotit či jiným způsobem uchovávat v digitální podobě;
   - seed nesmí být zapsán na počítači, tabletu, telefonu či jiném zařízení;
   - seed nesmí být nahrát na cloudové uložiště;
   - seed se nesmí nahrávat na internet či posílat prostřednictvím zprávy či emailu.

   Pro zapsání seedu jsou k dispozici dvě papírové karty, které byly součástí balení Trezoru. Seed je nutné na papírové kartičky zapsat, slovo po slovu. Při zápisu slov je nutné dodržovat jejich pořadí. Proházení slov by znamenalo nesprávně zadaný seed v případě obnovy zařízení. Po dokončení opisu všech 24 slov následuje kontrola. Seed je vhodné opsat minimálně 2x, z tohoto důvodu jsou přiložené papírové karty dvě. Jednu kartu je možné uschovat u zařízení, v případě potřeby aktualizace, obnovy či jiné práce se zařízením. Druhý opsaný seed, tedy druhou papírovou kartu je vhodné schovat na bezpečné místo. Tato karta bude fungovat možnost poslední záchrany, nastala by jakákoliv nepříznivá situace. Seed bude využit v případě ztráty, odcizení či poničení zařízení. V dnešní době je možné zakoupit i specializované „uchovávače“ seedu, které jsou vyráběny z kovu. Zapsaný seed by tak přežil i v případě požáru či jiné nehody. Ukázka seedu společně se zařízením Trezor One je zobrazena na obrázku 21.

Obrázek 21 Ukázka seedu



Zdroj: Finex [online]. Dostupné z: https://finex.cz/co-jsou-kryptomenove-seedy-a-proc-jsou-pro-vas-dulezite/

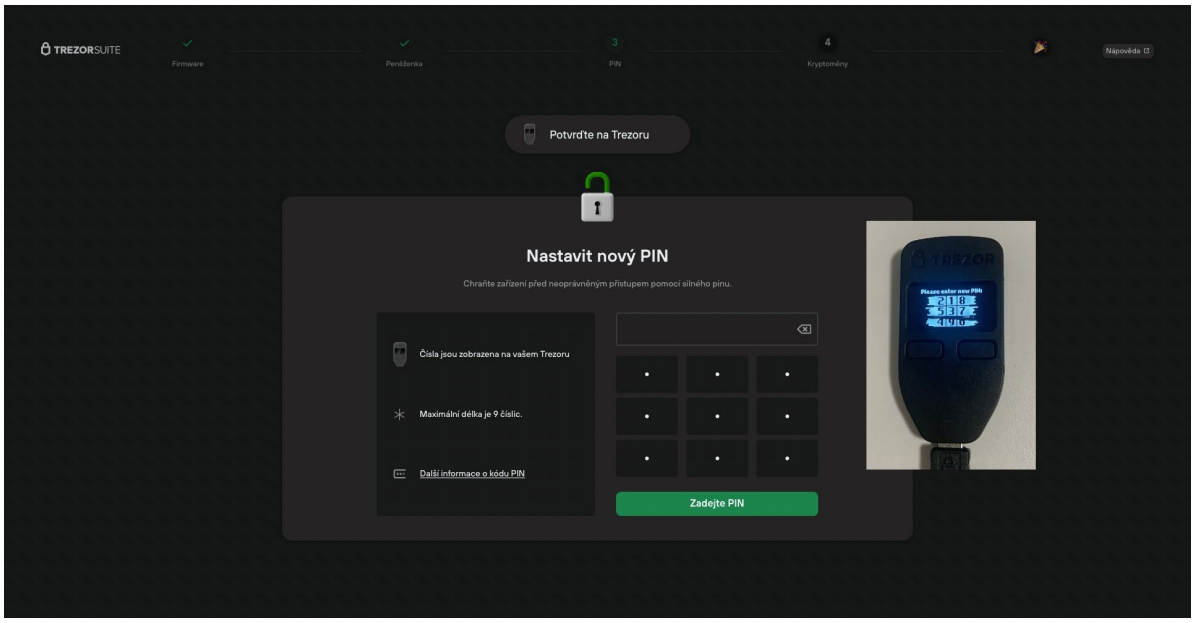
V případě, že by uživatel neměl seed správně uložený, v případě ztráty, zničení či odcizení zařízení již nikdy nebude mít možnost získat uložené bitcoiny zpět. V dnešní době je odhadováno, že zhruba 13 % celkově doposud vytěženého objemu je nenávratně ztraceno, což vychází na více než 2,5 milionu bitcoinů [283] Současně je důležité, aby se seed nedostal do rukou nikoho jiného nežli majitele zařízení. V moment, co se zmocní cizí osoba seedu, může uložené bitcoiny z Trezoru kdykoliv odcizit i v případě, že nemá přístup k samotnému zařízení.

8. Následně je nutné nastavit PIN kód zařízení o délce 4 až 9 čísel. PIN kód se vždy bude zobrazovat na display zařízení v polích 3x3 mřížky při každém přihlášení, nicméně vždy v jiném rozmístění čísel, které je poté nutné vyplnit do slepé mřížky na počítači dle skutečného rozmístění na display zařízení, jak se zachyceno v obrázku 22. Zvyšuje se tak bezpečnost přihlášení. V případě zapomenutí PIN kódu je možné zařízení obnovit do továrního nastavení a za

[283] HedgewithCrypto. *How much Bitcoin is lost forever?* [online]. Dostupné z: https://www.hedgewithcrypto.com/how-much-bitcoin-is-lost/

pomocí seedu zařízení obnovit. Ukázka zadání PINu v prostředí Trezor Suite je zachycena v obrázku 22. [284] [285]

Obrázek 22 Ukázka PINu v prostředí Trezor Suite



Zdroj: Finex [online]. Dostupné z: https://finex.cz/trezor-model-one-spusteni-navod/

Základní nastavení Trezoru je nyní zajištěné a následně je možné provést výběr Bitcoinu z burzy.

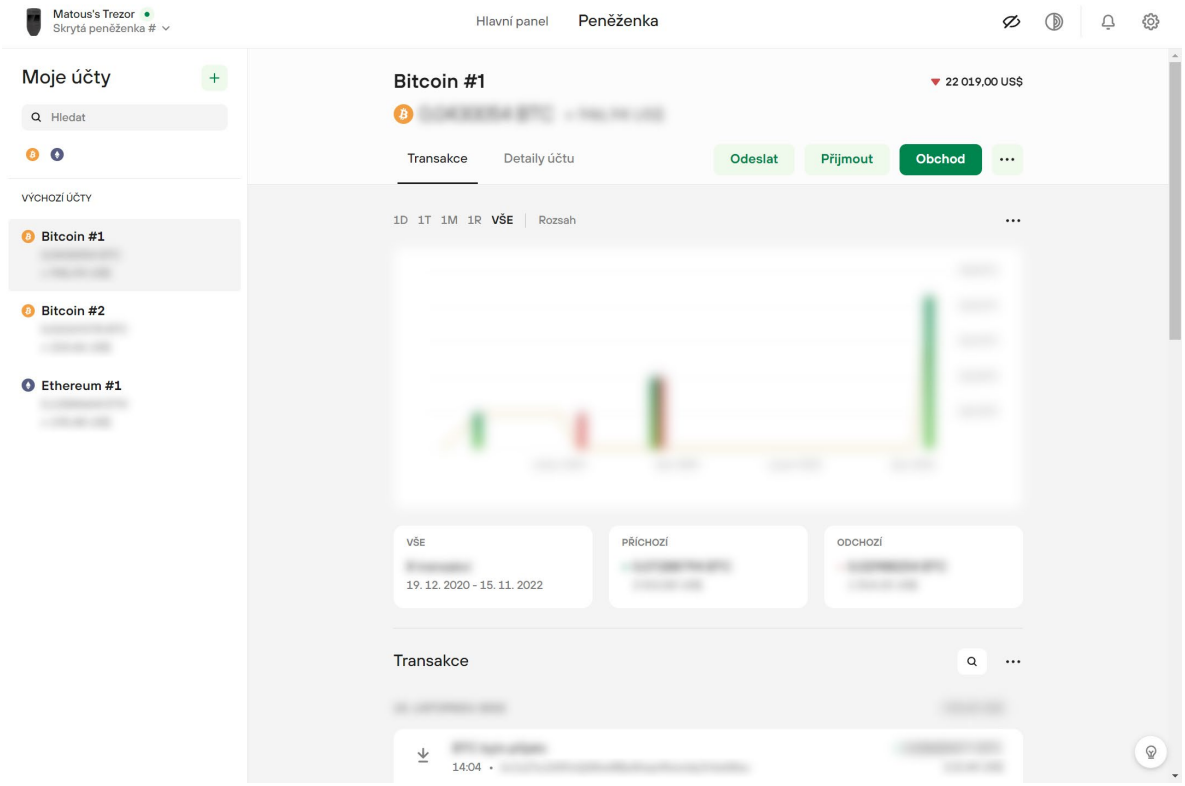
4.4.1 Výběr Bitcoinu

Nejdříve je nutné se do Trezoru přihlásit. Trezoru je zapotřebí připojit k PC přes USB kabel, otevřít aplikaci Trezor Suite, zadat PIN kód a přejít do sekce „Peněženka“. Zde je nutné otevřít peněženku pro kryptoměnu Bitcoin.

Ukázka prostředí Trezor Suite je zachycena v obrázku 23.

[284] Trezor. *Start* [online]. Dostupné z: https://trezor.io/start
[285] Finex. *Trezor Model One – Spuštění nové peněženky krok za krokem* [online]. Dostupné z: https://finex.cz/trezor-model-one-spusteni-navod/

Obrázek 23 Ukázka prostředí Trezor Suite

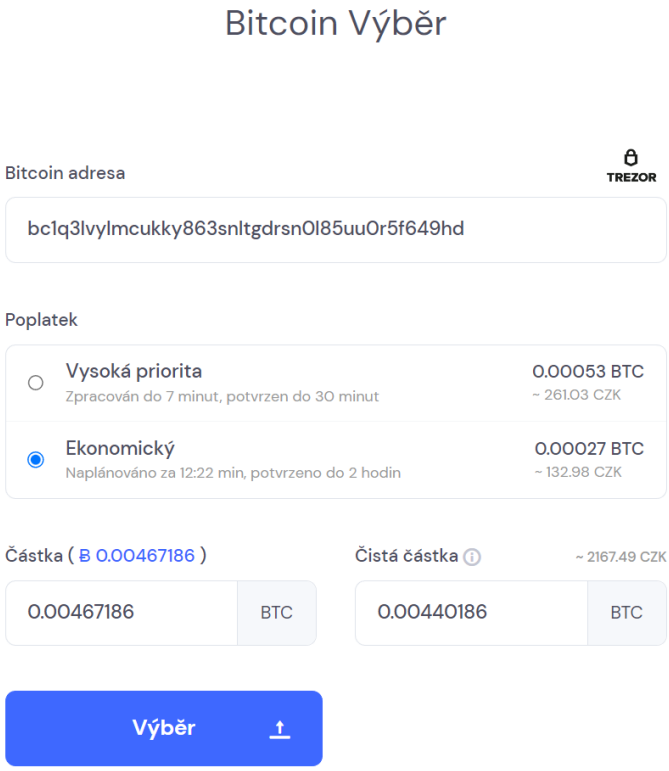


Zdroj: Trezor Suite

Následně zvolit pole „Přijmout“ a „Zobrazit celou adresu“, která se zobrazí jako QR kód a kombinace znaků, a to jak v prostředí Trezor Suite, tak i na display zařízení, kde je po vzájemné kontrole shody obou adres nutné shodu potvrdit políčkem „Confirm“.

Nyní je zapotřebí se opět přihlásit na burzu Coinmate a přejít do sekce „Výběry“. Z nabízených možností vybrat možnost „Bitcoin. Následně se opět vrátit do prostředí Trezor Suite a přes pole „Kopírovat adresu“ vložit adresu na burzu do pole „Bitcoin adresa“. Vždy je nutné bitcoinovou adresu kopírovat a následně zkontrolovat, zda každé písmeno a číslo sedí na originální adresu. Vynechá či záměna pouze jednoho znaku by znamená odeslání Bitcoinu na neplatnou adresu, a tedy trvalá ztráta prostředků. Z tohoto důvodu není rozumně adresu ručně opisovat, ale kopírovat. V dnešní době však většina prostředí pro odeslání Bitcoinu, ať již například prostředí burzy či Trezor Suite, zavedla automatickou kontrolu platnosti zadané adresy pro odeslání. Následně se zvolí druh poplatku, výše výběru a zadá se žádost o výběr přes pole „Výběr“. Pro ověření se musí zadat šesti místný kód z aplikace Google Authenticator a výběr se dokončí přes pole „Potvrdit“. Ukázka výběru Bitcoinu z burzy na Trezor je zobrazena v obrázku 24.

Obrázek 24 Ukázka výběru Bitcoinu z burzy



Zdroj: Coinmate [online]. Dostupné z: https://coinmate.io/pages/secured/withdrawal.page

Vybrané bitcoiny dorazí na Trezor dle zadané rychlosti potvrzení transakce. Často je však po několika minutách v prostředí Trezoru zobrazí nepotvrzená transakce, která čeká na potvrzení o zapsání do blockchainu. V momentu, co je transakce potvrzena, jsou prostředky plně k dispozici a výběr je dokončen. V prostředí Trezor Suite je možné s prostředky nadále pracoval, například odesílat či s nimi nadále obchodovat.[286]

Celkový proces odeslání Bitcoinu se tak může jevit pro nového uživatele jako složitá činnost, při které se může něco pokazit a dojít tak ke ztrátě bitcoinů. Nicméně proces se stává po pár odesláních pro uživatele jednoduší a zkušenější investoři tak již nemají s odesíláním vůbec žádný problém, vždy je však nutné se ujistit správnost zadané adresy. V případě investované částky nad 10.000 CZK do Bitcoinu je nutné si pořídit Trezor pro bezpečné uložení a pravidelně zakoupené bitcoiny z burzy vybírat. Minimalizuje se tak riziko ztráty investovaných prostředků.

[286] Coinmate. *Výběr* [online]. Dostupné z: https://coinmate.io/pages/secured/withdrawal.page

4.4.2 Správa portfolia

Pro správu svých nákupů a svého bitcoinového portfolia je možné využít různých portfolio trackerů. Přes ně je možné vést podrobnější evidenci o svých nákupech, transakcích, zaplacených transakčních poplatcích, investovaných sumách, výkonnosti svého porfolia, skutečného stavu a celkovou hodnotu svého investičního portfolia. Je možné tak získat celkový přehled o své investici. Záznamy jsou do budoucna užitečné při nastavení své investiční strategie, rozhodnutí pro exitovou strategii a odprodej bitcoinů či při následném zdanění zisků z prodeje Bitcoinu. Pro potřeby zdanění je možné z burzy vygenerovat přehled nákupů a prodejů.

