# ZÁPADOČESKÁ UNIVERZITA V PLZNI

FAKULTA EKONOMICKÁ


Bakalářská práce

# Kryptoměny, ekonomické zhodnocení možností těžby

# Cryptocurrency, economic analysis of mining


Lenka Davídková



Plzeň 2021

**Čestné prohlášení**

Prohlašuji, že jsem bakalářskou práci na téma

„*Kryptoměny, ekonomické zhodnocení možností těžby*“

vypracovala samostatně pod odborným dohledem vedoucího bakalářské práce za použití pramenů uvedených v přiložené bibliografii.

V Plzni dne

……..…….

Podpis autora

**Poděkování**

V první řadě bych ráda poděkovala svému vedoucímu práce Ing. Václavu Martinovskému za odborný dohled, vedení a cennou pomoc při zpracování této práce. Dále poděkování patří mé rodině za podporu během celého studia.

# Obsah

# Úvod

Bakalářská práce se zabývá studiem tématu kryptoměn a jejich ekonomického zhodnocení těžby. Jelikož se v současné době kryptoměny pohybují na svých dosavadních maximech, je téma značně aktuální. Tento fakt způsobuje zvýšený zájem o danou oblast, a to nejen z pohledu investorů, ale i z pohledu běžných uživatelů či těžařů. Kryptoměny jsou atraktivní investiční příležitostí mimo jiné díky svému decentralizovaného charakteru, a to i navzdory jejich vysoké volatilitě. Konzervativní investoři však na tuto oblast trhu mohou stále pohlížet jako na velmi málo prozkoumanou zónu a označovat ji za rizikovou.

Hlavním cílem této práce je zhodnotit jednotlivé možnosti těžby kryptoměn a analyzovat jejich výhodnost. Vedle tohoto cíle jsou zvoleny i další, které vhodným způsobem hlavní cíl doplňují a obohacují ho o širší kontext. Jedná se zejména o definici kryptoměn a jejich ekosystému z obecného hlediska, popis základních principů kryptografie, šifrování a dalších aspektů. Dále se jedná o uvedení demonstrativního výčtu způsobů získávání kryptoměn a zevrubného popisu problematiky těžby.

Záměrem práce je poskytnout potenciálnímu zájemci o těžbu kryptoměn ucelený přehled vstupů a rizik s těžbou spojených tak, aby si mohl v daném místě a čase sám vypočítat pravděpodobnou návratnost investice a uvážit příslušná rizika.

Práce bude strukturována do dvou částí, teoretické a praktické. Základem teoretické části bude seznámení čtenáře s elementárními pojmy z oblasti kryptoměn. V první řadě bude vysvětlen samotný pojem kryptoměny a jejich dělení. Dále také dojde k nastínění některých druhů kryptoměn a nezbytnou částí pak bude vysvětlení fungování ekosystému, aby došlo k pochopení principu těžby. Těžbě se bude věnovat celá kapitola, jelikož před zahájením procesu těžby je nezbytné tuto problematiku podrobně znát a porozumět ji. V neposlední řadě bude v práci pojednáno o kryptoměně jako o investičním nástroji, kde budou popsány určité způsoby pořízení kryptoměn a zohledněna zásadní kritéria, se kterými by měl být potencionální investor seznámen. Práce se okrajově věnuje i legálnímu a daňovému hledisku, neboť tato hlediska je třeba s ohledem na platnou legislativu brát v potaz.

V druhé části práce dojde k seznámení čtenáře s metodikou výpočtu, která je použita při zhodnocení těžby kryptoměn. V této části práce bude uveden výčet jednotlivých parametrů,

které budou přímo vstupovat do výpočtu. Podstatné zastoupení zde bude mít i kapitola vysvětlující konkrétní rozhodovací kritéria, která je nutné před procesem těžby uvážit.

V části, která se bude věnovat výpočtu rentability dojde k dosazení do namodelovaného výpočtového vzorce, který bude podrobně definovaný již v metodice. Dosazením do tohoto vzorce si bude moci potenciální investor spočítat zhodnocení vlastního vloženého kapitálu. V této práci budou do vzorce dosazena data související s referenční kryptoměnou Bitcoin, která bude sloužit jako vzor pro případné dosazení dalších druhů kryptoměn, respektive odlišných parametrů související s jakoukoliv další kryptoměnou.

Hypotézou práce je především definování výpočetního vzorce a zároveň zohlednění historického vývoje a jiných atributů s kryptoměnami souvisejících, např. značné volatility kryptoměn. Proto bude výpočet aplikovaný v určitém časovém horizontu, aby došlo k věrnému zachycení tendencí chování proměnných vstupů v závislosti na výstupech v čase.

Po posouzení těchto dílčích aspektů bude možné předložit čtenáři jeden z možných způsobů, jak posoudit výhodnost těžby jím zvolené kryptoměny při zohlednění důležitých aspektů a vnějších vlivů. Potencionální investor si pak bude moci zanalyzovat jím zvolenou kryptoměnu.

# 1 Teoretická část

## 1.1 Pojem

Kryptoměna je virtuální měna, která nese hodnotu a není emitována centrální autoritou, nýbrž vzniká nezávisle na ní. Převody a veškeré transakce probíhají bez dozoru centrálního regulátora. Je akceptována jako prostředek platby, lze ji elektronicky převádět, uložit, anebo s ní obchodovat.

S narůstajícím počtem kryptoměn může být tato definice nepřesná. Aby nedocházelo k záměně pojmu kryptoměna s jinými typy měn a jiných platebních prostředků, je definici třeba zúžit a pojmout do ní další podmínky jako např.:

- je decentralizovaná a není vydávána centrální autoritou
- uchovává přehled o jednotkách a jejich vlastnictví
- prokazování vlastnictví je formou šifrovaného kódu
- je určeno, zda mohou či nemohou vznikat nové jednotky kryptoměny, pokud vznikají jednotky nové, je zde určeno, jak vznikají a kdo bude jejich vlastníkem
- pouze vlastník kryptoměny může zadávat a provádět transakce

Při splnění výše uvedených podmínek lze tedy prohlásit, že se jedná o kryptoměnu, která splňuje definici[1].

[1] LÁNSKÝ, Jan. Kryptoměny. 1. vyd. Praha: C. H. Beck, 2018. s. 2-3.

## 1.2 Vlastnosti kryptoměn

Pro ještě přesnější přiblížení toho, co je to kryptoměna, a zvlášť pak pro pochopení, co je její podstatou, jak na ní reagují ekonomické subjekty, jaké jsou možnosti jejího využití a teď je třeba důkladně popsat, její jednotlivé vlastnosti[2].

### Decentralizace

Mezi obecnou vlastnost digitálních měn se řadí decentralizace. Spočívá v existenci měny bez řízení jediného organizačního ústředí. Dohled nad veškerými pohyby a transakcemi vykonávají běžní uživatelé pomocí tzv. blockchainu[3].

### Dělitelnost

Kryptoměny jsou dělitelné, pokud lze jednotku rozdělit na jednotky menší, např. nejvyšší jednotkou Bitcoinu je 1 BTC a nejnižší je 1 Satoshi = 0.00000001 BTC. Jedná se o jednu z důležitých vlastností, kterou měny vykazují[4].

### Přenositelnost a uchovatelnost

Kryptoměny je možné uchovávat a přenášet. Uchovávat je lze na speciálním účtě, ve virtuální či hardwarové peněžence, anebo jiných místech k tomu určených. Uchovává se prostřednicvím kódu, resp. ve formě digitální informace. Tento kód lze uchovávat i vytisknutý na papíře, na pevném disku či flash disku. Pro ještě bezpečnější uchovávání se používají hardwarové peněženky např. Trezor nebo Ledger.[5]

---

[2] Někdy již samotná definice kryptoměny obsahuje její vlastnosti, jako například "Kryptoměny vznikaly původně jako programátorský teoretický koncept. Decentralizované, nepadělatelné a neovlivnitelné měny, oddělené od konkrétního subjektu, který by mohl měnu ovlivňovat (tisknout, devalvovat)." V některých případech se zahrnutí vlastnost do definice nelze vyhnout, což ale v nadměrné míře může způsobovat nepřesnosti v další interpretaci dle Kryptoměny a Bitcoin. Kam investovat? Vzdělávej se a propoj s odborníky [online]. [cit. 27.4.2021]. Dostupné z: https://investree.cz/category/kryptomeny/

[3] ROTHSTEIN, Adam. The End of Money The Story of bitcoin, cryptocurrencies and the blockchain revolution. London: Hodder & Stoughton General Division, 2017. p. 35 – 36 ISBN 978-1473-62953-0.

[4] STROUKAL, Dominik a Jan SKALICKÝ. Bitcoin a jiné kryptopeníze budoucnosti: historie, ekonomie a technologie kryptoměn, stručná příručka pro úplné začátečníky. 2., rozšířené vydání. Praha: Grada Publishing, 2018. Finance pro každého. s. 32

[5] STROUKAL, Dominik a Jan SKALICKÝ. Bitcoin a jiné kryptopeníze budoucnosti: historie, ekonomie a technologie kryptoměn, stručná příručka pro úplné začátečníky. 2., rozšířené vydání. Praha: Grada Publishing, 2018. Finance pro každého. s. 33

**Zaměnitelnost**

Všechny jednotky kryptoměny jsou navzájem zaměnitelné, a tedy každá z jednotek má stejnou hodnotu.[6]

**Omezené množství**

Kryptoměny mají předem určené množství jednotek v oběhu. Např. kryptoměna Bitcoin má přesně definované množství jednotek přímo ve zdrojovém kódu, a to 20 999 999, 9769 BTC.

## 1.3 Dělení a druhy kryptoměn

Tvorba nových kryptoměn v zásadě není omezena. Limitována je pouze znalostmi programování a hardwarem pro její vývoj, který není však na tolik specifický, aby byl dostupný jenom v úzkém okruhu programátorů. Dá se říci, že v současné době trend vzniku nových kryptoměn sílí, což lze přisuzovat úspěšnosti již známých a zaběhnutých kryptoměn, jako například Bitcoin, který se stal jedním z prvních zástupců kryptoměn, se kterým je možné provést peněžní transakci, de facto zaplatit. O úspěšnosti nové kryptoměny rozhoduje její atraktivita, resp. zájem těžařů a investorů.

Kryptoměny lze rozdělit dle různých kritérií, např. využívaného algoritmu.

**Kritérium algoritmu**

**Proof of work (PoW)** – tzv. důkaz o práci je algoritmus, který funguje na principu řešení obtížných matematických operací, které vypočítává těžař, resp. jeho těžební počítač. Za úspěšné vyřešení matematické úlohy těžař získává odměnu v podobě nově vytěžené kryptoměny. Do systému vstupují bloky transakcí, které mají předem definovaná pravidla, která obsahují značné množství dat. Těžaři pak převádějí tyto bloky, pomocí hashovací funkce na hash (např. u Bitcoinu je využívána hashovací funkce SHA256). Hash je pouze zlomkem bloku a obsahuje krátký řetězec symbolů. V tomto algoritmu je důležitá tzv. nonce, kterou těžaři používají k iteraci výstupu svých hash výpočtů. Na řešení těchto obtížných matematických operacích se

[6] Tamtéž

podílí velké množství těžařů, ten, který z nich jako první vypočítá validní nonci, tedy platný hash bloku, má právo zařadit blok do Blokchainu, za což mu náleží odměna v podobě nově vytěžené kryptoměny.[7]

**Proof of Stake (PoS) –** tzv. důkaz o podílu je algoritmus, který ke svém fungování nepotřebuje těžaře. Jsou nahrazeny validátory, kteří ověřují transakce, za které jsou odměňováni. Validátorem se stává ten, kdo odešle speciální transakci, ve které dojde k uzamčení prostředků, což pak slouží jako depozit. Tvorby nových bloků se mohou účastnit všichni validátoři, kteří jsou náhodně vybráni. Výběr je přímo závislý na výši vloženého depozitu. Pokud validátor validuje nesprávné transakce, přijde o celý svůj vložený depozit. K tvorbě nových bloků se nevyužívá energie, avšak množství investovaných peněz.[8]

## Druhy kryptoměn

### Bitcoin (BTC)

Virtuální měna P2P Bitcoin vznikla v roce 2009, jejímž zakladatelem je vývojář Satoshi Nakamoto, o jehož osobě je dnes minimum informací.[9] Bitcoin má předem dané množství jednotek v oběhu, přesně 20 999 999, 9769 BTC. Uvolňování Bitcoinů do oběhu je definováno ve zdrojovém kódu sítě. V oblasti těžby platí pravidlo, čím více vytěžených jednotek Bitcoinů v oběhu, tím je těžba náročnější. Těžba nových kryptoměn funguje na algoritmu Proof of Work.

V současnosti má Bitcoin omezenou dělitelnost na osm desetinných míst. Nejvyšší možnou jednotkou Bitcoinu je 1 BTC a nejnižší možnou jednotkou je 1 Satoshi = 1/100 000 000 BTC.[10]

[7] Nonce | Binance Academy. [online]. [cit. 27.4.2021]. Dostupné z: https://academy.binance.com/en/glossary/nonce
[8] Proof-of-stake (PoS) | ethereum.org. [online].[cit. 27.4.2021]. Dostupné z: https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/
[9] POPPER, Nathaniel. Digital gold: bitcoin and the inside story of the misfits and millionaires trying to reinvent money. New York: Harper, 2016. ISBN 9780062362506.
[10] OZORA, Ogino: PROOF-OF-STAKE (POS) [online].[cit. 27.4.2021]. Dostupné z: https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/

K zabezpečení sítě se používá kryptografie, která šifruje data pomocí protokolu SHA-256, který zabezpečuje síť proti hackerským útokům, např.: collision útokům, pre-image[11] útokům aj. Hodnota Bitcoinu závisí na směnném kurzu, který je prudce volatilní a je důležité ho sledovat, jeho výše k datu 28.4.2021 je: 53 633 $[12].

Obrázek 1 - Vývoj kurzu Bitcoinu v čase[13]


**Bitcoin Cash (BCH)**

Z virtuální měny Bitcoin se v roce 2017 oddělila nová měna Bitcoin Cash. Je omezena na 21 milionů jednotek této kryptoměny. Přičemž v listopadu roku 2018 bylo vytěženo již 17,5 milionu jednotek tzn., že během jednoho roku se vytěžilo více než 75 % dostupných zdrojů. Pro těžbu využívá protokol Proof of Work. Důvodem rozdělení bylo ohromné přibývání transakcí a díky tomu docházelo ke zpomalení ověřování transakcí, které se běžně pohybovalo až kolem jedné hodiny. Jeden blok je omezen na 1 MB, tzn. že za minutu je schopen systém

[11] Jak funguje Bitcoin? [online].[cit. 27.4.2021] Dostupné z: http://kryptostart.cz/kryptomeny/bitcoin/
[12] BITCOIN - Kurz BTC/Bitcoin [online].[cit. 27.4.2021]. Dostupné z: http://www.kurzy.cz/bitcoin/
[13] tamtéž

zpracovat cca 3 transakce. S porovnáním např.: s Visa, která za minutu zpracovává až 1677 transakcí, je tento výsledek limitující pro provádění běžných plateb. Díky tomu vzniká „hard fork“ (programátorský výraz pro odvětví kódu) Bitcoinu – Bitcoin Cash, který částečně řeší problém s rychlostí zpracovávání transakcí[14].

Bitcoin Cash vznikl začátkem srpna 2017. Z počátku se směnný kurz pohyboval kolem 555 $. K datu 27.4.2021 je kurz 883 $.[15]

Obrázek 2 - Vývoj kurzu Bitcoin Cash v čase[16]


[14] Kurzy.cz, spol. s. r. o., AliaWeb, spol. s.r.o.[online]. [cit. 23.04.2019]. Dostupné z: https://bitcoinblog.cz/
[15] Bitcoin Cash - aktuální a historické ceny kryptoměny [online]. [cit. 23.04.2019]. Dostupné z: http://www.kurzy.cz/komodity/bitcoin-cash-graf-vyvoje-ceny/usd
[16] tamtéž

**Ethereum (ETH)**

Digitální měna Ethereum Virtual Machine, fungující na decentralizované databázi blockchainu. Vznikla 30. července v roce 2015. Autory jsou Vitalik Buterin a Gavin Wood. Transakce se zde provádí pomocí tokenu ETH a funguje na protokolu Proof of Work. Jedná se o kryptoměnu s konceptem tzv. next-generation, to znamená, že nemá předem určený konečný počet jednotek v oběhu. Omezený je však počet nově přibývajících bloků za rok a to na 18 milionů ETH. Ethereum ukládá zdrojové kódy a stavy výpočtů, na nichž jsou postaveny aplikace „smart contracts“. Aplikace slouží pro uzavírání pomyslných smluv mezi dvěma stranami a lze o nich hovořit jako o způsobu financování ICO (Initial Coin Offering). Chytré kontrakty nahrazují crowdfundingové platformy. Výhodou je, že autoři mohou předem nadefinovat podmínky pro investory. V roce 2017 ICO vybralo 5,6 miliard $ na podpoření nejrůznějších startupů. Dalším možným využitím chytrých kontraktů může být sázení. Například na výsledky sportovních zápasů. Kdy se povede podmíněný kontrakt, který bude potvrzen ve chvíli splnění podmínky, tedy tipnutí si správného výsledku sportovního zápasu.[17]

**Dash (DASH)**

Kryptoměna vznikla v roce 2014 s názvem XCoin, ještě v tom samém roce byla přejmenována na Darcoin. Název Dash získala v březnu 2019. Používá hashovací funkci řetězeného hashování X11, která má 11 hashovacích funkcí. Využívá algoritmus Proof of Work. Oproti ostatním kryptoměnám je více zaměřena na anonymitu, což zajišťuje obtížnější dohledávání původu jednotek kryptoměny.[18] K datu 27.4.2021 je kurz 289 $.[19]

[17] How does Ethereum work, anyway?. Introduction | by Preethi Kasireddy | Medium. Preethi Kasireddy – Medium [online]. [cit. 23.04.2019]. Dostupné z: https://preethikasireddy.medium.com/how-does-ethereum-work-anyway-22d1df506369

[18] Mining - Dash. Dash - Dash is Digital Cash You Can Spend Anywhere [online].[cit. 23.04.2019]. Dostupné z: https://www.dash.org/mining/

[19] Dash - DASH/Dash kurz [online].[cit. 23.04.2019]. Dostupné z: http://www.kurzy.cz/dash/