Vedení záznamů svého portfolia je pracnější a záleží na každém investorovi, zda si chce vést takto přehledný záznam o svých investicích. Většině uživatelů postačí záznamy z burzy, kde mají kompletní přehled o svých nákupech, či záznamy o automatických nákupech ze Štosuj.cz. V prostředí Trezoru Suit je možné po přijetí zaslaných bitcoinů získat přehled o stavu svého portfolia.

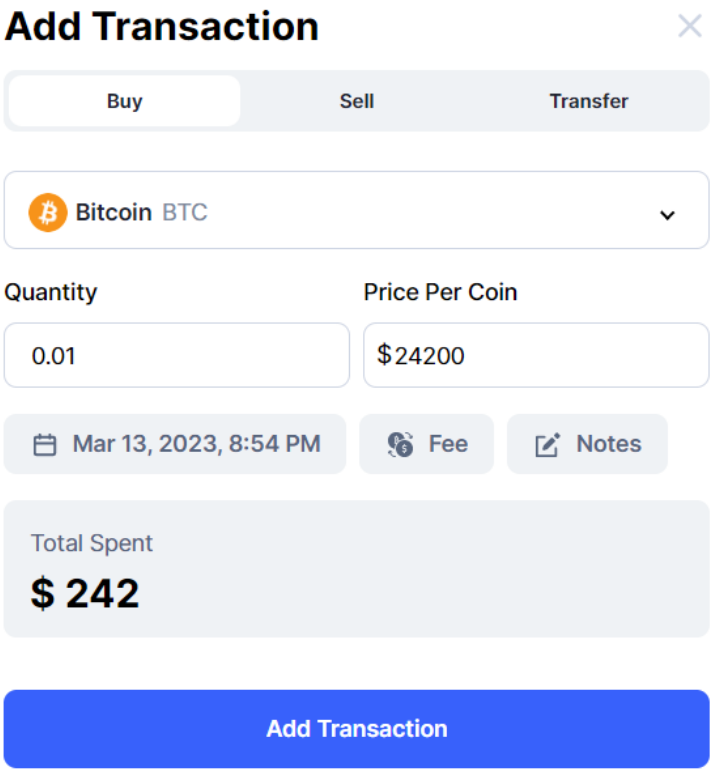
V případě využití portfolio trackeru, lze najít spousta internetových stránek či mobilních aplikacích, které nabízejí prostředí pro správu svého portfolia. Pro potřeby této práce bude zvolen portfolio tracker od CoinMarketCap, který je možné používat přes internetový prohlížeč i přes mobilní aplikaci.

Registrace a následné přihlášení na účet CoinMarketCap není nic složitého, je potřeba pouze e-mail a bezpečné heslo. Následné je možné manuálně zadávat provedené obchody, přes „Add new“ a zvolením Bitcoinu, a to jak při nákupu, tak i při prodeji. Pro zaznamenání transakce je nutné zadat objem, cenu a transakční poplatek. Následně se transakce uloží. Ukázka uložení provedené transakce do portfolia trackeru je zobrazena na obrázku 25. Vzniká tak přehledný záznam při správě svého investičního portfolia, jak je zobrazeno v obrázku 26.[287]

Jak již bylo zmíněno, vedení investičního portfolia trackeru není nutností, spíše se jedná o nadstandard. Nicméně při řádném vedení portfolio tracker dokáže poskytnout přesně a důležité informace, které se dají použít při rozhodovacím procesu či při jiném případu, je tak na každém investorovi, zda se rozhodne takto podrobnou evidenci vést.

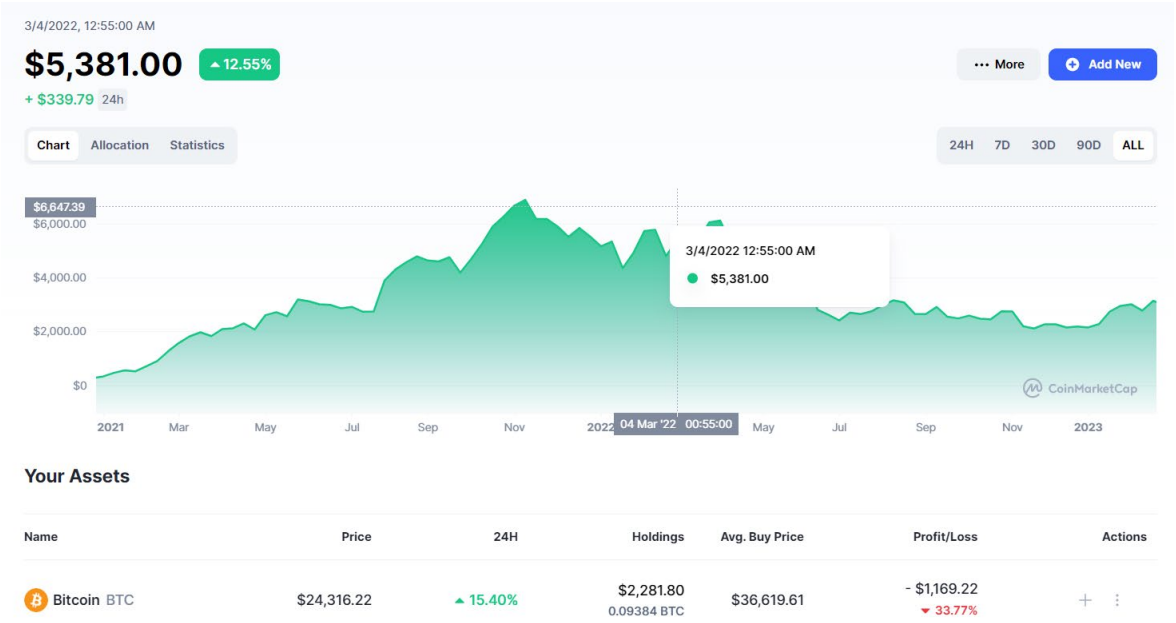
[287] CoinMarketCap. *Portfolio* [online]. Dostupné z: https://coinmarketcap.com/portfolio-tracker/

Obrázek 25 Uložení transakce do portfolia trackeru



Zdroj: CoinMarketCap [online]. Dostupné z: https://coinmarketcap.com/portfolio-tracker/

Obrázek 26 Přehled portfolia



Zdroj: CoinMarketCap [online]. Dostupné z: https://coinmarketcap.com/portfolio-tracker/

4.5 Predikce ceny Bitcoinu

Cena Bitcoinu má obecně stoupavou tendenci s určitými výkyvy. Obecně cena od svého počátku rostla nicméně s pády ceny v roce 2017, kdy pozvolný pokles pokračoval až do roku 2019. V roce 2021 Bitcoin dosáhl svého ATH a od tohoto momentu cena opět klesala. Ke dnu 13.3.2023 se cena pohybovala kolem 24.000 USD/BTC. Meziroční vývoj ceny Bitcoinu je zachycen na obrázku 27.

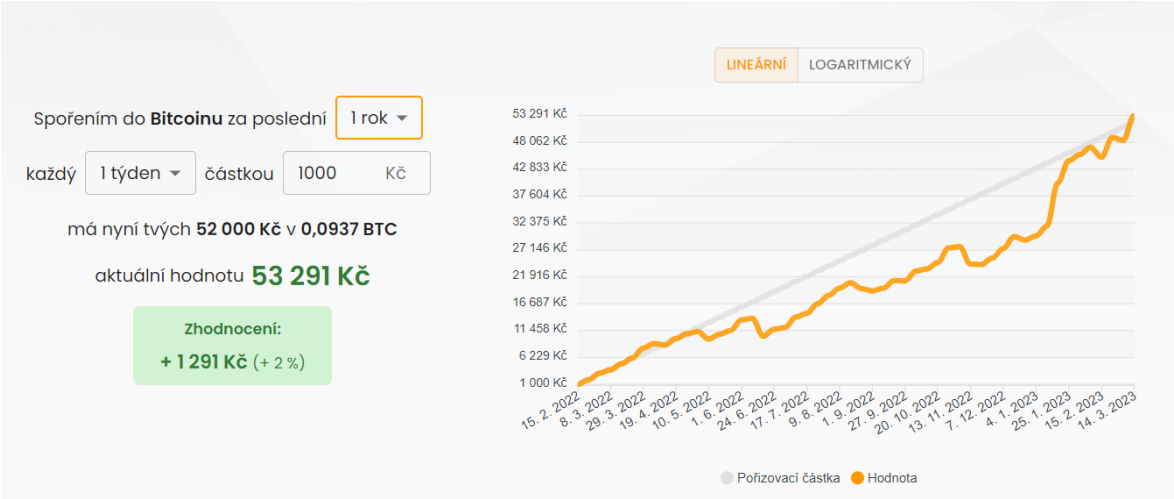
Obrázek 27 Meziroční vývoj ceny Bitcoinu

Zdroj: CoinMarketCap [online]. Dostupné https://coinmarketcap.com/currencies/bitcoin/historical-data/

Obecně se pokládá, že pro dlouhodobého investora je nejlepší investiční strategií metoda DCA. I v případě nepříznivého vývoje trhu lze pravidelnými nákupy a dostatečnou dobou držení Bitcoinu propady ceny, volatilitu a „býčí“ trhy překonat. V případě, že by investor nakupoval BTC za 1.000 CZK týdně, tedy 52.000 ročně, po dobu 1 až 5 let byly by výsledky následující:

- doba investice 1 rok, celková investice 52.000 CZK, při které došlo k 2 % zhodnocení investice, tedy zisku 1.291 CZK, vývoj je zachycen na obrázku 28;

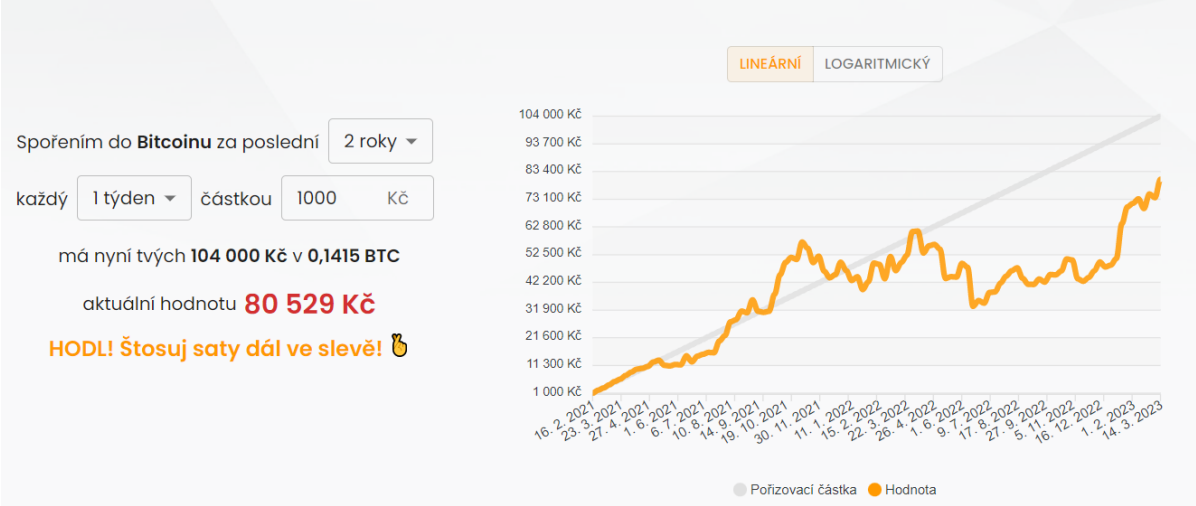
Obrázek 28 Vývoj investiční strategie DCA po dobu 1 roku



Zdroj: Štosuj.cz [online]. Dostupné z: https://stosuj.cz/

- doba investice 2 roky, celková investice 104.000 CZK, při které by došlo k nezrealizované ztrátě 80.528 CZK, vývoj je zachycen v obrázku 29;

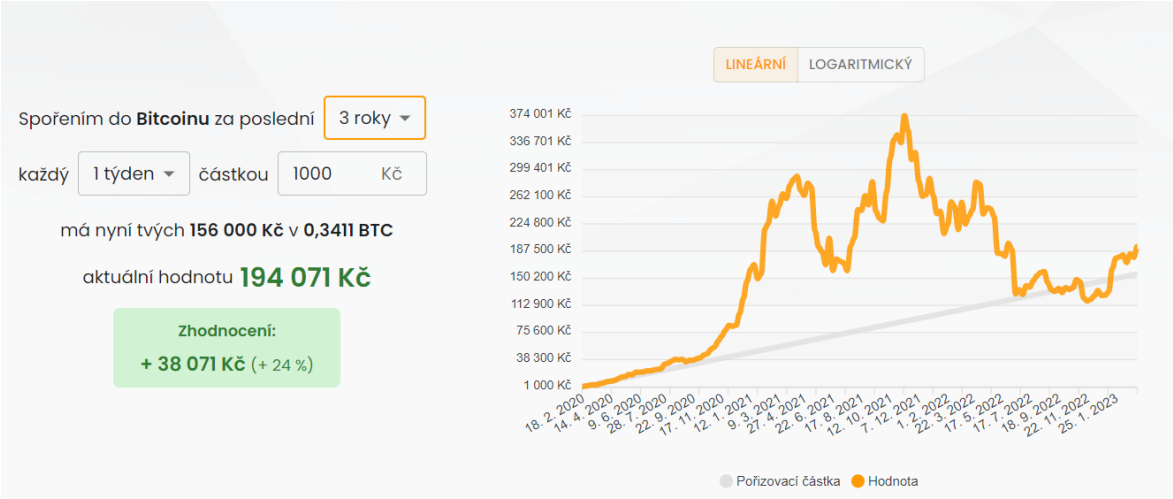
Obrázek 29 Vývoj investiční strategie DCA po dobu 2 let



Zdroj: Štosuj.cz [online]. Dostupné z: https://stosuj.cz/

- doba investice 3 roky, celková investice 156.000 CZK; při které došlo k zhodnocení investice o 24 %, tedy k 38.071 CZK zisku; vývoj je zachycen v obrázku 30;