## 1.4 Kryptoměny a jejich ekosystém

### 1.4.1 Ekosystém – Blockchain

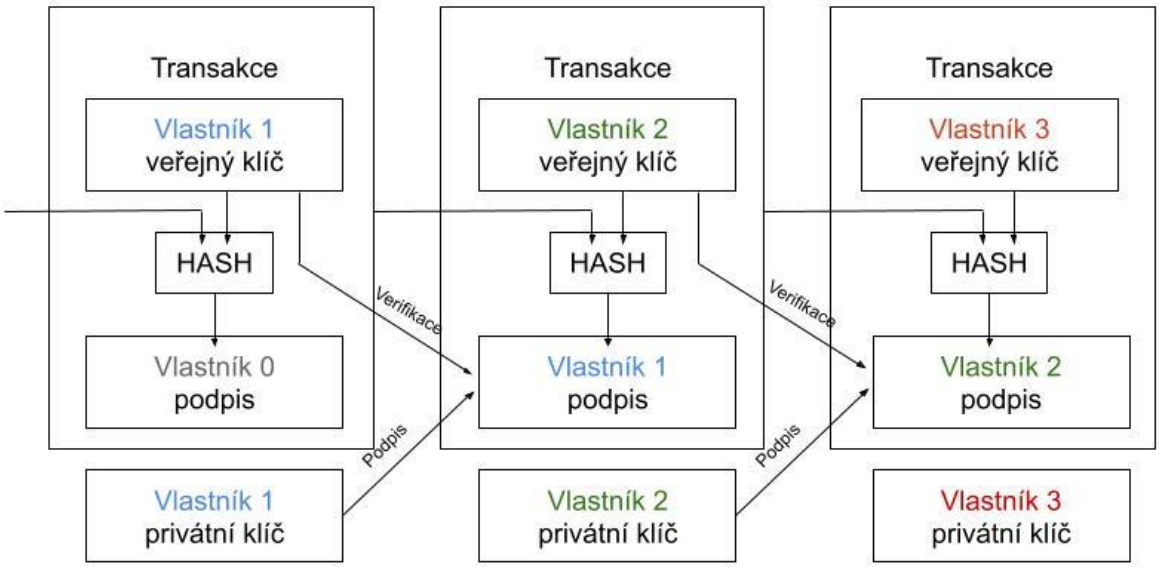
Ekosystém kryptoměn je odlišný od ekosystému fiat měn, o čemž svědčí celá řada rozdílů a vzájemná nekompatibilita těchto dvou ekosystémů. Většina současných kryptoměn funguje na decentralizované distribuované síti blockchainu, kde jsou vedené veškeré operace s kryptoměny. Tyto operace jsou z důvodu bezpečnosti zašifrované pomocí asymetrické kryptografie. Používané jsou dva klíče, privátní a veřejný klíč. K provedení transakce je nezbytné zadání privátního klíče. Uživatel, který chce provést transakci, musí zadat kód privátního klíče, čímž transakci pomyslně podepíše a potvrdí tak svoji identitu, čímž je potvrzena i transakce. V síti blockchainu jsou zaznamenávány kromě transakcí i jednotlivé jednotky kryptoměn, což zabraňuje tzv. Double Attackům.[20]

Pro zabránění tzv. Double Attackům je třeba sledovat transakci, jak se řetězí. Je nezbytné ověřovat, jak uživatel získal jednotku kryptoměny, proto je třeba sledovat historii vlastníků dané jednotky kryptoměny.

Např. Vlastník č. 1 vlastní jednotku, kterou získal od Vlastníka č. 0, aby mohl provést transakci Vlastník 1 transakci s Vlastníkem 2, je zapotřebí zadání veřejného klíče Vlastníkem 2 a poté tzv. podpis Vlastníkem 1, pomocí privátního klíče. Tím je zabráněno, že neproběhne dvojí útrata.

[20] LEE, Kuo, Chuen, David ed. and DENG, H. Robert ed. Handbook of blockchain, digital finance, and inclusion. Volume 1, Cryptocurrency, finTech, insurTech, and regulation [online]. London, England: Academic Press, 2018, [cit. 2021-05-10]. ISBN 978-0-12-810442-2. Dostupné z: https://ebookcentral.proquest.com/lib/natl-ebooks/detail.action?docID=4939374

Obrázek 3 - Schéma řetězení transakcí v Blockchainu [21]




**Privátní a veřejný klíč**

U kryptoměn se kryptografické šifrování využívá především pro tři konkrétní účely, a to k zajišťování transakcí, kontrole a vytváření nových jednotek kryptoměn a pro ověřování převodu aktiv. V těchto případech vycházíme z veřejného klíče.

Kryptografie veřejného klíče je spojena s klíčem privátním. Veřejný klíč je totiž hash privátního klíče. Oba klíče jsou šifrované a mají přidělené náhodné kódy, které se skládají z písmen a číslic. Mají přibližně 30 znaků a mohou vypadat např. takto: NUomgIOIln754338MFMkuzk84lihj8. Veřejný klíč zajišťuje poskytování adresy uživatele pro posílání peněz. Privátní klíč je nástroj pro generaci digitálních podpisů. Pomocí privátních klíčů se autentizuje vlastník adresy. Účelem privátního klíče je odemknutí veřejného klíče k tomu, aby mohly být transakce provedeny. Odemknout veřejný klíč dokáže pouze osoba, která zná adresu privátního klíče. Pro lepší pochopení tohoto systému je uveden názorný příklad:

[21] Vlastní zpracování dle informací: ROTHSTEIN, Adam. The End of Money The Story of bitcoin, cryptocurrencies and the blockchain revolution. London: Hodder & Stoughton General Division, p. 33 – 49. ISBN 978-1473-62953-0.

Představte si oranžovou poštovní schránku, která je k dispozici kdekoliv na veřejnosti. Každý do této schránky může vhodit dopis, ale pouze pošťačka může schránku odemknout a odebrat dopis. Privátní a veřejný klíč funguje na stejném principu. Každý může vložit peníze na veřejnou adresu, ale přistup k nim mají pouze uživatelé, kteří znají privátní klíč. Ve světě kryptoměn si můžeme představit, že každý vlastník kryptoměny má svoji schránku a klíč. Tedy pouze skutečný vlastník může provádět transakční operace s vlastněnou kryptoměnou.

Riziko může nastat tehdy, pokud uživatel ztratí svůj privátní klíč, anebo ho odhalí někomu jinému. Při ztrátě privátního klíče již není možnost získat znovu přístup k prostředkům, které má uživatel uložené ve své virtuální peněžence. Při vyzrazení svého privátního klíče třetí osobě, může třetí strana získat přístup k uloženým prostředkům, převzít nad nimi kontrolu a provádět s nimi veškeré transakční operace. [22]

**Bezpečnost privátního klíče**

Pro zachování bezpečnosti privátního klíče, by o něm neměl jeho vlastník sdílet žádné informace. V této problematice je zásadní počínat si velice opatrně. Na internetu probíhá neustálé sbírání dat o uživatelích, a především vlastníci kryptoměn jsou velice atraktivním cílem pro hackerské útoky. Ekosystém není hlídán žádnou centrální autoritou, a pokud tedy dojde k odcizení kryptoměny, neexistuje žádná náhrada škody prostřednictvím centrální autority. Pro vyšší standard bezpečnosti se všeobecně využívají hardwarové peněženky, kam si uživatelé ukládají privátní klíč.

Hardwarová peněženka je externí úložiště, které je dostupné ke koupi na internetu či v elektro prodejnách. Její pořizovací náklady se pohybují v kolem pár tisíců korun. Přístup k hardwarové peněžence není k dispozici v online rozhraní, což poskytuje větší kontrolu nad přístupem do peněženky, navíc nabízejí možnost dalšího zabezpečení heslem. U hardwarové peněženky hrozí minimální riziko odcizení privátního klíče. Největším rizikem je pouze její

[22] Difference between Private key and Public key - GeeksforGeeks. GeeksforGeeks | A computer science portal for geeks [online].[cit. 23.04.2021]. Dostupné z: https://www.geeksforgeeks.org/difference-between-private-key-and-public-key/

ztráta. [23] Dále lze kryptoměny uchovávat v softwarové peněžence, která je dostupná okamžitě a její pořizovací náklady jsou výrazně nižší, až zanedbatelné. Peněženka je druh SW, který je široce dostupný. Přístup do peněženky je umožněn z jakéhokoliv počítače, který je připojený k internetu a chráněn heslem. Nevýhodou je ztráta kontroly nad privátním klíčem, který je vlastněný společností, která SW peněženku poskytuje. To znamená, že riziko možného odcizení může být vysoké. [24]

Rizika spojená s odcizením privátního klíče jsou vysoká, toto riziko lze částečně pokrýt pojištěním. Historicky se ekosystém setkal s obrovskými hackerskými útoky, a to např. v roce 2014 bylo na burze Mt. Gox odcizeno v celkovém součtu 740 000 Bitcoinů od různých uživatelů. V přepočtu na kurz k datu 4.5.2021 se jedná o necelých 41 mil. $.[25]

Mnoho burz, z důvodu bezpečnosti, své kryptoměny uchovává v tzv. Cold Storage Facilities. Napadnut může být tedy pouze zlomek kryptoměn na burze, zbytek uchovávaný v HW zařízeních zůstane ochráněn.

### 1.4.2 Těžba

**Princip**

Základní princip fungování těžby je založen na výpočtu netriviálních matematických operací, ke kterým je vždy přidružena další matematická operace související s potvrzováním transakcí. V souvislosti s těžbou se používá pojem uzel, což je počítač/server těžaře s vysokým výpočetním výkonem. Ten je napojen na síť kryptoměny, ve které řeší matematické operace a získává informace o nových transakcích. Těžař, který matematickou operaci dokáže vyřešit jako první, vyhrává a náleží mu odměna. Zároveň s tímto dojde k zařazení transakce do blockchainu, která v síti probíhá, za což také náleží odměna. Ostatní těžaři, kteří matematickou operaci vyřeší pozdě, musí výsledek zahodit. Jejich snaha není nikterak honorována a musí

[23]Trezor. [online].[cit. 23.04.2019]. Dostupné z: https://trezor.io/
[24] Software wallet [online].[cit. 23.04.2019]. Dostupné z: https://btcdirect.eu/en-gb/software-wallet
[25] Crypto Exchange Hacks: The Mt. Gox Scandal and More | Gemini. Cryptocurrency Exchange to Buy Bitcoin and Ether | Gemini [online]. [cit. 20.04.2021]. Dostupné z: https://www.gemini.com/cryptopedia/mt-gox-bitcoin-exchange-hacked

začít počítat znovu. Již z tohoto základního zjednodušeného popisu těžby je patrné, že mají šanci pouze těžaři s vysokým výpočetním výkonem.

V praxi taková těžba vypadá tak, že si jednotliví těžaři nainstalují speciální program na těžbu kryptoměny na svůj počítač a nechají ho počítat. O výpočty a potvrzování konkrétních transakcí se postará program sám. Velcí hráči na poli těžby si programují vlastní programy a upravují algoritmy pro výpočet matematické úlohy. Tím dosahují maximální optimalizace s ohledem na používaný těžební hardware.

Potvrzení transakce probíhá na principu, že uživatel vytvoří novou transakci a pošle informaci o této transakci všem svým sousedním těžařům v síti. Každý uzel v síti tuto informaci příjme a provede základní ověření transakce. Kontroluje, zdali je zpráva o transakci validní. Tato zpráva obsahuje informaci o adrese příjemce, adrese odesílatele a velikosti posílané částky. Validace probíhá na základě zjištění správných informací a zda odesílatel disponuje takovou částkou, kterou odesílá. Pokud ano, tak posílá informaci o této transakci dalším sousedním těžařům. Tím je u kryptoměn zajištěno, že se sítí šíří pouze správné a bezpečné informace o transakcích. Těžaři si každou tuto informaci ukládají do své mezipaměti. Po určité době těžař nashromáždí potřebné množství transakcí, který se nazývá transakční blok. Ten se uzamkne a započne proces těžby.[26]

Bloky transakcí jsou pro každou kryptoměnu různě veliké. U některých kryptoměn jsou bloky dokonce s variabilní velikostí. Například u nejrozšířenější kryptoměny Bitcoin je velikost bloku pevně určená a má hodnotu 1024 bytů. Proces těžby se na síti provádí paralelně. Těžař tedy stále přijímá a kontroluje další transakce a připravuje si nové bloky, které bude těžit hned po vytěžení předchozího bloku. [27]

Nyní se dostaneme k samotnému výpočtu, který zaručí úspěšné vytěžení bloku. Těžař má za úkol z každého bloku vypočítat hash. Hash je speciální řetězec, který slouží jako určitý druh otisku. Jedná se o kryptografickou metodu, při které se jednoduchým výpočtem dosáhne otisku

[26] MYSLÍN, Josef. Obecné technické aspekty fungování virtuálních měn. In: HUJOVÁ, Gabriela, ed. Zkušenosti s virtuálními měnami - Bitcoin měna budoucnosti?: sborník z konference: Praha, 26. března 2014. Praha: Vysoká škola manažerské informatiky, ekonomiky a práva, 2014. s. 75 -76. ISBN 978-80-86847-71-9.

[27] Mining for nil-transaction blocks only - gaming the incentive scheme by rogue miners / consortium? - Bitcoin Stack Exchange. Bitcoin Stack Exchange [online].[cit. 23.04.2021]. Dostupné z: https://bitcoin.stackexchange.com/questions/41411/mining-for-nil-transaction-blocks-only-gaming-the-incentive-scheme-by-rogue-mi

určitého množství dat. Je ale matematicky náročné reverzně zjistit původní data, ze kterých byl daný hash počítán. Na tomto principu funguje naprostá většina certifikátů a zabezpečení na internetu. Jak již bylo řečeno, výpočet hashe, na rozdíl od jeho dekódování, není nikterak náročná výpočetní operace. Jeho výpočet na povaze algoritmu šifrování a velikosti dat může trvat pouze zlomky vteřin. U kryptoměn jsou ale kladeny nároky na konkrétní podobu kódu, který vznikne výsledkem dešifrování. To danou úlohu značně zesložiťuje, protože vstupní data nesmí těžař nijak měnit. Každá kryptoměna má tato pravidla nastavena jinak, a proto trvá různě dlouhou dobu výpočet bloku. Například u Bitcoinu je složitost výpočtu nastavena tak, že vytěžit jeden blok trvá přibližně 10 minut. Mezi pravidla pro výstupní hash patří například taková, že každý hash musí začínat stejnou skupinou řetězců. [28]

Výpočtové operace při těžbě využívají metodu Proof of Work. Do tohoto systému vstupují bloky transakcí, které mají předem definovaná pravidla a obsahují značné množství dat. Těžaři pak převádějí tyto bloky pomocí hashovací funkce na hash (např. u Bitcoinu je využívána hashovací funkce SHA256). Hash je pouze zlomkem bloku a obsahuje krátký řetězec symbolů. V tomto algoritmu důležitou roli hraje tzv. nonce, kterou těžaři používají k iteraci výstupu svých hash výpočtů. Na řešení matematické operace se podílí velké množství těžařů, pouze ten, který z nich jako první vypočítá validní nonci, tedy platný hash bloku, má právo zařadit blok do Blokchainu, za což mu náleží odměna v podobě nově vytěžené kryptoměny. Hashovací algoritmy lze snadno vypočítat, ale je téměř nemožné reverzně vypočítat vstupní data. Proto si reverzní metodou při výpočtu bloku nelze pomoci. Je tedy nutné nonci měnit náhodně pouze hrubou silou a metodou pokus omyl stále dokola počítat nové a nové hashe, dokud nedostaneme vyhovující výsledek.[29]

Při těžbě se tak setkáváme s metodou „pokus-omyl“ při výpočtech. Je tedy potřeba vysokého výpočetního výkonu, abychom v dané výpočetní smyčce dokázali vypočítat co největší množství hash řetězců za dané časové období. Jedině tak má těžař šanci uspět s potvrzením bloku. S vyšším hrubým výkonem uzlu se značně zvyšuje pravděpodobnost úspěšné těžby. Postupem času se zlepšují algoritmy a výpočetní výkon hardwaru. Proto mají jednotlivé kryptoměny ve svém zdrojovém kódu mechanismy, které jednou za čas mění

[28] STROUKAL, Dominik a SKALICKÝ, Jan. Bitcoin a jiné kryptopeníze budoucnosti: historie, ekonomie a technologie kryptoměn, stručná příručka pro úplné začátečníky. 2., rozšířené vydání. Praha: Grada Publishing, 2018. s. 82 – 87. ISBN 978-80-271-0742-1.
[29] Nonce [online].[cit. 23.04.2021]. Dostupné z: https://academy.binance.com/en/glossary/nonce

složitost výpočtu. Snahou je, aby výpočet trval pořád přibližně stejnou dobu. Lze tedy algoritmus jak ztížit (v případě, že se začnou bloky potvrzovat rychleji), nebo naopak zlehčit (pokud se začnou potvrzování transakcí postupně prodlužovat)[30].

V případě, že uzel těžaře dokáže matematickou úlohu výpočtu požadovaného hashe vyřešit jako první, má právo provést potvrzení bloku a jeho tzv. zaúčtování. V praxi to vypadá tak, že vítězný uzel zašle ostatním těžařům výsledek. Tedy zašle vstupní data v podobě řešeného bloku a poté výstupní data v podobě daného hashe. Na ostatních těžařských uzlech je, aby tento výpočet potvrdili a uznali za správný. Jedná se o další kontrolní mechanismus, který kryptoměny obsahují. Po potvrzení správnosti řešení ostatními uzly v síti, dojde k finálnímu potvrzení. Každá transakce má nějaký stav. Tyto stavy se mohou lišit podle konkrétní kryptoměny, která může blockchain implementovat jiným způsobem. Obecně mají transakce tři základní stavy: uložená, zrušená, uzamčená a potvrzená. Při vytvoření a poslání nové transakce, má jako výchozí stav uložená, pokud není transakce validní, tak je nastavena jako zrušená. V případě zahájení těžby bloku, ve kterém se tato transakce nachází, dojde k jejímu uzamčení. Pokud se povede blok vytěžit a potvrdit jeho správnost, tak se transakcím nastaví stav potvrzená.

Potvrzený blok se může zaúčtovat, to znamená, že se připojí do blockchainu. Blockchain je speciální soubor obsahující bloky s historií všech transakcí. Tento soubor je sdílený napříč sítí mezi uzly, které danou kryptoměnu těží. Jedná se o veřejně dostupný soubor decentralizované měny. Tento vytěžený blok se tedy připojí do blockchain souboru ke starším blokům. Pokud je blok potvrzen a zařazen do blockchainu, tak se jedná o nevratný proces. Transakce z tohoto zaúčtovaného bloku nelze vzít zpět. Teprve až po operaci zaúčtování má těžař nárok na odměnu za vytěžení bloku. Odměna se typicky stává ze dvou částí. Jednou z nich je určitý počet digitálních mincí dané kryptoměny. Ty se vygenerují po každém vytěženém bloku, další částí odměny mohou být poplatky za potvrzení transakcí. Touto odměnou si uživatel pro svojí transakci zajistí, že nějaký těžařský uzel bude mít vůbec zájem jeho transakci zařadit do bloku, který bude zpracovávat. To má často vliv na rychlost, za kterou nějaký těžař vaší transakci potvrdí. Pokud potřebuje uživatel rychle uskutečnit platební transakci, tak je nucen k platbě

[30] Těžba kryptoměn - návod a tipy jak na to | E15.cz. E15.cz - Byznys, politika, ekonomika, finance, události [online].[cit. 23.04.2021]. Dostupné z: https://www.e15.cz/tezba-kryptomen

připojit vyšší odměnu pro těžaře. Tato odměna není povinná, ale dost ovlivňuje, zdali se nějaký těžařský uzel vůbec bude vaší transakcí zaobírat.