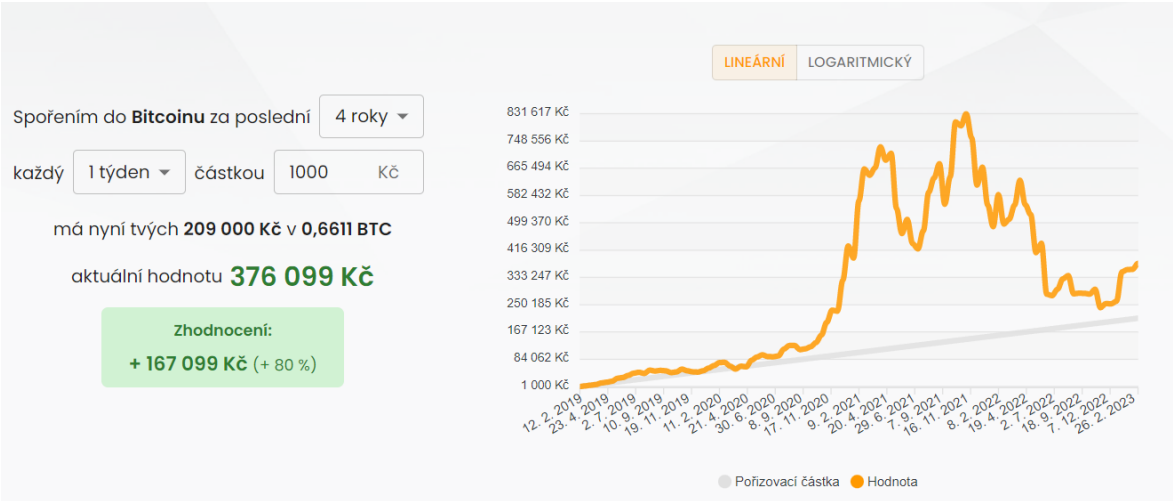
Obrázek 30 Vývoj investiční strategie DCA po dobu 3 let



Zdroj: Štosuj.cz [online]. Dostupné z: https://stosuj.cz/

- doba investice 4 roky, celková investice 209.000 CZK, při které došlo k 80 % zhodnocení investice a profitu 167.099 CZK, vývoj je zachycen v obrázku 31;

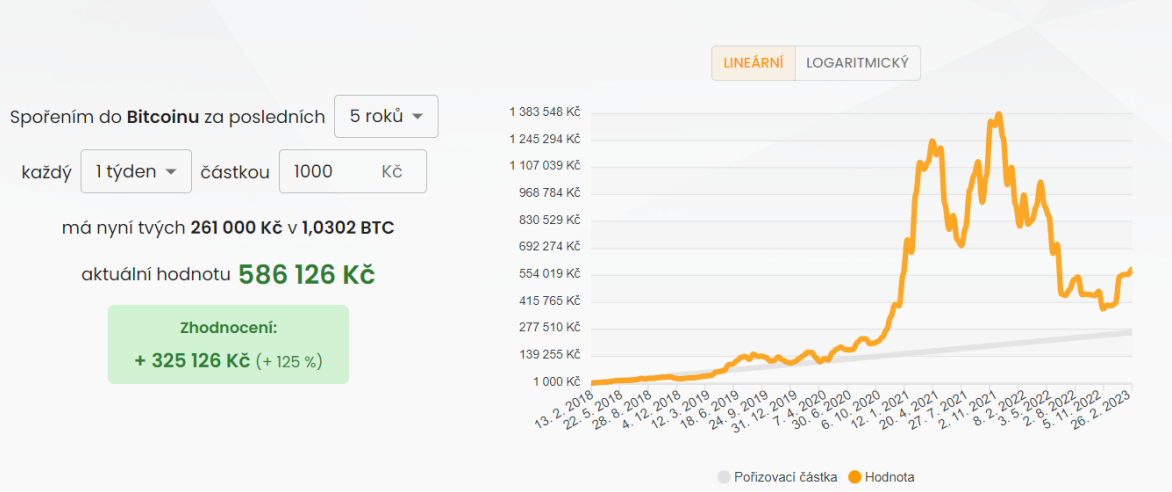
Obrázek 31 Vývoj investiční strategie DCA po dobu 4 let



Zdroj: Štosuj.cz [online]. Dostupné z: https://stosuj.cz/

- doba investice 5 let, celková investice 261.000 CZK, při které došlo k 125 % zhodnocení investice, a tedy zisku 325.126 CZK, vývoj je zachycen v obrázku 32.

Obrázek 32 Vývoj investiční strategie DCA po dobu 5 let



Zdroj: Štosuj.cz [online]. Dostupné z: https://stosuj.cz/

Dlouhodobá investice investiční strategií DCA je nesnadnější a jednou z nejefektivnějších metod investování a je doporučena jak začínajícímu investorovi, tak i tomu zkušenému. Časování trhů, kdy se investor snaží predikovat pokles ceny, je ošemetnou a nevyzpytatelnou disciplínou. I tak je možné a vhodné doplnit strategií DCA jednorázovými nákupy při dočasném poklesu ceny. V bitcoinové komunitě se označuje tato příležitost jako **„buy the dip“**. Pro predikci růstu či poklesu ceny Bitcoinu lze použít mnoho analýz, indikátorů či informací, ať již se jedná o predikci krátkodobou, střednědobou, či dlouhodobou.

Hlavní je však nestát investorem, který investuje nepravidelně a pod vlivem FOMO nakupuje bitcoiny při rostoucí ceně a následně při poklesu ceny, který přijde či později přijde, prodá své nakoupené bitcoiny se ztrátou.

4.5.1 Analýza sentimentu

Analýza tržního sentimentu je forma výzkumu, která využívá informací tržního sentimentu k predikci cenových pohybů. Sledováním dynamiky trhu s celkovými postoji účastníků je možné pochopit, proč hodnota bitcoinu roste nebo klesá. V tržním sentimentu jsou zohledněny myšlenky, pocity a nálady investorů týkající se právě Bitcoinu. Tyto pocity nemusí odrážet fundamentální vlastnosti aktiva, ale mohou významně ovlivnit cenu.

Analýza se zaměřuje spíše na předpověď ceny v krátkodobém či střednědobém horizontu. Analýza tržního sentimentu bývá součástí mnoho obchodních strategií a napomáhá v rozhodovacím procesu. Analýza může pomoci odhalit, zda FOMO na trhu je oprávněné či nikoliv. Celkově tak umožňuje získat lepší představu o krátkodobé a střednědobé cenové akci, získat lepší kontrolu nad svými emocemi a odhalit potenciál ziskové příležitosti.

Analýza mlže být v podstatě prováděna sledováním aktuální dění na trhu, zpráv z bitcoinového a kryptoměnového světa, popularitou na sociální sítích, v Google vyhledáváních a trendech.[288]

Bitcoin Fear & Greed Index je jedním z krátkodobých ukazatelů vývoje ceny. Tento index se zaměřuje na analýzu lidských emocí a sentimentu, vzhledem k tomu, jak hodně je celkový kryptoměnových trh ovlivněn emočním rozhodování lidí. Index se skládá celkově z:

- 25 % z volatility – denní analýza volatility, které se porovnávají k průměrům ceny z posledních 30 a 90 dnů;
- 25 % objem trhu a momentu – denní analýza zobchodovaných objemů porovnána k průměrům z posledních 30 a 90 dnů;
- 15 % sociální média – analýza klíčových slovech na sociálním médiích jako Twitter a jiné;
- 10 % dominance – analýza celková dominance tržní kapitalizace Bitcoinu na tržní kapitalizaci celkového kryptoměnového trhu;

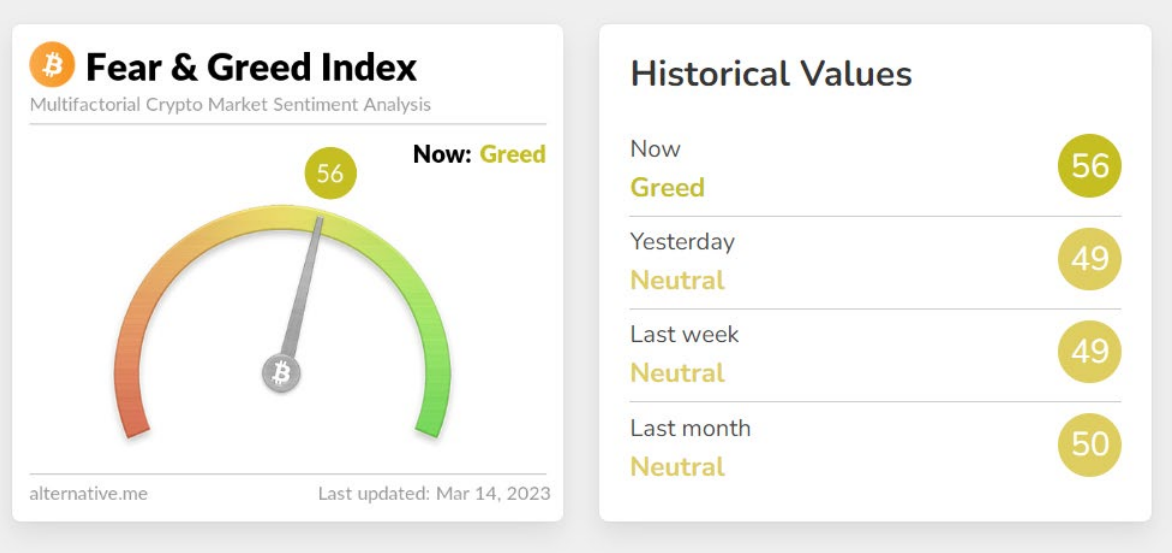
[288] Binance Academy. *Co je to sentiment na kryptoměnovém trhu?* [online]. Dostupné z: https://academy.binance.com/cs/articles/what-is-technical-analysis?UTM=BinanceAcademy

- 10 % trendy – analýza aktuálních trendů například za pomocí Google Trends, tedy denním vyhledáváním klíčových slov;
- 15 % průzkumy – ty jsou v současné době pozastaveny.

Všechny tyto faktory mohou tvořit obrázek o současném stavu Bitcoinového trhu. Index vykazuje číslo mezi 0 a 100, přičemž 0 označuje „extreme fear“, velký strach a 100 vypovídá o „extreme greed“, tedy velkou chamtivost.

Například velký růst ceny, velké zobchodované objemy, vysoká trendovost, nízká dominance a popularita na sociální médií vše vedou k růstu hodnoty indexu a tedy indikaci „greedu“. Tento fajn je spojen s FOMO a indikuje přemrštěnou aktuální cenu Bitcoinu a může predikovat přicházející korekci a ochlazení trhu. V opačném případě, kdy dochází k poklesu ceny, zobchodované objemy transakcí jsou malé, Bitcoin netrenduje a není o něm zveřejňováno mnoho informací, či jsou zveřejňované spíše negativní informace a nastupuje FUD, současně je dominance tržní kapitalizace na celkovém kryptoměnovém trhu vyšší, což přirozeně nastává při strachu spojený s pádem ceny nastává fáze „fear. Při takové fázi se mohou naskytnou zajímavé nákupní příležitosti. V následujícím obrázku je zachycen současný stav indexu Fear & Greed, který se nachází dne 14.3.2023 na úrovni 56 bodů, tedy v počáteční úrovní „greedu“. Současný stav je zachycen v obrázku 33.[289]

Obrázek 33 Fear & Greed Index

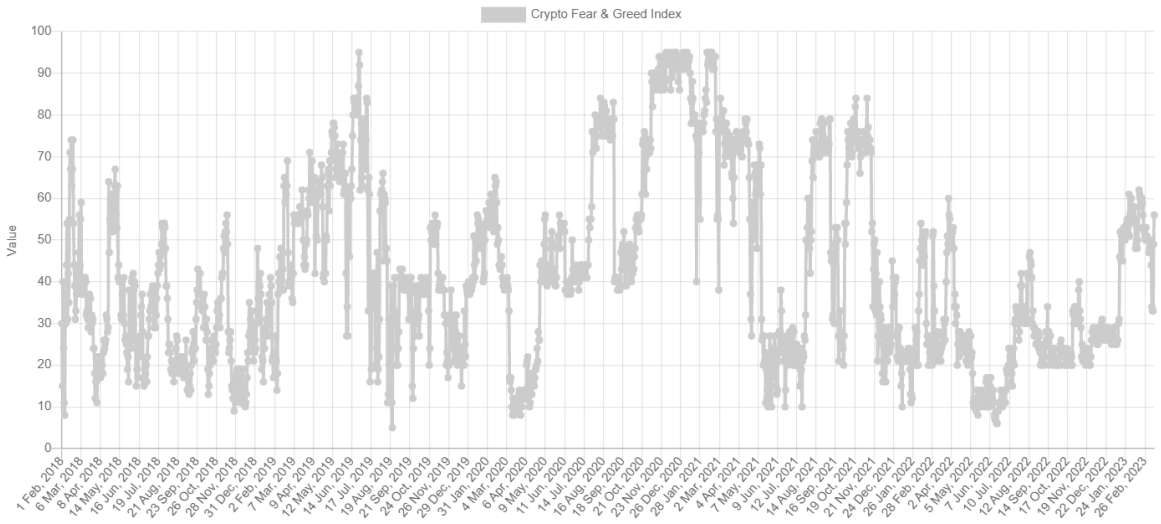


Zdroj: Alternative [online]. Dostupné z: https://alternative.me/crypto/fear-and-greed-index/

[289] Alternative. *Crypto Fear & Greed Index* [online]. Dostupné z: https://alternative.me/crypto/fear-and-greed-index/

V grafu 16 je znázorněn vývoj indexu od roku 2018.