Pokud těžař zjistí, že jiný uzel vytěžil blok, tak okamžitě přeruší výpočty a počítaný blok zahodí. Bere další blok s transakcemi, které nasbíral v mezidobí, kdy počítal. Nemůže si být ale jistý, že nový blok náhodou neobsahuje některou transakci, která již byla obsažena v nově vypočteném bloku, proto je zapotřebí nejprve zkontrolovat, že v bloku nejsou žádné transakce, které již byly potvrzeny a zaúčtovány. Jedná se o pasivní kontrolní mechanismus. Lze hovořit o synchronizaci všech těžebních uzlů na základě aktuální verze souboru blockchain. Teprve po provedení této kontroly začne uzel tento nový blok počítat. V některých krajních případech může nastat situace, že nový blok vyřeší více uzlů současně. Díky decentralizaci a prodlevě v komunikaci pak dojde k situaci, že každá část sítě pracuje s jinou verzí blockchainu. To se poté srovná u dalšího bloku, kdy má pro tyto případy daná kryptoměna naprogramovaný rozhodovací mechanismus. [31]

**Prostředky pro těžbu**

V předchozí kapitole popisuji, že je potřeba vysoký výpočetní výkon, aby došlo k rychlému vyřešení matematické operace. Při výpočtu soutěží s ostatními těžaři, aby dokázali tento výpočet vyřešit jako první. Je logické, že se zvyšujícím se počtem těžařů a také výpočetním výkonem jednotlivých uzlů těchto těžařů, rostou nároky na hardware, se kterým lze v těžbě kryptoměn uspět.

V počátcích kryptoměn pro těžbu stačily klasické procesory výkonných počítačů, později bylo zapotřebí pro úspěch těžit na výkonných serverech, nebo na grafických kartách. Grafické karty obsahují grafické procesory, které jsou uzpůsobeny na velice rychlé vektorové výpočty pro renderování a zobrazování grafiky. Výpočty hash otisků jednotlivých bloků kryptoměny se od těchto grafických výpočtů z pohledu procesorů moc neliší. Proto jsou grafické karty pro tyto výpočty vhodnější než klasické procesory. Později bylo potřeba pro rychlé vyřešení úlohy využívat pro výpočet více paralelně zapojených grafických karet. U těch ale začali těžaři

[31] Těžba kryptoměn - návod a tipy jak na to | E15.cz. E15.cz - Byznys, politika, ekonomika, finance, události [online].[cit. 23.04.2021]. Dostupné z: https://www.e15.cz/tezba-kryptomen

pomalu narážet na vysoký příkon, který tyto grafické karty mají. Proto se začaly postupně objevovat speciální procesory a výpočetní ASIC čipy na těžbu kryptoměn. ASIC čipy jsou navrženy přímo pro tyto výpočty a mají značně menší spotřebu elektřiny než grafické karty. [32]

**Těžební pool**

Pro jednotlivé těžaře je stále složitější dosáhnout ziskovosti. Jedním z faktorů je stále se zvyšující nároky na těžební hardware, ten se postupně stává pro jednotlivce finančně nedosažitelný. Dalším výrazným faktorem je cena elektřiny. Jednotlivci mají maloobchodní ceny za elektrickou energii oproti velkým společnostem, které mají zvýhodněnou sazbu ceny. Na začátku v dobách velkého růstu hodnoty největší kryptoměny Bitcoin byla hodnota této měny v korelaci se zvyšující se náročností pro potvrzení bloku (a s ní i spotřebě elektrické energie). Hodnota Bitcoinu však začala klesat a pro malé těžaře začala být těžba stéle méně rentabilní. V druhé polovině roku 2018 se stala těžba Bitcoinu pro většinu malých těžařů prodělečná. Tedy pro potvrzení bloku při těžbě spotřebovali elektrickou energii v hodnotě převyšující valuaci odměny v dané kryptoměně. Jedná se o statistiky, které berou v potaz průměrnou cenu elektřiny v západních zemích. Například v Číně se těžba kryptoměn pro jedince vyplatila mnohem déle, protože průměrná cena elektrické energie pro koncové zákazníky je nižší než v ČR. Dalším faktorem odrazující malé těžaře je samotná odměna za vytěžení jednoho blok, která se mění. Proto se těžaři, kteří i nadále chtějí svůj hardware využívat k těžbě kryptoměn zapojují do tzv. těžebních poolů. Jedná se o obrovské decentralizované výpočetní sítě. Často za poolem stojí jedna velká firma vlastnící velký výpočetní výkon, kdokoliv se však do poolu může za určitých podmínek zapojit a svým výkonem se podílet na decentralizovaném paralelním výpočtu bloku. Po úspěšném vytěžení bloku se zisk dělí mezi zúčastněné podle daných pravidel. V praxi to vypadá tak, že všichni v poolu počítají hash pro vyřešení úlohy a pro potvrzení boku, pokud někdo z nich dokáže blok potvrdit tak si odměnu nenechá, ale jeho odměna je rozdělena mezi ostatní těžaře v poměru výpočetnímu výkonu, který při výpočtu každý z nich dodává. Dále každý těžař musí platit nějaké poplatky za to, že může být součástí poolu. Tyto poplatky se obvykle pohybují okolo

[32] The Bitmain Antminer E9 is the world's most powerful Etherium mining ASIC - NotebookCheck.net News. Notebook / Laptop Reviews and News - NotebookCheck.net [online].[cit. 23.04.2021]. Dostupné z: https://www.notebookcheck.net/The-Bitmain-Antminer-E9-is-the-world-s-most-powerful-Ethereum-mining-ASIC.535225.0.html

2% ze zisku. Při výběru, vhodného poolu, kam se těžař připojí se jedná občas o začarovaný kruh. Pokud se připojí do nějakého zavedeného a velikého poolu, tak má vysokou jistotu, že bude těžit hodně bloků, tedy že budou zisky. V takovém poolu je ale připojeno hodně těžařů, takže dochází k vysoké granularitě zisku mezi velké množství zúčastněných. U malých poolů si naopak může přijít na zajímavá procenta ze zisku, ale nejspíše pool vytěží méně bloků. Většina těchto těžěbních poolů se nespecializuje pouze na těžbu BTC, ale těží více kryptoměn.[33]

### 1.4.3 Investice

Investovat do kryptoměn lze nejrůznějšími způsoby. Jednou z možností investice je jejich samotná těžba, popis těžby viz předchozí kapitoly. Dalšími způsoby, jak do kryptoměny investovat, je jejich nákupem, a to v různých formách.

Jednou z možností, jak si pořídit kryptoměnu, jsou bitcoinové bankomaty, nebo tzv. Bitcoinmaty. V Bitcoinmatu si nelze pořídit všechny kryptoměny, které momentálně existují, pouze Bitcoin a Litecoin. Nákup kryptoměny v těchto Bitcoinmatech je jednoduchý a téměř okamžitý. Potřebujeme k tomu mít osobní QR kód peněženky, buď v mobilní aplikaci, nebo vytištěný na papíře. Do Bitcoinmatu vložíme peníze, které chceme směnit za Bitcoiny či Litecoiny, přiložíme ke čtečce QR kód, aby bankomat věděl, na jakou adresu má mince poslat a potvrdíme transakci. Bitcoinmat vám zobrazí přepočítanou částku do kryptoměny dle daného kurzu. Nevýhodou pořízení kryptoměn v Bitcoinmatu jsou vysoké poplatky. Mimo jiné pomocí Bitcoinmatů lze kryptoměny i prodávat, resp. vyzvednout si hotovost ve fiat měně.[34]

Dalším způsobem získání kryptoměny je nákup od prodejce z okolí. Takového prodejce lze vyhledávat online např. na inzercích, aukcích, aj. Přímo pro Bitcoin byl založen server localbitcoin.com, kde zadáte množství peněz, za které chcete BTC nakoupit a ve stát ve kterém chceme kryptoměnu nakoupit. U prodejců je možné sledovat počet již proběhlých transakcí,

[33] Těžba kryptoměn - Jak těžit Bitcoin a jiné krypto? » Finex.cz. Finanční magazín Finex.cz - Objektivní průvodce světem financí [online].[cit. 23.04.2021]. Dostupné z: https://finex.cz/rubrika/kryptomeny/tezba/
[34] Bitcoinmat [online].[cit. 23.04.2021]. Dostupné z: https://bitcomat.com/

od ostatních zákazníků, což přispívá k důvěryhodnosti. Obdobně lze využít tuto cestu pro opačnou transakci, kdy budete chtít kryptoměnu prodat.

Možnost pořízení kryptoměny nám také poskytují směnárny a burzy. Na burze si lze koupit kryptoměnu od uživatelů, kdy burza je prostředníkem. U směnáren obchodujete přímo se společností. Lze zde kryptoměny i prodávat. Na burze probíhá obchod s uživateli, kteří jsou zde buď za účelem koupě, nebo prodeje. Objednávky se zadávají dvojím způsobem: Limit a Market. V případě objednávky Limit si uživatel určí množství peněz a požadovanou cenu, za kterou chce nakoupit nebo prodávat. Objednávka se zařadí do nabídky a čeká na přijetí. V druhém případě u objednávky Market se zvolí pouze požadované množství prostředků pro prodej nebo nákup a burza sama přiřadí k objednávce aktuální nejvýhodnější nabídku. Burzy si za tyto služby účtují poplatky. Mezi ověřené burzy patří např. Binance, Bitfinex aj. [35]

V neposlední řadě lze kryptoměny získávat těžbou. Těžba je „proces při kterém se pomocí strojově náročného výpočtu hledá další blok pro napojení do blockchainu. Validní blok je nalezen, pokud splňuje podmínku, že jeho hash (přesněji hash vypočtený nad serializací jeho dat), je nižší než určitý cíl (parametr target – číslo začínající na mnoho nul v numerickém zápisu hashe. Tento cíl se odvozuje z momentální obtížnosti (parametr difficulty), která se mění každých 2016 bloků v závislosti na rychlosti jejich nalezení tak, aby průměrná rychlost generování nových bloků činila 1 blok za 10 min. Pokud blok nesplňuje podmínku na nízký hash, je nutné jeho serializaci pozměnit (obsahuje k tomu určené pole nonce, které může nabývat libovolné hodnoty) a zkusit hash přepočítat. Těžba je vlastně částečná inverze hashovací funkce.“ Náročnost těžby, s počtem přibývajícího množství mincí v oběhu, se stupňuje vzestupně. Těžba se ztěžuje i počtem přibývajících těžařů. V dnešní době je téměř nemožné těžit pomocí vlastního počítače sám pomocí procesoru či grafické karty. Jelikož je těžba v dnešní době natolik hardwarově náročná, distribuuje se do tzv. poolů. Těžební pooly jsou shluky těžařů, kteří vlastní těžební zařízení a podílejí se jím na těžbě bloků jako celek.

[35] Kryptoměnová burza Bittrex – recenze, zkušenosti, návod na obchodování, poplatky. Investice a spoření | InvestPlus [online].[cit. 23.04.2021]. Dostupné z: https://investplus.cz/investice/kryptomenova-burza-bittrex-recenze-zkusenosti-navod-na-obchodovani-poplatky/

Největší těžební pooly jsou BTC.com, ViaBTC dokonce mezi jeden největší těžební pool se řadí český Slush pool. [36]

**Kryptoměny jako investiční nástroj**

Investice do kryptoměn všeobecně shledává vysoký zájem. Už jen z hlediska historického vývoje kryptoměny Bitcoin je v roce 2021 v žebříčku svého maxima, což poutá velkou pozornost a zájem investorů vkládat do této kryptoměny své prostředky, taktéž jako jsou oslovováni další potencionální investoři. Ovšem stále s sebou kryptoměny nesou riziko vysoké volatility. Před samotnou investicí do kryptoměny je vhodné posoudit, jaké výhody a nevýhody s sebou tato investice může nést.

Jednou z vlastností kryptoměn všeobecně je její transparentnost, každá uskutečněná transakce je sledována a zaznamenávána do veřejné účetní knihy známé také pod názvem Blockchain. Jakmile je transakce potvrzena, nelze ji v žádném případě změnit. Každá transakce je v systému ověřována, a tak je velice nepravděpodobné, že by mohlo dojít k odcizení vlastněných kryptoměn. Transakce můžou být prováděny kdykoliv, jedinou podmínkou je připojení k internetu. Ověřování transakcí totiž probíhá neustále a bez přestávky. Uživatelé mají naprostou kontrolu nad svými prostředky a transakcemi, což zabezpečuje především privátní a veřejný klíč. Od investice do Bitcoinu lze očekávat velký potenciál pro zhodnocení vložených prostředků. Tato vidina přitahuje stále více investorů, avšak jak je již zmíněno, je třeba dbát zvýšené pozornosti jejich volatilitě. Tyto vlastnosti jsou všeobecně posuzovány jako výhody investice do kryptoměn, avšak záleží na individuálním posouzení jednotlivých investorů. [37]

Bitcoiny a další kryptoměny existují pouze v digitální podobě a taktéž musí být v této podobě uchovávány. Pokud uživatel ztratí přístupové údaje ke své peněžence, přichází tak o svůj privátní klíš a tím pádem o své investované peníze. Aktuálně neexistují žádné mechanismy pro obnovení hesla k přístupu, což se jeví jako značná nevýhoda. Z hlediska investice může

[36] STROUKAL, Dominik a SKALICKÝ, Jan. Bitcoin a jiné kryptopeníze budoucnosti: historie, ekonomie a technologie kryptoměn, stručná příručka pro úplné začátečníky. 2., rozšířené vydání. Praha: Grada Publishing, 2018. s. 45- 50. ISBN 978-80-271-0742-1.

[37] MARTINÁK, Tomáš a kol. Bezhotovostní peníze versus elektronické peníze. 1. vydání. Olomouc: Iuridicum Olomoucense, s.r.o., ve spolupráci s Právnickou fakultou Univerzity Palackého v Olomouci, 2015. s. 52 Acta iuridica Olomucensia. Monografie a studie. ISBN 978-80-87382-74-5

být nevýhodou kolísání trhu. Před samotnou investicí je vhodné podrobit se výzkumu vývoje kurzu a seznámit se s příčinami volatility kryptoměn.

Všeobecnou povahou kurzu Bitcoinu je velké kolísání. Jeho cenové výkyvy jsou rutinní záležitostí. Spousta investorů však požaduje stabilitu, což Bitcoin stabilitu zatím slíbit nemůže. Bitcoin vznikl v roce 2009 a do roku 2021 ještě nedosáhl své stabilní formy. Hlavním důvodem této nestability je, že tato měna není celosvětově uznávána. Avšak v roce 2021 je již obecně šířenou měnou ve Spojených státech. Každý stát má ale pohled na kryptoměny jiný, v některých státech je v roce 2021 naopak úplně zakázána. Ke stabilitě může dojít pouze tehdy, když bude uznávána globálně. Dalším důvodem velké volatility je regulace. Kryptoměny nejsou regulovány centrální autoritou, což zapříčiňuje ztrátu nad kontrolou její stability. Nedostatečná regulace mimo jiné svádí jejich vlastníky i k tzv. praní peněz v tomto anonymním systému. Bitcoin může uspět nebo selhat na základě síťového efektu. Síťový efekt nastává tehdy, když zboží nebo služba zvýší hodnotu na základě počtu lidí, kteří tuto službu či zboží používají. K lepšímu přiblížení fungování síťového efektu je nastíněn následující příklad: V začátcích internetu jste byl jedním z prvních, který využíval tuto technologii, avšak v té době internet neměl téměř žádnou přidanou hodnotu. Neexistoval nikdo, komu byste mohli poslat e-mail a k dispozici bylo pouze pár webových stránek k prohlížení. S rostoucím počtem uživatelů internetu však začalo přibývat množství webových stránek a přidávání dalších funkcí, což zvyšuje jeho celkovou hodnotu. Dochází tedy k spekulacím, že trh kryptoměn se bude chovat na podobné bázi.

Pro obchodování s Bitcoinem či jinou kryptoměnou, může a nemusí být, vysoká volatilita výhodou. Je pravda, že se Bitcoiny stále více využívají jako globální měna, nicméně ji využívají především investoři a obchodníci ke tvorbě zisku z jejich pravidelných výkyvů na trhu. Tito obchodníci jsou skupinou lidí, kteří vysokou proměnlivost kryptoměn nikdy nezpochybňují, jelikož právě fluktuace je to, co určuje jejich zisky. U obchodování se setkáváme s pojmem indexu cenové volatility, což je měřítko pro pohyb ceny nahoru či dolů. Index lze sledovat z hlediska krátkodobého i dlouhodobého. Obchodníky zajímá v zásadě pouze okamžitá volatilita, která je vyjádřena průměrnou denní změnou ceny[38].

[38] ttention Required! | Cloudflare. Attention Required! | Cloudflare [online].[cit. 23.04.2021]. Dostupné z: https://www.etoro.com/crypto/why-bitcoin-fluctuates/

Index cenové volatility je měřítkem toho, jak moc se mění cena finančního aktiva v průběhu času a je vyjádřena v procentech. Pokud se cena mění rychle, index se zvyšuje a pokud se cena mění pomalu, index klesá. S růstem indexu taktéž roste míra rizika a naopak. Index cenové volatility rozdělujeme na historickou volatilitu, která je ukazatelem toho, jak se cena vyvíjela v minulosti. Dále se rozděluje na implikovanou volatilitu, což je volatilita, která se předpokládá v budoucnu. .[39] U Bitcoinu se cenová volatilita pohybuje kolem 5% - 10%, což je považováno za extrémně volatilní aktivum. Pro zkušené investory to může být značnou výhodou, jelikož je vysoká pravděpodobnost velkého zhodnocení vložené investice v krátkém časovém úseku. Toto pravidlo platí i naopak. Investor se tak sekává s vysokým rizikem.[40]

### 1.4.4 Legální a daňové hledisko

Kryptoměny jsou v České republice posuzovány jako nehmotný movitý majetek. ČNB je nepovažuje za kryptoměny, cizí měny ani jako cenné papíry. Každá země má odlišnou legislativní regulaci kryptoměn, v některých jsou dokonce zakázány. Před zahájením těžby je nutné mít povědomí o této regulaci a přizpůsobit jí daný záměr. Jelikož jsou podmínky legálnosti kryptoměn velice proměnné, je třeba aktivně sledovat vývoj v této oblasti a případně mít diverzifikované portfolio[41]. Pokud není definována právní úprava kryptoměny v dané lokalitě, budeme uvažovat, že jsou zde aktivity spojené s kryptoměnou v souladu se zákonem, tedy legální. Tato zásada je v českém právním řádu promítnuta v listině základních lidských práv a svobod, a to že "Každý může činit, co není zákonem zakázáno, a nikdo nesmí být nucen činit, co zákon neukládá.[42]" Nelze však opomenout i zásadu personality působnosti právních norem a sice, že pro občany vybraných států může být držení, resp. těžba kryptoměn nelegální

[39] VIX Index - vše co je nutné vědět o indexu volatility [2020]. Broker LYNX | Investujte s výhodami [online].[cit. 23.04.2021]. Dostupné z: https://www.lynxbroker.cz/vzdelavani/vix-index-vse-co-je-nutne-vedet-o-indexu-volatility/