Graf 16 Vývoj indexu Fear & Greed



Zdroj: Alternative [online]. Dostupné z: https://alternative.me/crypto/fear-and-greed-index/

4.5.2 Technická analýza

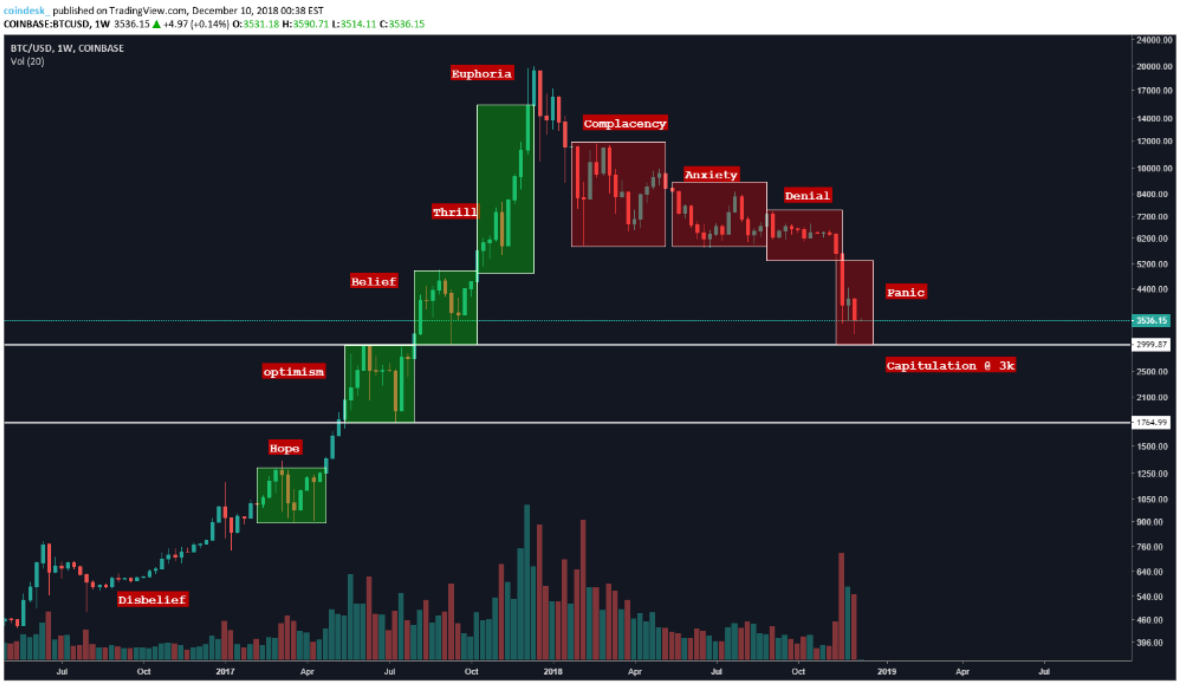
Technická analýza je druhem analýzy pracující s grafy, jejíž cílem je předpověď budoucího chování trhu na základně předchozích cenových o objemových vývojů. Technická analýza se zaměřuje výhradně na historický cenový vývoj. Z tohoto důvodu jsou zkoumána cenové výkyvy a objemová data pro identifikaci trendů a vhodné obchodní příležitosti.

Jedná se tedy v podstatě o studium současných a historických cen Bitcoinu. Hlavní předpokladem technické analýzy je, že kolísání ceny není náhodně, ale vyvíjí se dle identifikovatelných trendů. Podstatou je tedy analýza tržních sil nabídky a poptávky, které úzce souvisí s emocemi obchodníků a investorů.

Pro analýzu jsou využívány různé nástroje tvorby grafů, které se nazývají indikátory. Ty pomáhají zkoumat současnou cenu a rozpoznat vhodnou příležitost pro nákup či prodej bitcoinů. Indikátory dále napomáhají identifikovat stávající trendy a také poskytnout představu o trendech budoucích. Využívá se tedy zejména pro krátkodobé a střednědobé

cenové predikce. Ukázka technické analýzy je zachycena v grafu 16. Indikátory jsou používány na základě grafu 17.[290]

Graf 17 Idikátory technické analýzy



Zdroj: Coindesk [online]. Dostupné z: https://www.coindesk.com/markets/2018/12/11/panic-mode-what-a-wall-street-chart-tells-us-about-bitcoins-price/

4.5.3 Fundamentální analýza

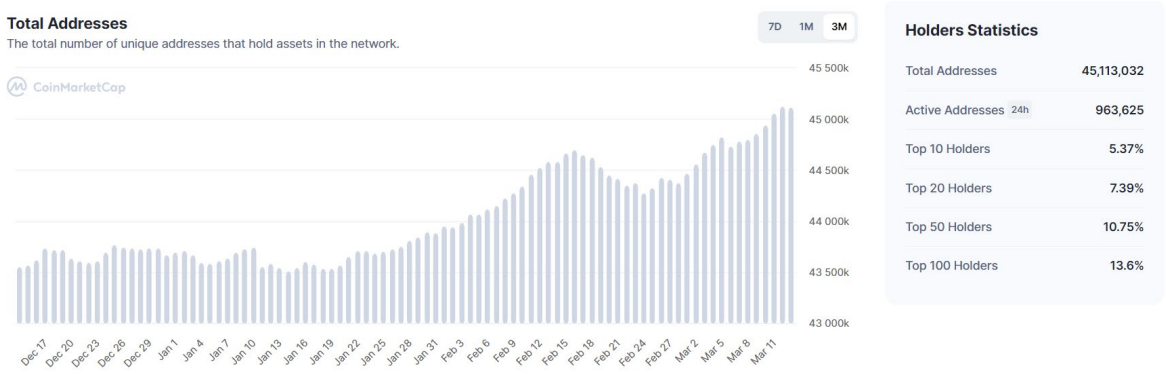
Fundamentální analýza Bitcoinu zahrnuje hloubkový rozbor dostupných informací, jako je například jeho způsob využití, počet uživatelů či tým vývojářů. Účelem je zjistit, zda je cena nadhodnocena či podhodnocena. Zaměřuje se zejména na dlouhodobou cenou predikci.

Analýza stanovuje „vnitřní hodnotu“ aktiva. Hlavním cílem je na základě vnitřních a vnějších faktorů určit adekvátnost současné cenové hladiny, což následně může být použito pro rozhodovací proces. Podstatné informace jsou získávány ze studie klíčových ukazatelů, mezi které může patřit:

[290] Binance Academy. *Co je technická analýza?* [online]. Dostupné z: https://academy.binance.com/cs/articles/what-is-technical-analysis?UTM=BinanceAcademy

- počet transakcí;
- hodnota transakce;
- uhrazené poplatky;
- úroveň hast rate;
- počet aktivních adres, které je zobrazeno v obrázku 35.
- tržní kapitalizace;
- a jiné.[291]

Obrázek 34 Vývoj počtu adres a jejich rozprostření



Zdroj: CoinMarketCap [online]. Dostupné z: https://coinmarketcap.com/currencies/bitcoin/holders/

Stock-to-flow model je populárním ukazatelem ceny Bitcoinu. Model nahlíží na Bitcoin jako na fixní, vzácný zdroj. Vzhledem k tomu, že existuje známá a omezená nabídka bez možnosti nálezu nových zdrojů, Bitcoin je využíván jako uchovatel hodnoty.

Ukazatel je vypočítán tak, že se sečte celková světová nabídka v oběhu a vydělí se množstvím vyprodukovaným za rok. Klesající výnosy z těžby vedou k vyššímu poměru odrážející vzácnost Bitcoinu, což zvyšuje jeho hodnotu. V modelu je také zachycen halving.

Model je poměrně dobrým ukazatelem ceny Bitcoinu. Cena byla navrstvena na 365 denní průměr a vykazuje dobrou shodu, nicméně model má i své nedostatky, například zahrnutí faktoru deflace.

Vývoj stock-to-flow modelu ze zachycen v grafu 18.

[291] Binance Academy.*Průvodce fundamentální analýzou kryptoměny* [online]. Dostupné z: https://academy.binance.com/cs/articles/a-guide-to-cryptocurrency-fundamental-analysis?UTM=BinanceAcademy

Graf 18 Stock-to-flow model

Zdroj: Buy Bitcoin Worldwide [online]. Dostupné z: https://buybitcoinworldwide.com/stats/stock-to-flow/

Graf 19 Vývoj ceny Bitcoinu po halvingu

Zdroj: Bitcoin Block Half [online]. Dostupné z: https://www.bitcoinblockhalf.com/images/

Havling, který nastane v dubnu roku 2024, může způsobit růst ceny Bitcoinu, jak již k tomu došlo v poslední třech případech. V tento moment dojde ke snížení odměny z 6,25 BTC za vytěžený blok na 3,123 BTC za vytěžený blok. Bitcoin se tak stane vzácnější a 2x náročnější a dražší vytěžit. Do oběhu se tak bude dostávat o 50 % méně nových bitcoinů, což ovlivní nabídku, které může být spojena s růstem ceny. Vývoj ceny Bitcoin po halvingu je zachycen v grafu 19.

Dorovnání tržní kapitalizace zlata je jednou z potencionálních scénářů, který by mohl nastat v dlouhodobém horizontu.

Již v minulosti nastala situace, kdy v podstatě lepší či dominantnější alternativa fiat měny demonetizovala alternativu druhou, tedy kdy podpora zlata dokázala vytlačit z monetárního světa stříbro.[292] V případě, že by byla podpora Bitcoinu v dnešní době obdobná, mohlo by alespoň k dorovnání tržní kapitalizace zlata dojít.

I když k tomuto dorovnání má Bitcoin stále daleko, v momentu naplnění tohoto scénáře cena jednoho bitcoinu přesahovala hodnotu 680.000 USD.[293]

Tržní kapitalizace zlate je v současné době nad 13 bil. USD a tržní kapitalizace Bitcoinu přesahuje 500 mld. USD a řadí ho tak na 12 nejhodnotnější aktivum světa. Seznam 12 nejhodnotnější aktiv světa je zobrazen v obrázku 37 a porovnání vývoje tržní kapitalizace zlata a tržní kapitalizace Bitcoinu je zachyceno v grafu 20.

I přes potencionální možnost predikovat cenu Bitcoinu, nejefektivnější strategií zůstává metoda pravidelných nákupů DCA. Je vhodné pravidelné nákupy menších částek doplňovat jednorázových nákupem větší částky, nežli bývá částka pravidelného nákupu. Nicméně DCA by měla přinášet většinou nově zakoupených bitcoinů do portfolia investora. V případě jednorázových nákupů je tak nejlepší využít kombinaci všech 3 analýz, tedy analýzu sentimentu, technickou analýzu a fundamentální analýzu, která investorovy mohou pomoci v rozhodovacím procesu nákupu nových bitcoinů.

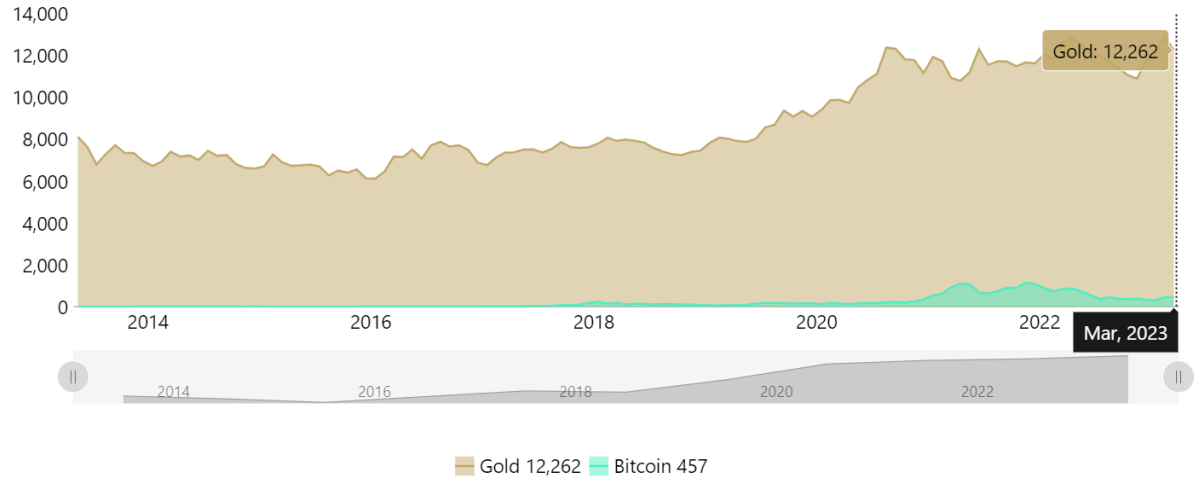
[292] AMMOUS, S. *The Bitcoin Standard.* 2018, s. 167-168
[293] Infinite Market Cap [online]. Dostupné z: https://8marketcap.com/compare/bitcoin/gold/

Obrázek 35 Tržní kapitalizace TOP12 světových aktiv

Rank	Name	Symbol	Market Cap	Price	24h	7d	Price (30 days)
1	Gold	GOLD	$13.196 T	$2,000	0.78%	0.29%	
2	Apple	AAPL	$2.618 T	$162.31	0.96%	2.13%	
3	Microsoft	MSFT	$2.154 T	$284.04	1.26%	2.30%	
4	Saudi Aramco	2222.SR	$1.895 T	$8.62	-0.31%	0.47%	
5	Silver	SILVER	$1.352 T	$24.02	2.36%	3.67%	
6	Alphabet (Google)	GOOG	$1.3 T	$101.28	-0.61%	-4.69%	
7	Amazon	AMZN	$1.076 T	$101.93	1.68%	3.26%	
^1 8	NVIDIA	NVDA	$682.38 B	$273.83	1.48%	0.71%	
v1 9	Berkshire Hathaway	BRK-B	$675.07 B	$305.03	-0.09%	2.23%	
10	Tesla	TSLA	$632.92 B	$195.2	0.68%	1.55%	
^1 11	Meta Platforms (Facebook)	META	$551.31 B	$207.81	1.20%	1.73%	
v1 12	Bitcoin	BTC	$541.5 B	$28,010	-1.47%	-1.52%	

Zdroj: Infinite Market Cap [online]. Dostupné z: https://8marketcap.com/

Graf 20 Vývoj tržní kapitalizace Bitcoinu a zlata



Zdroj: InGoldWeTrust [online]. Dostupné z: https://ingoldwetrust.report/chart-gold-bitcoin-marketcap/?lang=en