[40] Bitcoin Volatility Index (0.69%) | Bitcoin Volatility Explained (2021 Updated). 99Bitcoins - How to Buy Bitcoin in 2021 | Best Bitcoin Wallets & Exchanges [online].[cit. 23.04.2021]. Dostupné z: https://99bitcoins.com/bitcoin/historical-price/volatility/

[41] **Indie** - Indie plánuje striktní zákaz kryptoměn, těžbu, obchod i jejich držení. Nová legislativa vzniká ve prospěch projektu oficiální státní kryptoměny. Zákon se aktuálně projednává. Podrobněji: Bitcoin mining is still huge in China despite new ban in Inner Mongolia – SupChina. SupChina | Reporting on China without fear or favor [online].[cit. 23.04.2021]. Dostupné z: https://supchina.com/2021/03/09/bitcoin-mining-is-still-huge-in-china-despite-new-ban-in-inner-mongolia/

[42] LISTINA ZÁKLADNÍCH PRÁV A SVOBOD [online].[cit. 23.04.2021]. Dostupné z: http://www.psp.cz/docs/laws/listina.html

i v případě, kdy k takové aktivitě bude docházet i na území jiného státu, kde jsou takové aktivity legální.[43]

Samotná legálnost těžby je nutným, nikoliv však postačujícím požadavkem pro splněných zákonných předpisů. Na rozdíl od pouhé směny kryptoměn z hlediska právních předpisů je považována za podnikání, neboť je provozovaná soustavně a za účelem zisku.[44] Subsumpce pod podnikatelskou činnost s sebou přináší povinnosti se k podnikání registrovat, vést potřebné evidence a příp. se účastnit na veřejných financích. Těžba kryptoměn je posuzována jako poskytování služby třetí osobě v podobě ověřování transakcí. Pro vykonávání této činnosti potřebujeme mít živnostenské oprávnění.[45] Přesněji živnost volnou v oboru činnosti č. 56: „Poskytování software, poradenství v oblasti informačních technologií, zpracování dat, hostingové a související činnosti a webové portály.“[46]

Důležitým aspektem těžby kryptoměn je daňové hledisko. Příjmy z této činnosti spadají do kategorie tzv. kapitálových příjmů. Při překročení příjmu 30 tisíc Kč za jedno zdaňovací období, podléhají dani z příjmů dle ustanovení § 10 a násl. zák. 586/1992 Sb. o daních z příjmů.[47]

Základem daně v případě zdanění kryptoměn je rozdíl mezi částkou, za kterou se kryptoměna nakoupila či vytěžila a částkou, za kterou se kryptoměna prodala. Např.: pokud nakoupím na burze kryptoměny za 100 tisíc Kč a prodám je za 300 tisíc Kč, dílčím základem daně je pak rozdíl 200 tisíc Kč. Od základu si lze pak odečíst prokazatelné náklady. Do nákladů lze zahrnout buď náklady skutečné, které souvisejí s těžbu kryptoměn, nebo náklady paušální dle

[43] **Maroko** - Tamní vláda považuje všechny aktivity spojené s kryptoměnami za nelegální činnosti. Např. Pokud se občan Maroka nachází na území České republiky, vztahují se na něj tamní zákony. Může zde legálně držet, obchodovat a těžit kryptoměnu. Pokud by však po překročení hranic Maroka stále držel kryptoměnu, kterou vytěžil na území České republiky, bude se dopouštět nelegální činnosti. Více dostupné z: The status of cryptocurrency in Morocco - ScienceDirect. ScienceDirect.com | Science, health and medical journals, full text articles and books. [online].[cit. 23.04.2021]. Dostupné z: https://www.sciencedirect.com/science/article/pii/S2590051X21000058

[44] Dle ustanovení § 420 odst. 1 zák. 89/2012 Sb.. Podnikatelem je ten - kdo samostatně vykonává na vlastní účet a odpovědnost výdělečnou činnost živnostenským nebo obdobným způsobem se záměrem činit tak soustavně za účelem dosažení zisku, je považován se zřetelem k této činnosti za podnikatele.

[45] Jak na zdanění digitálních měn - Služby a podnikání. Vzdělávací a rekvalifikační kurzy Praha [online].[cit. 23.04.2021]. Dostupné z: https://www.sluzbyapodnikani.cz/jak-na-zdaneni-digitalnich-men/

[46] Dle přílohy č. 1 k zákonu č. 455/1991 Sb. o živnostenském podnikání.

[47] KALISKÝ, Boris. Bitcoin a ti druzí: nepostradatelný průvodce světem kryptoměn. [Praha]: IFP Publishing, 2018. s. 20 ISBN 978-80-87383-71-1

ustanovení § 7 odst. 7 b) zák. 586/1992 Sb. o daních z příjmů, ve výši 60 %. Odečíst ze základu je možné i ztrátu, kterou lze odečíst i v budoucnu až po dobu pěti let.[48]

Při prodeji vytěžené kryptoměny podléhá příjem dani. Příjem jsme povinni zahrnout do daňového přiznání společně s daňově uznatelnými výdaji a zaplatit daň. Výše daně se liší v závislosti na právní formě investování. Vhodnou právní formu si zvolíme ještě před zahájením těžby kryptoměny. Příjem z obchodování podléhá dani z ostatního příjmu zákona o dani z příjmu dle §10, pro FO 15%, pro PO 19%. Na příjmy se nevztahuje sociální ani zdravotní pojištění. [49]

..

[48] Dle ustanovení § 34 zák. 586/1992 Sb. o daních z příjmů.
[49] KRYPTOMĚNY a DANĚ - Jak na to? Návod [Aktuální 2021]. Finanční magazín Finex.cz - Objektivní průvodce světem financí [online].[cit. 23.04.2021]. Dostupné z: https://finex.cz/zdaneni-kryptomen-kompletni-navod/

# 2 Praktická část

## 2.1 Metodika

Vzhledem k tomu, že těžba kryptoměn může být velice nákladná a ve více ohledech riziková, je vhodné si před rozhodnutím vytvořit metodický postup proveditelnosti a rentability těžby.

Cílem této práce je provést finanční analýzu rentability. Budeme se zabývat ukazatelem ROE (Return of Equity) - rentability vlastního kapitálu. Ukazatele rentability zjistíme dosazením do výchozího vzorce:

**Vzorec pro výpočet ROE (Return Of Equity)** - rentabilita vlastního kapitálu[50]

$$ROE = \frac{EAT}{Eq} * 100$$

***EAT*** *(Earnings after Taxes) - zisk po zdanění*
***Eq*** *(Equity) – vlastní vložený kapitál*

Pro účely výpočtu rentability těžby kryptoměn je za Equity třeba dosadit celkové pořizovací náklady těžebního vybavení. Zisk po zdanění vypočteme jako rozdíl příjmů a výdajů ponížený o daň z příjmu.

$$ROE = \frac{Re - Co - T}{TPhw} * 100$$

***Re*** *(Revenue) - příjmy za sledované období*
***Co*** *(Costs) - výdaje za sledované období*
***T*** *(Taxes) – daně*
***TPhw*** *(Total Hardware Price) - celková cena těžebního hardwaru vč. příslušné režie k zprovoznění těžební jednotky*

[50] KALOUDA, František. Finanční a cost-benefit analýza podniku. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2019. s. 36. ISBN 978-80-7380-778-8.

Dílčí výpočty pro ROE:

**EAT** (Earnings After Taxes) - zisk po zdanění

$$EAT = EBT - T$$

**EBT** (Earnings Before Taxes) - zisk před zdaněním

$$EBT = Re - Co$$

**Vzorec pro výpočet Re (Revenue)** – příjmy za sledované období

$$Re = \left[\left(\frac{HSRhw}{HSRn} * \frac{t}{Mt}\right) * (Rb + Rtr)\right] * R$$

***HSRhw*** *(Hardware Hashrate) - Hashrate hardwaru*
***HSRn*** *(Network Hashrate) - Hashrate sítě*
***t*** *(Time) – čas*
***Mt*** *(Time Per One Mined Block) - doba vytěžení bloku*
***Rb*** *(Revenue Per Block) - příjem za vytěžený blok*
***Rtr*** *(Revenue Per Transaction) - příjem za potvrzení transakce*[51]
***R*** *(Rate) - směnný kurz*

Podílem Hashrate vlastního hardwaru na aktuálním Hashratu sítě lze zjistit podíl konkrétního těžaře na vytěženém bloku. Podílem času na době vytěžení jednoho bloku pak lze dojít k určení počtu bloků vytěžených za sledované období. Součinem těchto proměnných pak získáme počet těžařem vytěžených bloků za sledované období. Součtem Příjmu za vytěžený blok a Příjmu za potvrzení transakce získáme celkové množství kryptoměny na jeden vytěžený blok. Součinem Počtu těžařem vytěžených bloků za sledované období a Celkového množství kryptoměny na

[51] STROUKAL, Dominik a SKALICKÝ, Jan. Bitcoin a jiné kryptopeníze budoucnosti: historie, ekonomie a technologie kryptoměn, stručná příručka pro úplné začátečníky. 2., rozšířené vydání. Praha: Grada Publishing, 2018. s. 83 ISBN 978-80-271-0742-1.

jeden vytěžený blok získáme Množství těžařem vytěžené kryptoměny. Součin Množství těžařem vytěžené kryptoměny a aktuálního Směnného kurzu nám ukáže výsledný Příjem za sledované období (ve fiat měně).