4.6 Prodej Bitcoinu

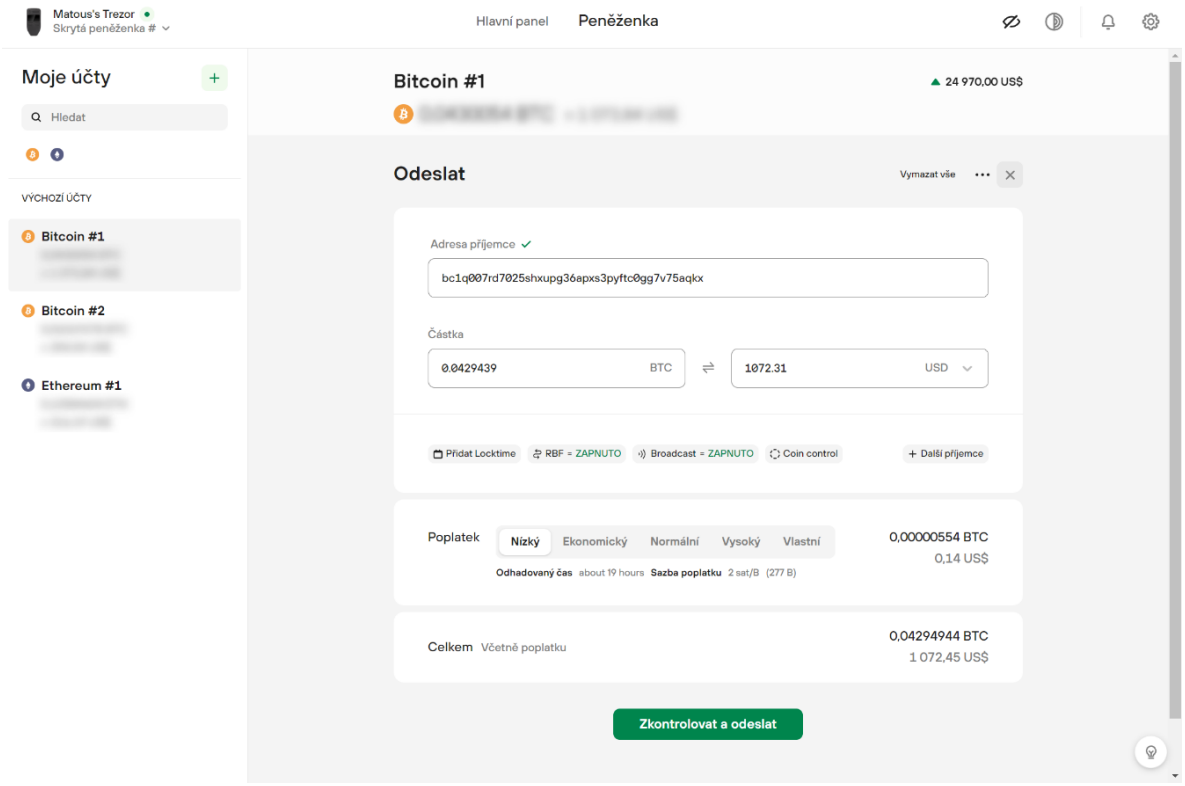
V momentu rozhodnutí odprodeje části či celého bitcoinového portfolia se bude postupovat obdobným způsobem, jako pří nákupu a následným uložením, jen v opačném směru toku finančních prostředků. Bitcoiny je nutné přesunou na prodejní místo, tedy v tomto případě zpět na burzu Coinmate. Nejdříve je zapotřebí zapojit Trezor do počítače, kde jsou prostředky bezpečně uloženy a přihlásit se do prostředí Trezoru Suite. Zde přejít přes panel „Peněženka“ ke svým zůstatkům a vybrat se možnost „odeslat“.

Následně je nutná se přihlásit na burzu, kam budou bitcoiny odeslány. Na burzu se přihlásit, přejít do lišty „vklady/výběry“, označit pole vklad, vybrat možnost Bitcoinu, kde se zobrazí adresa pro přijetí bitcoinu společně s QR kódem. Adresu je nutné zkopírovat a vrátit se do prostředí Trezor Suite.

Zde se do pole „Adresa příjemce“ vloží zkopírovaná bitcoinová adresa, u které dojde ke kontrole validity. Následně se vyplní částka, kolik má být odesláno satoshi, či je možné zvolit možnost „odeslat vše“. V následujícím kroku se vyplní poplatek, u kterého velikost bude odpovídat rychlost odeslání a potvrzení transakce. Například při možnosti „Nízký“ bude sazba poplatku pouze 2 satoshi/B, poplatek tak vyjde na pouhých 0,14 USD, tomu však bude odpovídat odhadovaný čas zápisu transakce, který je vyčíslen na 19 hodin. Je však možnost zvolit rychlejší možnosti odeslání či zvolit vlastní částku transakčního poplatku, ke kterému se vypočítá odhadovaná doba zápisu transakce. Po potvrzení odeslání je nutné potvrdit pole „Zkontrolovat a odeslat“ a následně zadat PIN kód Trezoru. Poté budou prostředky odeslány a připsány k účtu na burze. Prostředí Trezoru Suite pro odeslání Bitcoinu je zachyceno v obrázku 38.

Na burze se přejde do prostředí „pokročilého obchodování“ a zde se může buďto Bitcoin prodat jednorázově, přes market order nebo nastavit postupné prodeje, tedy v podstatě DCA s nastavením limitů prodeje přes limit order. Není však rozumné nechávat velké množství prostředků po dlouhou dobu na burze.

Obrázek 36 Prostředí Trezoru Suit pro odeslání Bitcoinu



Zdroj: Trezor Suite

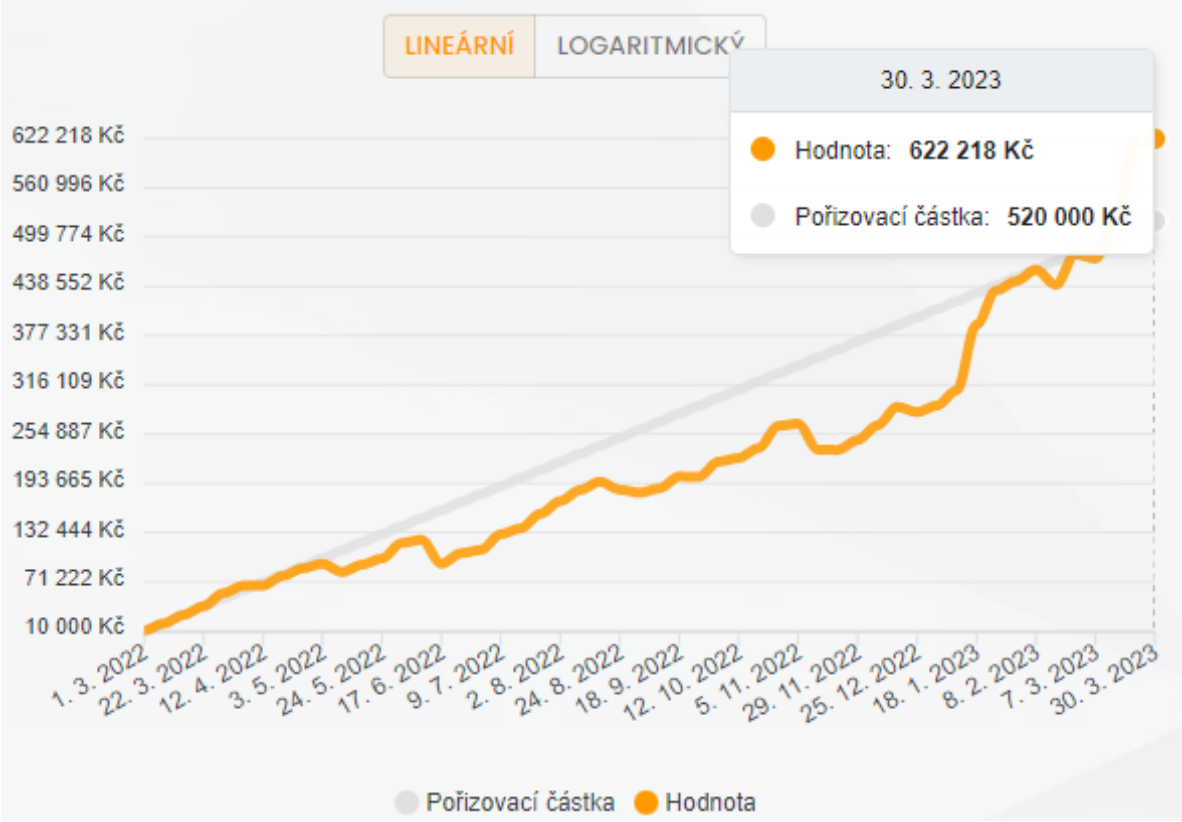
4.6.1 Exitová strategie

Exitová strategie není nic víc než obchodní plán, který je běžnou součástí investování a kterou by měli mít připraveni i největší bitcoinový Hodleři. Investice je od toho, aby přinesla investorovy zisk a realizace zisku je provedena prostřednictvím prodeje, kdy nákupní cena je nižší než cena prodejní a proto je třeba Bitcoin prodat ve správný čas. Exitová strategie má zejména za úkol předejít emočnímu rozhodování investora tak, aby nedocházelo k prodeji ve ztrátových pozicích způsobených strachem z ještě větší ztráty či skutečné realizaci zisku v případě růstu ceny tak, aby investor nečekal na stále vyšší hodnotu BTC a v podstatě by se nikdy nedočkal, protože růst ceny netrvá věčně. Je však nutné zmínit, že každé exitová strategie bude vypadat jinak, v závislosti na skutečné situaci investora. Modelová situace exitové strategie bude zachycena v následujícím příkladu a tabulce 4.

Příklad:

Investor nakupoval BTC pravidelně metodou DCA s nákupy 1x týden za 10.000 CZK po dobu jednoho roku. Za tuto dobu naakumulovat 0,9455 BTC s celkovou investovanou částkou 520.000 CZK, vývoj bych zachycen v grafu 21. Za pomocí drobných nákupů při poklesu ceny přidal do svého portfolia 0,0545 BTC za 30.000 CZK. Celkově tedy vlastní 1 BTC s investovanou částkou 550.000 CZK. V tento moment se růstem ceny se rozhodl nákupu ukončit. Průměrná cena nákupů je tedy 550.000 CZK/BTC.

Graf 21 Vývoj nákupů metodou DCA po dobu jednoho roku



Zdroj: Štosuj.cz [online]. Dostupné z: https://stosuj.cz/

Následně se s růstem ceny investor rozhodl postupně BTC odprodávat, jak je zaznamenáno v tabulce 4.

Tabulka 4 Exitová strategie

	Prodej BTC	Prodej BTC v %	Prodejní cena CZK/BTC	Zaokrouhlená prodejní cena USD/BTC	Zisk v CZK
	0,1	10 %	1 000 000 Kč	$ 46 000	45 000 Kč
	0,1	10 %	1 200 000 Kč	$ 55 000	120 000 Kč
	0,1	10 %	1 400 000 Kč	$ 65 000	140 000 Kč
	0,1	10 %	1 600 000 Kč	$ 74 000	160 000 Kč
	0,1	10 %	1 800 000 Kč	$ 83 000	180 000 Kč
	0,1	10 %	2 000 000 Kč	$ 92 000	200 000 Kč
	0,1	10 %	2 100 000 Kč	$ 97 000	210 000 Kč
	0,1	10 %	2 400 000 Kč	$ 110 000	240 000 Kč
	0,1	10 %	2 500 000 Kč	$ 115 000	250 000 Kč
	0,1	10 %	2 800 000 Kč	$ 129 000	280 000 Kč
Celkem	1	100 %			1 825 000 Kč
Průměrná prodejní cena			1 880 000 Kč	$ 86 600	
Průměrná nákupní cena			550 000 Kč	$ 25 000	

Zdroj: Vlastní zpracování

Investor by tedy v tomto případě realizoval zisk 1.825.000 CZK před zdaněním. Je však nutné zmínit, že růst ceny bitcoinu nemusí probíhat takto plynule a nemusí tak dojít ke všem prodejům v jednom bull marketu. Nicméně strategii lze upravit dle aktuální situace a pokračovat s ní i do budoucna. Je však žádoucí být na bull market řádně připraven.

4.7 Zdanění Bitcoinu

V současné době neexistuje žádná speciální úprava pro Bitcoin v oblasti daní. V případě investice do Bitcoinu jsou daněné pouze realizované zisky, které se daní jako zisk ze zboží a služeb. Rozhodně tedy neplatí, že se kryptoměny obecně nemusí dani. Daň z příjmů musí odvádět fyzické osoby, OSVČ či zaměstnanci, kteří s bitcoiny obchodují či firmy, které Bitcoin těží nebo za ně prodává své služby a produkty.

Bohužel v České republice ČNB pohlíží na veškeré kryptoměny, tedy i Bitcoin, jako na ekonomickou činnost, nikoliv jako investiční aktivum. Jsou totiž dle §10 zákona o daních z příjmů vedeny jako „ostatní příjmy“. Z tohoto důvodu v případě investice do Bitcoinu nelze počítat s časovým testem, což znamená, že nelze uplatnit pravidlo, že z investic držených dále než 3 roky se nemusí odvádět daň. Také neplatí, že by obchod s kryptoměnami mohl být součástí podnikání, a to jako hlavní ani vedlejší činnost, kterou má zaměstnanec s živnostenským listem. Česká finanční správa tedy vede kryptoměny jako zboží:

- s nímž se obchoduje – na kryptoměnové burze dochází ke směně za běžné peníze nebo jiné kryptoměny;
- které je produkováno – těžba;
- za nějž je možné směňovat na reálném trhu – nakupovat a prodávat zboží a služby.

Z tohoto důvodu je využívaná definice, kdy kryptoměna je nehmotným aktivem. Odpovídají k tomu používané metody oceňování:

- FIFO = „First In First Out“;
- aritmetický průměr.

Je za potřebí zvolit jednu metodu oceňování a v ní nadále pokračovat. Metodu již později v průběhu danění nelze lehce změnit.

Anonymita by neměla být záminkou pro nezdanění realizovaných zisků. Vzhledem k ověření KYC, pohybům peněz spojené s bankovními účty konkrétní osoby či operacím prováděných na burzách konkrétní osoby již rozhodně nelze obchod s bitcoiny považovat za anonymní. Anonymita je tedy spíše zdánlivá. Navíc je celý blockchain veřejný, nezměnitelný a uchovává všechny provedené transakce od počátku sítě. Stačí tedy, aby anonymita byla odhalena na jedná z adres uživatelů a veškeré provedené akce jsou snadno spojitelné. Informace jsou navíc ze strany bank a burz poskytovány finanční správě, které tak může kdykoliv nahlédnout do účtu uživatele bez zahájení finanční kontroly.

Předmětem daně aneb z čeho se daně platí, jsou realizované zisky, nikoliv samotné držení bitcoinů. Zisk neboli navýšení majetku je rozdílem mezi výdaji na nákup kryptoměny a příjmem z jejího prodeje nebo její směny, tedy v případě směny bitcoin/altcoin či zboží/služby. Vždy je rozdíl mezi hodnotou Bitcoinu při jeho pořízení a při jeho směně či prodeji. Od vypočítaného zisku lze ještě odečíst transakční náklady vzniklé v souvislosti s nákupem a prodejem či směnou, nic jiného odečíst nelze, jako například nákup Trezoru na uložení Bitcoinu. Zisk tedy vypočítáme v různých případech jako:

- zisk = prodejní cena BTC – nákupní cena BTC – transakční poplatky;
- zisk = výnosy z prodeje za BTC – náklad na produkci služby či směnu BTC – transakční poplatky;
- zisk = výnosy z těžby BTC – náklady na těžbu BTC – transakční poplatky.

Bitcoin je tedy brát tak, že při zacházením s ním je generován zisk nebo ztráta. I přesto, že se bitcoiny nakupují na burzách, nejedná se o investici a na Bitcoin tak nelze uplatnit žádná investiční úleva.

V případě těžby Bitcoinu je nutné mít vydané živnostenské oprávnění, pro obchodování s ním již potřeba není. U samotného zdanění je dále nutno rozlišovat, zda se jedná o:

- zaměstnance bez živnostenského oprávnění;
- OSVČ;
- právnické osoba.

Ve všech případech se bude jednat o zdanění „ostatních příjmů“.

U zaměstnance není obchodování s kryptoměnami soustavnou činností. Lze tedy uplatnit úlevu z daně, jako je osvobození od daně z důvodu tzv. „příležitostných příjmů“. Jedná se o situaci, kdy je roční příjem z ostatních činností, kam obchod s kryptoměnami spadá, nižší než 30.000 CZK. Do ročního limitu se však počítají všechny příležitostní příjmy, tedy nejen kryptoměny. V případě překročení se daní celá částka, ne pouze překročená částka. Limit 30.000 CZK je nutno brát jako celkový příjem, tedy celkovou částku, kterou obdržíme z prodeje bitcoinů. Nejedná se tedy pouze o částku zisku.

Daň ze zisku z prodeje Bitcoinu je 15 %. U osob, které překročí 48x průměrné měsíční mzdy za rok, tedy pro rok 2022 se jedná p roční příjem nad 1.867.728 CZK, je sazba daně zvýšena na 23 %. Zvýšená daň se uplatňuje na částku přesahující tento limit, do limitu je daněno základní sazbou 15 %. Do limitu jsou započítávány i pasivní a ostatní příjmy, tedy i

příjmy z prodeje Bitcoinu. Daňový základ je možné snížit o odečitatelné položky či využití slevy na dani zůstává i u zdanění kryptoměn.

U OSVČ, či zaměstnance s živnostenským listem, se kryptoměny daní jako „ostatní příjmy“ a je zdaněn realizovaný zisk. Vzhledem k tomu, že obchodování s kryptoměnami se nepovažuje za podnikatelskou činnost, nelze uplatnit výdajový paušál ani režim paušální daně. V momentu, co má poplatník DPFO ke zdanění „ostatní příjmy“, musí z paušálního režimu vystoupit. V případě výpočtu zisku, nelze od prodejní ceny Bitcoinu odečíst jiné náklady, něž cenu pořízení a transakční poplatky. Daň ze zisku je také 15 %, současně se také zvyšuje daň na 23 % při překročení hranice 1.867.728 CZK pro rok 2022.

U právnické osoby je daň ve výší 19 % ze základu daně. Výhodu je, že „ostatní příjmy“ se promítají do celkového hospodářského výsledku. Je tedy možné, případnou ztrátou firmy v jiné činnosti, ponížit zisk z prodeje Bitcoinu, vždy však v příslušném účetním období. V opačném případě se ztráta z obchodování s Bitcoinem nemůže rozložit do dalších období a vždy je nutna uplatnit v příslušném období, kdy byl prodej se ztrátou realizován.

Těžba Bitcoinu je již pokládána za podnikání, tedy soustavnou činnost. Může jít o činnost hlavní tak i vedlejší. Jedná se tedy o příjmy ze samostatné činnosti. Jako příjem se zde považuje směna za fiat měnu, tedy v tomto případě směna do CZK. V případě vedení účetnictví se skutečnými náklady, je možné od příjmu z těžby odečítat všechny náklad spojené s těžbou. Také zle nastavit paušální daň nebo paušální výdaje. Nicméně ztrátu v tomto případě nelze rozpustit do následujících účetních období. V případě překročení obratu 1 mil. CZK za rok se těžař automaticky stává plátcem DPH. V tomto případě odvádí DPH z Bitcoinu, pouze však z těžby. V oblasti obchodování je Bitcoin osvobozen od DPH.

Jedním z teoretických případů, kdy by obchod s Bitcoinem mohl být plně osvobozen od daně je dle §4 odst.1 písm. ze) osvobození daní pro veškeré kurzové zisky při směně zahraničních měn, pokud není účet v obchodním majetku firmy. Důvodem tohoto tvrzení je, že Bitcoin se stal v září roku 2021 oficiální legální měnou státu Salvador. Problémem, který při tomto případu však vzniká je, že současná česká daňová správa zatím neuznává Bitcoin a všechny ostatní kryptoměny jako měnu, ale jako majetek či výrobek, v případu těžby. Z tohoto důvodu je v současné době tak stále nutné daně z Bitcoinu řádně uhradit.[294]

[294] Banky.cz. *Jak na zdanění kryptoměn – kompletní návod* [online]. Dostupné z: https://www.banky.cz/clanky/jak-na-zdaneni-kryptomen-kompletni-navod/

4.7.1 Výpočet daně

Stanovení pořizovací ceny v momentu prodeje Bitcoinu je důležitý moment pro výpočet základu daně a následného daňového odvodu. Evidenci nákupu je možné vést individuálně za pomocí různých „portfolio trackerů“ nebo se spolehnout na záznamy z burzy, přes kterou byl Bitcoin zakoupen. U každé burzy je možné si nechat vygenerovat seznam nákupů. Jak již bylo uvedeno, nejčastějšími metodami pro zjištění nákupní ceny prodávaných jednotek Bitcoinu je metoda aritmetického průměru nebo metoda FIFO.

Metoda FIFO neboli metoda „první dovnitř, první ven“ vyžaduje vedení dobré evidence nákupů, které budou pro výpočet používány. V moment, co dojde k prodeji kryptoměny, za pořizovací cenu se pokládá ta, za které byly nakoupeny nestarší bitcoiny, které jsou stále v držení. Je tedy nutné v záznamech dohledat pořizovací cenu prodávaného bitcoinu a použit jí pro výpočet. V nákupní ceně bitcoinu, který není předmětem prodeje se nepřihlíží. Každý objem při prodeji se vypočítává zvlášť. Výsledným daňovým základem je tedy součet rozdílů mezi všemi nákupními cenami a cenou prodejní.[295] Opačnou metodou je metoda LIFO, tedy „poslední dovnitř, první ven. Tato metoda je mnohem méně využívána, a proto tato práce bude pojednávat pouze s metodou FIFO a metodou aritmetického průměru.[296]

Tyto skutečnosti jsou ukázány na konkrétní příkladu. Pro snadnější vysvětlení je počítáno v CZK, což je současně doporučené pro výpočet daně v ČR. I v případě, že je BTC nakupován v jiné měně, např. EUR nebo USD, záznamy o nákupech lze snadno převést na jinou měnu.

[295] Banky.cz. *Jak na zdanění kryptoměn – kompletní návod* [online]. Dostupné z: https://www.banky.cz/clanky/jak-na-zdaneni-kryptomen-kompletni-navod/
[296] Banky.cz. *FIFO* [online]. Dostupné z: https://www.banky.cz/slovnik/fifo/

Příklad 1:

Fyzická osoba uskutečnění 5 nákupů v různých časech:

- 0,01 BTC při směnném kurzu 400.000 CZK/BTC za 4.000 CZK dne 1.1.2022;
- 0,01 BTC při směnném kurzu 450.000 CZK/BTC za 4.500 CZK dne 1.2.2022;
- 0,01 BTC při směnném kurzu 500.000 CZK/BTC za 5.000 CZK dne 1.3.2022;
- 0,01 BTC při směnném kurzu 550.000 CZK/BTC za 5.500 CZK dne 1.4.2022;
- 0,01 BTC při směnném kurzu 600.000 CZK/BTC za 6.000 CZK dne 1.5.2022.

Následně se fyzická osoba rozhodne odprodat 0,03 BTC dne 1.12.2022 při cena 1.000.000 CZK/BTC. Do výpočtu se tedy započítají pouze první tři nákupy. Současná hodnota BTC při prodeji bude 0,03 BTC = 30.000. CZK. Pro zjištění základu daně je nutné vypočítat zisk, který se vypočítá jako: zisk = prodejní cena BTC – nákupní cena BTC – transakční poplatky (pro tento příklad se celková částka transakčních poplatků bude uvažovat 100 CZK).

- Zisk = 30.000 – (4.000 – 4.500 – 5.000) – 100 = 16.400 CZK

Realizovaný zisk při prodeji je tedy pokládán za základ daně. Daňová sazba je 15 %.

- Daň = 16.400 x 0,15 = 2.460 CZK

Daň k odvedení tedy bude 2.460 CZK při prodeji 0,03 BTC při hodnotě 1.000.000 CZK/BTC s čistým ziskem 13.940 CZK. V případě prodeje zbylého vlastněného BTC se již předchozí nákupy nebudou uvažovat. Pro prodej zbylého 0,02 BTC při ceně 1.100.000 CZK/BTC s transakčními poplatky 50 CZK byl:

- zisk = 22.000 – (5.500 – 6.000) – 50 = 10.450 CZK;
- daň = 10.450 x 0,15 = 1.567,50 CZK;
- čistý zisk = 10.450 – 1.567,50 = 8.882.50 CZK.

Celková investice 25.000 CZK rozdělena do 5 nákupů a 2 prodejů by přinesla čistý zisk 22.822,50 CZK a celková odvedená daň 4.027.50 CZK.

Metoda aritmetického průměru funguje na základě stanovení průměrné nákupní ceny ze všech provedených nákupů, do data prodeje, se zohledněním objemu jednotlivých nákupů. Tato metoda se bude používat pro výpočet zisku z prodeje a následné daně.[297]

Příklad 2:

Fyzická osoba uskutečnění 5 nákupů v různých časech:

- 0,01 BTC při směnném kurzu 400.000 CZK/BTC za 4.000 CZK dne 1.1.2022;
- 0,01 BTC při směnném kurzu 450.000 CZK/BTC za 4.500 CZK dne 1.2.2022;
- 0,01 BTC při směnném kurzu 500.000 CZK/BTC za 5.000 CZK dne 1.3.2022;
- 0,01 BTC při směnném kurzu 550.000 CZK/BTC za 5.500 CZK dne 1.4.2022;
- 0,01 BTC při směnném kurzu 600.000 CZK/BTC za 6.000 CZK dne 1.5.2022.

Následně se fyzická osoba rozhodne odprodat 0,03 BTC dne 1.12.2022 při cena 1.000.000 CZK/BTC. Do výpočtu se tedy započítají všechny uskutečněné nákupy, ze kterých se vypočítá aritmetický průměr nákupní ceny. Ta se vypočítá jako součet všech nákupních cen vynásobený objemem nákupu a následně vydělený počtem nákupů.

- Průměrná nákupní cena = (400.000 x 0,01 + 450.000 x 0,01 + 500.000 x 0,01 + 550.000 x 0,01 + 600.000 x 0,01) / 5 = 5.000 CZK/0,01 BTC = 500.000 CZK/BTC

Současná hodnota BTC při prodeji bude 0,03 BTC = 30.000. CZK. Pro zjištění základu daně je nutné vypočítat zisk, který se vypočítá jako: zisk = prodejní cena BTC – nákupní cena BTC – transakční poplatky (pro tento příklad se celková částka transakčních poplatků bude uvažovat 100 CZK).

- Zisk = 30.000 – (0,03 x 500.000) – 100 = 14.900 CZK

Realizovaný zisk při prodeji je tedy pokládán za základ daně. Daňová sazba je 15 %.

- Daň = 14.900 x 0,15 = 2.235 CZK

Daň k odvedení tedy bude 2.235 CZK při prodeji 0,03 BTC při hodnotě 1.000.000 CZK/BTC s čistým ziskem 12.665 CZK. Pro prodej zbylého 0,02 BTC při ceně 1.100.000 CZK/BTC s transakčními poplatky 50 CZK byl:

- zisk = 22.000 - (0,02 x 500.000) – 50 = 11.950 CZK;

[297] Banky.cz. *Jak na zdanění kryptoměn – kompletní návod* [online]. Dostupné z: https://www.banky.cz/clanky/jak-na-zdaneni-kryptomen-kompletni-navod/

- daň = 11.950 x 0,15 = 1.792.50 CZK;
- čistý zisk = 11.950 – 1.792.50 = 10.157,50 CZK.

Celková investice 25.000 CZK rozdělena do 5 nákupů a 2 prodejů by přinesla čistý zisk 22.822,50 CZK a odvedená daň 4.027,50 CZK.

Jak je tedy z výpočtů zjevné, celková odvedená daň bude vždy totožná s využitím obou metod. Nicméně průběžně odvedené daně při průběžných odprodejích budou rozdílné. Je tedy na samotném uživateli, kterou metodu výpočtu si zvolí.

V případě velkého množství provedených nákupů či nákupů na různých burzách může výpočet být velmi zdlouhavý či nepřehledný. Proto je již možné využít různých aplikací pro automatizaci procesu.

Daň se nutné odvést stejným způsobem i v případě nákupu Bitcoin jinde nežli na burzách či směnárnách, například při nákupu v Bitcoinovém ATM, P2P směnárnách a decentralizovaných burzách. [298]

[298] Banky.cz. *Jak na zdanění kryptoměn – kompletní návod* [online]. Dostupné z: https://www.banky.cz/clanky/jak-na-zdaneni-kryptomen-kompletni-navod/

5 Výsledky a diskuse

Z provedené analýzy fundamentu Bitcoinu v teoretické části práce je nyní zjevné, jakým způsobem samotný Bitcoin funguje. Pochopení základní terminologie Bitcoinu, základní ekonomický a investiční pojmů je zásadní pro závěr investice do Bitcoinu. Ze stručného shrnutí historie Bitcoinu je možné odvodit, jakým stylem se Bitcoin vyvíjí. Bylo nutné vysvětlit technické vlastnosti Bitcoinu pro plné pochopení fundamentu. Přesto, že Bitcoin byl navržen jako měna a nadále tak funguje, poskytuje vlastnosti spíše jako uchovatele hodnoty nežli platidla využívaného na denní bázi miliardami lidí. Bitcoin je však stále velmi volatilní, i když se jeho volatilita s každým cyklem bull marketu a bear marketu snižuje.

I přes to, že existuje mnoho potencionálních rizik, problémů a mýtů bitcoinová síť plynule funguje, každý 10 minut je vytěžen blok a přiděleny vypuštěny nové bitcoiny do oběhu. Bitcoinová síť tak funguje bez jakéhokoliv významného problému již od roku 2009, kdy byla spuštěna. Takto by měla pokračovat i nadále, vzhledem k vysokým úrovních hash ratu a vysoké úrovně difficulty, které jsou v podstatě na historických maximech, je síť bezpečnější než kdy předtím.

Současná cena Bitcoinu se pohybuje na nízkých cenových hladinách. V současné době se Bitcoin pohybuje kolem hodnoty 25.000 USD/BTC, tedy zhruba 70 % od svého cenového maxima, které přesahovalo cenu 69.000 USD/BTC. Cenová konsolidace tak může trvat ještě několik měsíců, ale současné cenové hodnoty se jeví jako vhodná investiční příležitost, pro investora, který chce zhodnotit své finanční prostředky v horizontu několika let. V momentu, co by se ceny Bitcoinu vrátila na původní hodnoty ATM, jedná se o zhodnocení investice o téměř 300 %. Po překonání hodnoty ATM Bitcoin v minulosti dále pokračoval v cenovém růstu, proto je jen otázkou, kam až hodnota Bitcoinu v dalším bull runu může vyšplhat.

Byl pracován celkový proces investice do Bitcoinu tak, aby byl co nejvýhodnější a nejefektivnější pro investovat. Byla pracována analýza nákupního prostředí, kde následnou komparativní analýzou byla vybrána burza Coinmate jako nejvhodnější nákupní prostředí pro investora v ČR. Následný proces nákupu Bitcoinu byl detailně zaznamenán. Využito bylo i možnosti nastavení automatických nákupů přes prostředí Štosuj.cz na týdenní bázi nákupů.

Následně byla vybrána nejbezpečnější možnost uložení zakoupeného Bitcoinu v podobě hardwarové peněženky Trezor, u které bylo popsáno nastavení samotné peněženky s detailním popisem procesu odeslání bitcoinu z burzy na peněženku a zajištění tak

bezpečného uložení investice. Byla vysvětlena i problematika správy investičního portfolia Bitcoinu.

Byla provedena predikce ceny Bitcoinu na základě několika predikční nástrojů, které mohou investorovy pomoci při posouzení vhodné nákupní příležitosti při dlouhodobém horizontu investice s potencionálními dodatečnými nákupy při vhodné ceně nežli pouze metodou DCA.

V neposlední řadě byl popsán způsob výstupu z investice do Bitcoinu v podobě jeho odprodeje. V tomto procesu byly popsány jednotlivé kroky odeslání bitcoinu z hardwarové peněženky Trezor na burzu Coinmate, kde došlo k nastavení prodejních příkazů. V návaznosti na prodej Bitcoinu bylo popsáno zdanění zisků s ukázkami jednotlivým metod výpočtů na konkrétních příkladech.

V práci byla i analýza potencionální investice do těžby Bitcoinu, nicméně díky nepříznivé současné situace se investice ukázala jako ztrátová, proto bylo rozhodnuto v investici do těžby Bitcoinu dále nepokračovat.

Bitcoin se tak jeví jako zajímavá investiční příležitost. Z minulosti je zjevné, že je schopen velkých cenových růstů. Velkou výhodou Bitcoinu je i jeho likvidita, kdy je možné v podstatě ihned převést na hotovost. Uložené bitcoiny lze z peněženky odeslat na burzu, kde při zaplacení vyššího transakčního poplatku mohou být v podstatě instantně a odprodej bitcoinů na burze přes market order je okamžitý. Investice do Bitcoinu však není metodou, jak rychle zbohatnout. Celkovou problematiku Bitcoinu a jeho fundament je nutno dobře znát. Nakupovat bitcoiny je vhodné za pomocí metody DCA s příležitostnými nákupy při vhodné ceně, například při jejím poklesu neboli „dipu“.

Díky vysoké volatilitě není vhodné mít do Bitcoinu 100 % expozici investičního portfolia. Měly by být využity finanční zdroje, o které si investor „může dovolit přijít“. I v případě výkyvu ceny, tedy poklesu hodnoty Bitcoinu je možné se správně nastavenou investiční strategií s dostatečně dlouhým horizontem období bear marketu v podstatě přečkat. Je velká pravděpodobnost, že cena se dříve či později vrátí na původní hodnoty, na kterých byl bitcoin zakoupen, či je překoná.

Bitcoin by tam měl mít zakoupený aspoň částečně ve svém investičním portfoliu každý investor.

6 Závěr

Bitcoin tedy alternativní investici, která by měla mít zastoupení v každém investičním portfoliu, ať již zkušeného, či začínajícího investora.

I přes to, že je Bitcoin stále spekulativnějším typem investice, jeho volatilita se v každém cyklu snižuje. Pro pochopení těchto cenových výkyvů je nutné znát fundament Bitcoinu, který je tak pro investora zásadní. Předchází se tak nepromyšleným a emočně založeným nákupům pod vlivem FOMA a následným prodejům ve ztrátových pozicích v případě FUD.

Investice do Bitcoinu tak není z počátku úplně jednoduchá. Postupy nákupu, prodeje, odeslání a jiné manipulace s bitcoiny se však stávají s časem přirozenější. Samotná investice do Bitcoinu není zrovna klidnou investiční cestou, nicméně při postupu dle zvolené investiční strategie a minimalizaci emočních prodejů či nákupů lze dosáhnou s dostatečně dlouhým investičním horizontem velmi vysokého zhodnocení své investice. Jak bylo řečeno v knize Inteligentní investor: *„Cesta za dosažením zisku je ve skutečnosti dlouhá a trpělivost pokoušenící zkušenost*.“ [299]

[299] GRAHAM, B. *Inteligentní investor*. 2007, s. 44-45

7 Seznam použitých zdrojů

7.1 Knižní zdroje

AMMOUS, Seifedean. *The Bitcoin Standard: The Decentralized Alternative to Central Banking*. United States of America: Wiley, 2018. ISBN 978-11-1947-386-2.

BRČÁK, Josef, Bohuslav SEKERKA a Dana STARÁ. *Makroekonomie: teorie a praxe*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2014. ISBN 978-80-7380-492-3.

GRAHAM, Benjamin. *Inteligentní investor*. 1. Praha: GRADA Publishing, 2007. ISBN 978-80-247-1792-0.

KALISKÝ, Borin. *Bitcoin a ti druzí: Nepostradatelný průvodce světem kryptoměn*. IFP Publishing, 2018. ISBN 978-80-87383-71-1.

NAKAMOTO, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2008.

PRITZKER, Yan. *Vynález jménem Bitcoin: Vznik a fungování první skutečně vzácné a decentralizované měny*. Braiins Systems, 2020. ISBN 978-80-907975-0-5.

SAMUELSON, Paul Anthony a William D. NORDHAUS. *Ekonomie*. Praha: Svoboda, 1991. ISBN 80-205-0192-4.

STROUKAL, Dominik a Jan SKALICKÝ. *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*. Braiins Systems, 2021. ISBN 978-80-907975-5-0.

7.2 Internetové zdroje

1000 Logos: Bitcoin logo [online]. [cit. 2023-03-31]. Dostupné z: https://1000logos.net/bitcoin-logo/

Alternative [online]. [cit. 2023-03-31]. Dostupné z: https://alternative.me/crypto/fear-and-greed-index/

Alternative: Crypto Fear & Greed Index [online]. [cit. 2023-03-31]. Dostupné z: https://alternative.me/crypto/fear-and-greed-index/

Antminer Distribution Europe: Antminer S19J Pro+ [online]. [cit. 2023-03-31]. Dostupné z: https://www.antminerdistribution.com/antminer-s19j-pro-2/

Anycoin [online]. [cit. 2023-03-31]. Dostupné z: https://www.antminerdistribution.com/antminer-s19j-pro-2/

ASIC Miner value [online]. [cit. 2023-03-31]. Dostupné z: https://www.asicminervalue.com/miners/bitmain/antminer-s19j-pro-122th

Atcmarket: Altcoiny [online]. [cit. 2023-03-31]. Dostupné z: https://www.atcmarket.cz/articles/26318

Banky.cz: FIFO [online]. [cit. 2023-03-31]. Dostupné z: https://www.banky.cz/slovnik/fifo/

Banky.cz: Jak na zdanění kryptoměn – kompletní návod [online]. [cit. 2023-03-31]. Dostupné z: https://www.banky.cz/clanky/jak-na-zdaneni-kryptomen-kompletni-navod/

BBC: Elon Musk's Tesla sells most of its Bitcoin holding [online]. [cit. 2023-03-31]. Dostupné z: https://www.bbc.com/news/business-62246367

Binance Academy: Co je postup KYC (poznej svého klienta)? [online]. [cit. 2023-03-31]. Dostupné z: https://academy.binance.com/cs/articles/what-is-kyc-know-your-customer

Binance Academy: Co je technická analýza? [online]. [cit. 2023-03-31]. Dostupné z: https://academy.binance.com/cs/articles/what-is-technical-analysis?UTM=BinanceAcademy

Binance Academy: Co je to sentiment na kryptoměnovém trhu? [online]. [cit. 2023-03-31]. Dostupné z: https://academy.binance.com/cs/articles/what-is-crypto-market-sentiment

Binance Academy: Co jsou blockchainové transakční poplatky? [online]. [cit. 2023-03-31]. Dostupné z: https://academy.binance.com/cs/articles/what-are-blockchain-transaction-fees

Binance Academy: Průvodce fundamentální analýzou kryptoměn [online]. [cit. 2023-03-31]. Dostupné z: https://academy.binance.com/cs/articles/a-guide-to-cryptocurrency-fundamental-analysis?UTM=BinanceAcademy

Binance: Binance [online]. [cit. 2023-03-31]. Dostupné z: https://www.binance.com/en

Bisq [online]. [cit. 2023-03-31]. Dostupné z: https://bisq.markets/

Bisq: The Bisq DAO [online]. [cit. 2023-03-31]. Dostupné z: https://bisq.network/dao/

Bitcoin Block Half: Bitcoin Block Reward Halving Countdown [online]. [cit. 2023-03-31]. Dostupné z: https://www.bitcoinblockhalf.com/

Bitmain: Bitcoin miner S19J Pro+ [online]. [cit. 2023-03-31]. Dostupné z: https://shop.bitmain.com/product/detail?pid=00020230108213609854b369SGwI0654

Business Today: One year since El Salvador announced Bitcoin adoption plans! Shat's te latest? [online]. [cit. 2023-03-31]. Dostupné z: https://www.businesstoday.in/crypto/story/one-year-since-el-salvador-announced-bitcoin-adoption-plans-whats-the-latest-336443-2022-06-06

Coinbase [online]. [cit. 2023-03-31]. Dostupné z: https://www.coinbase.com/advanced-trade/

Coinbase: Home [online]. [cit. 2023-03-31]. Dostupné z: https://www.coinbase.com/home

Coindesk [online]. [cit. 2023-03-31]. Dostupné z: https://www.coindesk.com/markets/2018/12/11/panic-mode-what-a-wall-street-chart-tells-us-about-bitcoins-price/

Coindesk: Panic Mode? What a Wall Street Chart Tells Us About Bitcoin's Price [online]. [cit. 2023-03-31]. Dostupné z: https://www.coindesk.com/markets/2018/12/11/panic-mode-what-a-wall-street-chart-tells-us-about-bitcoins-price/

Coindesk: What is Bitcoin Pizza Day [online]. [cit. 2023-03-31]. Dostupné z: https://www.coindesk.com/markets/2018/12/11/panic-mode-what-a-wall-street-chart-tells-us-about-bitcoins-price/

CoinGecko: Ceny kryptoměny od historického maxima (ATH) [online]. [cit. 2023-03-31]. Dostupné z: https://www.coingecko.com/cs/watchlists/all-time-high-crypto

CoinMarketCap [online]. [cit. 2023-03-31]. Dostupné z: https://coinmarketcap.com/currencies/bitcoin/historical-data/

CoinMarketCap [online]. [cit. 2023-03-31]. Dostupné z: https://coinmarketcap.com/currencies/bitcoin/holders/

CoinMarketCap [online]. [cit. 2023-03-31]. Dostupné z: https://coinmarketcap.com/portfolio-tracker/

CoinMarketCap [online]. [cit. 2023-03-31]. Dostupné z: https://coinmarketcap.com/charts/

CoinMarketCap: Bitcoin [online]. [cit. 2023-03-31]. Dostupné z: https://coinmarketcap.com/currencies/bitcoin/

CoinMarketCap: Portfolio [online]. [cit. 2023-03-31]. Dostupné z: https://coinmarketcap.com/portfolio-tracker/

CoinMarketCap: Top Cryptocurrency Spot Exchanges [online]. [cit. 2023-03-31]. Dostupné z: https://coinmarketcap.com/rankings/exchanges/

Coinmate [online]. [cit. 2023-03-31]. Dostupné z: https://coinmate.io/pages/secured/withdrawal.page

Coinmate [online]. [cit. 2023-03-31]. Dostupné z: https://coinmate.io/

Coinmate [online]. [cit. 2023-03-31]. Dostupné z: https://coinmate.io/pages/secured/trade.page

Coinmate: Home [online]. [cit. 2023-03-31]. Dostupné z: https://coinmate.io/cs

Coinmate: Výběr [online]. [cit. 2023-03-31]. Dostupné z: https://coinmate.io/pages/secured/withdrawal.page

ČNB: Kurzy devizového trhu [online]. [cit. 2023-03-31]. Dostupné z: https://www.cnb.cz/cs/financni-trhy/devizovy-trh/kurzy-devizoveho-trhu/kurzy-devizoveho-trhu/index.html?date=01.01.2023

E15: Další oběť pádu burzy FTX. Půjčovna kryptoměn BlockFi vyhlásila bankrot [online]. [cit. 2023-03-31]. Dostupné z: https://www.e15.cz/kryptomeny/dalsi-obet-padu-burzy-ftx-pujcovna-kryptomen-blockfi-vyhlasila-bankrot-1395177

E15: Hořký konec kryptobanky. Uvízly v ní tisíce Čechů, ukazují dokumenty [online]. [cit. 2023-03-31]. Dostupné z: https://www.e15.cz/kryptomeny/horky-konec-kryptobanky-uvizly-v-ni-tisice-cechu-ukazuji-dokumenty-1394177

E15: Inflace [online]. [cit. 2023-03-31]. Dostupné z: https://www.e15.cz/inflace-v-cr-a-ve-svete-ceny-graf

E15: Kryptoměnová burza FTX přišla o licenci pro působení v EU, v USA vyhlásila bankrot [online]. [cit. 2023-03-31]. Dostupné z: https://www.e15.cz/kryptomeny/kryptomenova-burza-ftx-prisla-o-licenci-pro-pusobeni-v-eu-v-usa-vyhlasila-bankrot-1394819

E15: Kryptoměny [online]. [cit. 2023-03-31]. Dostupné z: https://www.e15.cz/bitcoin-wiki?fbclid=IwAR25qrgD3BD293H1nVis4MfxVxpV6U6tHDSAQTWLxh1klK0xzyZqRyX06UM#penezenka_btc

E15: Mapa inflace [online]. [cit. 2023-03-31]. Dostupné z: https://www.e15.cz/inflace-v-cr-a-ve-svete-ceny-graf

E15: NFT přehledně: Kde koupit a jak vytvořit token, jenž hýbe kryptosvětem [online]. [cit. 2023-03-31]. Dostupné z: https://www.e15.cz/kryptomeny/nft-prehledne-kde-koupit-a-jak-vytvorit-token-jenz-hybe-kryptosvetem-1383564

E15: Pád kryptoburzy. Po krachu FTX se smráká i nad Crypto.com a BlockFi [online]. [cit. 2023-03-31]. Dostupné z: https://www.e15.cz/kryptomeny/pad-kryptoburz-po-krachu-ftx-se-smraka-i-nad-crypto-com-a-blockfi-1394927

E-on: Kolik stojí kWh energie [online]. [cit. 2023-03-31]. Dostupné z: https://www.eon.cz/radce/zelena-energie/ceny-energie/kolik-stoji-kwh-energie/

Finex [online]. [cit. 2023-03-31]. Dostupné z: https://finex.cz/co-jsou-kryptomenove-seedy-a-proc-jsou-pro-vas-dulezite/

Finex [online]. [cit. 2023-03-31]. Dostupné z: https://finex.cz/trezor-model-one-spusteni-navod/

Finex: Akciový index S&P500 [online]. [cit. 2023-03-31]. Dostupné z: https://finex.cz/index/standard-and-poors-500/

Finex: Co je to spread? [online]. [cit. 2023-03-31]. Dostupné z: https://finex.cz/co-je-to-spread/

Finex: Coinmate [online]. [cit. 2023-03-31]. Dostupné z: https://finex.cz/recenze/coinmate//

Finex: Decentralizovaná P2P burza Bisq [online]. [cit. 2023-03-31]. Dostupné z: https://finex.cz/recenze/bisq/

Finex: Decentralizované burzy [online]. [cit. 2023-03-31]. Dostupné z: https://finex.cz/rubrika/kryptomeny/decentralizovane-burzy/?ac=decentralizova&sc=autocomplete

Finex: Jak nakoupit nebo prodat bitcoin v automatu [online]. [cit. 2023-03-31]. Dostupné z: https://finex.cz/jak-nakoupit-nebo-prodat-bitcoin-v-automatu/

Finex: Jak se těží bitcoin? Co je těžba bitcoinu a jak funguje? [online]. [cit. 2023-03-31]. Dostupné z: https://finex.cz/jak-se-tezi-bitcoin-co-je-to-tezba-bitcoinu-a-jak-funguje/

Finex: Kryptoměnová směnárna Anycoin [online]. [cit. 2023-03-31]. Dostupné z: https://finex.cz/recenze/anycoin/

Finex: Kryptoměnové burzy [online]. [cit. 2023-03-31]. Dostupné z: https://finex.cz/rubrika/kryptomeny/burzy/

Finex: Kryptoměnové směnárny [online]. [cit. 2023-03-31]. Dostupné z: https://finex.cz/rubrika/kryptomeny/krypto-smenarny/

Finex: Recenze burzy Binance [online]. [cit. 2023-03-31]. Dostupné z: https://finex.cz/recenze/binance/

Finex: Recenze nurzy burzy Coinbase Pro [online]. [cit. 2023-03-31]. Dostupné z: https://finex.cz/recenze/coinbase-pro/

Finex: S&P500 [online]. [cit. 2023-03-31]. Dostupné z: https://finex.cz/index/standard-and-poors-500/

Finex: Těžba [online]. [cit. 2023-03-31]. Dostupné z: https://finex.cz/rubrika/kryptomeny/tezba/

Finex: Trezor Model One – Spuštění nové peněženky krok za krokem [online]. [cit. 2023-03-31]. Dostupné z: https://finex.cz/trezor-model-one-spusteni-navod/

Forbes: Todays's Winners and Losers [online]. [cit. 2023-03-31]. Dostupné z: https://www.forbes.com/real-time-billionaires/#5c0e9a593d78

Hashrate Index [online]. [cit. 2023-03-31]. Dostupné z: https://data.hashrateindex.com/chart/bitcoin-price-and-difficulty

Hashrate Index [online]. [cit. 2023-03-31]. Dostupné z: https://hashrateindex.com/rigs/bitmain-antminer-s19jpro+

Hashrate Index: 10 Bitcoin Mining Predictions for 2023 [online]. [cit. 2023-03-31]. Dostupné z: https://hashrateindex.com/blog/10-bitcoin-mining-predictions-for-2023/

Hashrate Index: ASIC Index data [online]. [cit. 2023-03-31]. Dostupné z: https://data.hashrateindex.com/asic-index-data

Hashrate Index: ASIC Rigs [online]. [cit. 2023-03-31]. Dostupné z: https://hashrateindex.com/rigs

HedgewithCrypto: How much Bitcoin is lost forever? [online]. [cit. 2023-03-31]. Dostupné z: https://www.hedgewithcrypto.com/how-much-bitcoin-is-lost/¨

iDnes: Zlato kvůli válce na Ukrajině značně posiluje. Kryptoměny začínají krvácet [online]. [cit. 2023-03-31]. Dostupné z:

https://www.idnes.cz/ekonomika/zahranicni/zlato-bitcoin-investice-riziko-pokles-cena-ukrajina.A220224_094020 _eko-zahranicni_jla

Imore: imore. Bitcoinový bankomat: Jak funguje a jak jej používat? [online]. [cit. 2023-03-31]. Dostupné z: https://www.imore.cz/post/14512-bitcoinovy-bankomat-jak-funguje-a-jak-jej-pouzivat

Infinite Market Cap [online]. [cit. 2023-03-31]. Dostupné z: https://8marketcap.com/

InGoldWeTrust [online]. [cit. 2023-03-31]. Dostupné z: https://ingoldwetrust.report/chart-gold-bitcoin-marketcap/?lang=en

Kriptomat: Co je tržní kapitalizace kryptoměny? [online]. [cit. 2023-03-31]. Dostupné z: https://kriptomat.io/cs/kryptomeny/co-je-trzni-kapitalizace-kryptomeny/

Kriptomat: Jak funguje těžení kryptoměn [online]. [cit. 2023-03-31]. Dostupné z: https://kriptomat.io/cs/kryptomeny/co-je-to-tezba-kryptomen/

Kurzy.cz [online]. [cit. 2023-03-31]. Dostupné z: https://www.kurzy.cz/komodity/cena-elektriny-graf-vyvoje-ceny/

Kurzy.cz: Burzy a směnárny kryptoměn [online]. [cit. 2023-03-31]. Dostupné z: https://www.kurzy.cz/kryptomeny/burzy-smenarny

Kurzy.cz: Elektřina [online]. [cit. 2023-03-31]. Dostupné z: https://www.kurzy.cz/komodity/cena-elektriny-graf-vyvoje-ceny/1kWh-czk-1-rok?dat_field=01.01.2013&dat_field2=01.01.2023/

Kurzy.cz: Institucionální investoři nezpomalují s nákupy Bitcoinu, kolik ho vlastní? [online]. [cit. 2023-03-31]. Dostupné z: https://www.kurzy.cz/zpravy/607834-institucionalni-investori-nezpomaluji-s-nakupy-bitcoinu-kolik-ho-vlastni/

Ledger: Non-Custodial Wallet [online]. [cit. 2023-03-31]. Dostupné z: https://www.ledger.com/academy/glossary/non-custodial-wallet

LYNX [online]. [cit. 2023-03-31]. Dostupné z: https://www.lynxbroker.cz/investovani/burzovni-trhy/burzovni-informace/obchodovani-burza/investicni-pojmy/

Michael: Michael J. Saylor [online]. [cit. 2023-03-31]. Dostupné z: https://www.michael.com/ Miras. [online]. Dostupné z: https://www.miras.cz/akcie/moznosti-investovani.php

Money Control [online]. [cit. 2023-03-31]. Dostupné z: https://www.moneycontrol.com/europe/?url=https://www.moneycontrol.com/news/business/cryptocurrency/mining-and-hash-rate-difficulty-at-all-time-high-amid-bitcoin-slump-9100341.html

Portu [online]. [cit. 2023-03-31]. Dostupné z: https://www.portu.cz/blog/11-pojmu-ktere-by-mel-znat-kazdy-zacinajici-investor/

ProShares: BITO Bitcoin Strategy ETF [online]. [cit. 2023-03-31]. Dostupné z: https://www.proshares.com/our-etfs/strategic/bito

River Financial [online]. [cit. 2023-03-31]. Dostupné z: https://river.com/learn/who-creates-new-bitcoin/

Roklen24: Nejhorší den a měsíc pro trhy? [online]. [cit. 2023-03-31]. Dostupné z: https://roklen24.cz/nejhorsi-den-a-mesic-pro-trhy-pozor-na-pondeli-a-zari/

SoFi Learn: Bitcoin Hash Rate adn Why It Matters [online]. [cit. 2023-03-31]. Dostupné z: https://www.sofi.com/learn/content/bitcoin-hash-rate/

Štosuj.cz [online]. [cit. 2023-03-31]. Dostupné z: https://stosuj.cz/

Štosuj.cz: Můj přehled [online]. [cit. 2023-03-31]. Dostupné z: https://stosuj.cz/dashboard

Teorie grafů: Teorie her [online]. [cit. 2023-03-31]. Dostupné z: https://teorie-grafu.cz/vybrane-problemy/teorie-her.php

Trezor [online]. [cit. 2023-03-31]. Dostupné z: https://blog.trezor.io/trezor-one-tamper-evident-packaging-f98d3f63569d

Trezor: Start [online]. [cit. 2023-03-31]. Dostupné z: https://trezor.io/start

Trezor: Trezor Model One [online]. [cit. 2023-03-31]. Dostupné z: https://trezor.io/trezor-model-one

Tuesday: Bitcoin a další kryptoměny [online]. [cit. 2023-03-31]. Dostupné z: https://www.tuesday.cz/akce/bitcoiny/

USA Today [online]. [cit. 2023-03-31]. Dostupné z: https://eu.usatoday.com/in-depth/money/2020/05/12/coronavirushow-u-s-printing-dollars-save-economy-during-crisis-fed/3038117001/

Worldcoin: All you need to know about China's crypto ban [online]. [cit. 2023-03-31]. Dostupné z: https://worldcoin.org/articles/china-crypto-ban

YCharts: Těžba [online]. [cit. 2023-03-31]. Dostupné z: https://ycharts.com/indicators/bitcoin_network_hash_rate

Živě: Bitcoin na rekordní ceně. K novému ATH jej vyhnalo klíčové rozhodnutí americké Komise pro cenné papíry [online]. [cit. 2023-03-31]. Dostupné z: https://www.zive.cz/clanky/bitcoin-na-rekordni-cene-k-novemu-ath-jej-vyhnalo-klicove-rozhodnuti-americke-komise-pro-cenne-papiry/sc-3-a-212946/default.aspx

8 Seznam obrázků, tabulek, grafů a zkratek

8.1 Seznam obrázků

8.2 Seznam tabulek

8.3 Seznam grafů

8.4 Seznam použitých zkratek

2FA = dvou faktorové ověření

AML = Anti Money Laundering = proti praní špinavých peněz

ASIC = Application Specific Integrated Circuit = zákaznický integrovaný obvod

ATH = all time high = cenové maximum

ATM = Automated Teller Machine = bankomat

B = bajt

BCH = Bitcoin Cash

bil. = bilion

BITO = Bitcoin Strategy ETF

BTC = Bitcoin

CEO = Chief Executive Officer = výkonný ředitel obchodní společnosti

CEX = centralizovaná burza

CPU = centrální procesorová jednotka

CZK = Česká koruna

ČNB = Česká národní banka

ČR = Česká republika

dB = decibel

DCA = Dollar Cost Averaging = strategie průměrného dolarového nákupu

DEX = decentralizovaná burza

DPFO = daň z příjmů fyzických osob

DPH = daň z přidané hodnoty

ECDSA = The Elliptic Curve Digital Signature Algorithm = Algoritmus digitálního podpisu s využitím eliptických křivek

Eh/s = exahash za sekundu

ETF = Exchange Traded Fund = veřejně obchodovaný fond

EUR = euro

FIFO = First In, First Out = první dovnitř, první ven

FO = fyzická osoba

FOMO = Fear Of Missing Out = strach u ušlé příležitosti

FUD = Fear, Uncertainty, Doubt = strach, nejistota, pochyby

Gh/s = gigahash za sekundu

h/s = hash za sekundu

IP = internetový protokol

kB = kilobyte

Kč = korun českých

kh/s = kilohash za sekundu

kWh = kilowatt hodin

KYC = Know Your Customer = poznej svého zákazníka

LIFO = Last In, First Out = poslední dovnitř, první ven

LN = Lightning Network

MB = megabajt

Mh/s = megahash za sekundu

mld. = miliarda

NFT = Non-Fungible Tokens = nezastupitelných token

NYA = New York Agreement = New Yorská dohoda

NYKNYC = Not Your Keys, Not Your Coins = nevlastníte-li svoje klíče, nevlastníte svoje mince

OSVČ = osoba samostatně výdělečně činná

p.a. = per annum = za rok

P2P = peer-to-peer = klient-klient

Ph/s = petahash za sekundu

PIN = Personal Identification Number = osobní identifikační číslo

PoW = Proof of Work = důkaz o vynaložené práci

QR = Quick Response = kód rychlé reakce

ROI = Return On Investment = návratnost investice

ROR = Rate Of Return = rentabilita, míra návratnosti

SEPA = Single Europe Payment Area = jednotná oblast pro platby v eurech

SPV = Simplified Payment Verification = zjednodušené ověřování plateb

Th = terahash

Th/s = terahash za sekundu

UAHF = User Activated Hardfork = uživatelsky aktivovaný Hardfork

UASF = User Activated Softfork = uživatelsky aktivovaný Softfork

USA = Spojené státy americké

USB = univerzální sériová sběrnice

USD = Americký dolar

W = watt