Dílčí výpočty pro Re:

**TR** (Total Revenue) - příjmy za těžbu celkem

$$TR = Rb + Rtr$$

**D** (Difficulty) - obtížnost

$$D = \frac{HSRhw}{HSRn}$$

**TRns** (Total Revenue Per Network Share) - příjmy za těžbu podílu na síti

$$TRs = D^{*} TR$$

**NM** (Total Network Mined Block) - celkem vytěžených bloků na síti

$$NM = \frac{t}{Mt}$$

**Vzorec pro výpočet Co (Costs) – výdaje za sledované období**

$$Co = (Pe * t * e) + \left[\frac{(Phw+Pa)}{Lhw}\right]$$

***Pe*** *(Price Electricity) - cena elektřiny*
***t*** *(Time) – čas*
***e*** *(Electricity) - spotřeba elektřiny těžebního hardwaru*
***Phw*** *(Hardware Price) - cena těžebního hardwaru*[52]
***Pa*** *(Accessories Price) - cena hardwarového příslušenství*
***Lhw*** *(Hardware Lifetime) - životnost hardwaru*

Součinem Ceny elektřiny, Času a Spotřeby elektřiny těžebního hardwaru získáme Cenu těžbou spotřebované elektřiny za sledované období. Součtem Ceny těžebního hardwaru a Ceny hardwarového příslušenství získáme Celkovou cenu těžebního hardwaru vč. příslušné režie k zprovoznění těžební jednotky. Tento součet je třeba vydělit celkovou živností daného hardwaru, čímž zjistíme amortizaci, která je pro naše účely nákladem na hardware za zvolené časové období. Celý výsledek nám pak stanoví celkové Výdaje za sledované období.

Dílčí výpočty pro Co:

**TPhw** (HW price with accessories) - cena hardwaru včetně příslušenství

$$TPhw = Phw + Pa$$

**Lhws** (Hardware Lifetime share) - podíl ceny hardwaru v čase

$$Lhws = \frac{TPhw}{Lhw}$$

[52] Buy ASIC Bitcoin Miners & Bitcoin Mining Equipment - Bitmain. Wayback Machine [online]..[cit. 23.04.2021]. Dostupné z: http://web.archive.org/web/20180104105846/https://shop.bitmain.com/

**TPe** (Total Price Electricity) - celkem cena za elektřinu

$$TPe = Pe * t * e$$

## 2.2 Vstupy

Následující popis jednotlivých vstupních parametrů slouží k tomu, aby je stručně popsal a vysvětlil jejich návaznost na výpočet rentability těžby kryptoměn. Na tomto místě je nutné obecně popsat vybrané parametry, protože ve výpočtu samotném pro vysvětlování pojmu není místo a působí rušivým dojmem.

### Cena hardwaru (Phw)

Pro vykonávání činnosti těžby kryptoměn je podmínkou vhodný HW a příslušenství k němu. HW v tomto smyslu je myšlen těžební počítač s příslušenstvím, tj. zejména klasické příslušenství k počítači, jako je monitor, kabely, klávesnice, myš atd. V některých případech sofistikovaného HW určeného výhradně pro těžbu kryptoměn může být zapotřebí další speciální příslušenství. Toto je však velmi individuální a kompletní popis vzhledem k možnostem lze uvést pouze na konkrétním příkladu viz následující kapitola.

Jelikož cena těžebního počítače a příslušenství je přímým nákladem, který ovlivňuje výpočet rentability těžby, je nutné ho do výpočtu zahrnout.

Největší podíl na ceně HW a příslušenství, tedy vstupním nákladu má grafická karta. Tento komponent přímo ovlivňuje výkon těžebního počítače, což má značný vliv na efektivitu těžby a zastoupení těžaře v na síti.

Z důvodu zvýšené poptávky po grafických kartách neboli grafických procesorech, se ceny grafických karet razantně zvýšily, a to z důvodu zvýšeného zájmu o těžbu kryptoměny.

Dalším důležitým parametrem je i živnost HW, protože dobu možnosti těžby na tomto konkrétním HW a též se projevuje ve výpočtu rentability.

**Daně (T)**

Tento vstup vyjadřuje daň z příjmu 15% u FO nebo 19% u PO.[53]

**Cena a spotřeba elektřiny (Pe, e)**

Pro samotnou těžbu je cena energie podstatným kritériem, který výrazně ovlivňuje výsledky těžby. Pokud se cena elektrické energie zvyšuje, dochází k automatickému snížení hodnoty vytěžené jednotky kryptoměn. Naopak, pokud se cena elektrické energie snižuje, zvyšuje se hodnota vytěžené jednotky kryptoměny. Cena elektrické energie je přímým nákladem.

Z výše uvedeného je patrné, že cena elektrické energie přímo vstupuje do výpočtu rentability těžby kryptoměny a z tohoto důvodu je tedy nutné ji do výpočtu zahrnout.

Níže uvedená tabulka znázorňuje průměrné roční ceny elektrické energie ve světovém měřítku v amerických dolarech za rok 2020. Dle tabulky můžeme posuzovat státy ve kterých by byla těžba kryptoměn výhodnější či naopak.

Tabulka 1 - Porovnání cen elektřiny ve světovém měřítku[54]

| **č.** | **Stát** | **$/kWh (2020)** | **č.** | **Stát** | **$/kWh (2020)** |
|---|---|---|---|---|---|
| 1 | Venezuela | 0,000 | 31 | Indonesia | 0,101 |
| 2 | Argentina | 0,063 | 32 | Thailand | 0,122 |
| 3 | Burma | 0,043 | 33 | Canada | 0,112 |
| 4 | Egypt | 0,045 | 34 | South Korea | 0,098 |
| 5 | Iraq | 0,024 | 35 | Estonia | 0,171 |
| 6 | Iran | 0,005 | 36 | Brazil | 0,126 |

[53] STROUKAL, Dominik a SKALICKÝ, Jan. Bitcoin a jiné kryptopeníze budoucnosti: historie, ekonomie a technologie kryptoměn, stručná příručka pro úplné začátečníky. 2., rozšířené vydání. Praha: Grada Publishing, 2018. s. 105-107. ISBN 978-80-271-0742-1.

[54] Thailand electricity prices, September 2020 | GlobalPetrolPrices.com. Gasoline and diesel prices by country | GlobalPetrolPrices.com [online].[cit. 23.04.2021]. Dostupné z: https://www.globalpetrolprices.com/Thailand/electricity_prices/

| | | | | | |
|---|---|---|---|---|---|
| 7 | Uzbekistan | 0,028 | 37 | Hong Kong | 0,147 |
| 8 | Kuwait | 0,030 | 38 | United States | 0,150 |
| 9 | Quatar | 0,032 | 39 | Romania | 0,174 |
| 10 | Algeria | 0,040 | 40 | Turkey | 0,088 |
| 11 | Azerbaijan | 0,041 | 41 | Poland | 0,197 |
| 12 | Bahrain | 0,048 | 42 | Iceland | 0,140 |
| 13 | Kazakhstan | 0,041 | 43 | Finland | 0,189 |
| 14 | DR Congo | 0,062 | 44 | Columbia | 0,153 |
| 15 | Ukraine | 0,046 | 45 | Netherlands | 0,188 |
| 16 | Saudi Arabia | 0,048 | 46 | Czech Republic | 0,247 |
| 17 | Zambia | 0,025 | 47 | France | 0,220 |
| 18 | Ghana | 0,064 | 48 | New Zeland | 0,247 |
| 19 | Bangladesh | 0,066 | 49 | Sweden | 0,179 |
| 20 | Russia | 0,061 | 50 | Japan | 0,267 |
| 21 | Kosovo | 0,095 | 51 | United Kingdom | 0,266 |
| 22 | Pakistan | 0,062 | 52 | Austria | 0,244 |
| 23 | Tunisia | 0,076 | 53 | Spain | 0,242 |
| 25 | Serbia | 0,096 | 55 | Italy | 0,262 |
| 26 | China | 0,084 | 56 | Belgium | 0,310 |
| 27 | India | 0,077 | 57 | Germany | 0,372 |
| 28 | North Macedonia | 0,093 | 58 | Dánsko | 0,337 |

**Příjem za vytěžený blok (Rb)**

Je hodnota, která označuje množství kryptoměny za výpočtové operace hardwaru.

**Příjem za transakci (Rtr)**

Je odměna, která je současně připočtena k odměně za vytěžený blok. Do probíhajících výpočtů současně s výpočtovými operacemi, které provádí těžební hardware, za účelem těžby kryptoměny vstupují další výpočtové operace, které slouží k ověřování transakcí z již vytěžených jednotek kryptoměn, které mohou provádět, jejich držitelé.[55]

**Doba vytěžení bloku (Mt)**

Hodnota průměrné doba vytěžení jednoho bloku je volně přístupná na internetu, kdy se každý den aktualizuje z důvodu proměnnosti vytěžených bloků na síti. Tím pádem se mění i obtížnost těžby a proto i průměrná doba vytěžení jednoho bloku na síti.

**Čas (t)**

Pro výpočty je rozhodné období jeden den.

**Směnný kurz (R)**

Směnný kurz je hodnota jednotky kryptoměny přepočtená na fiat měnu.[56] Pro výpočet rentability je zásadním ukazatelem, protože výsledná rentabilita se počítá ve fiat měně a logicky je největší motivací těžaře k těžební činnosti. Do budoucna se dá předpokládat, že pokud dojde k ústupu fiat měn na úkor kryptoměn. Směnný kurz bude mít menší a menší relevanci směrem k těžbě. V případě, že běžný obchodní styk se bude dít v kryptoměně, přepočty na fiat měny se budou stávat zanedbatelnější a zanedbatelnější. Tento stav se však zdá v blízké budoucnosti

[55] MYSLÍN, Josef. Obecné technické aspekty fungování virtuálních měn. In: HUJOVÁ, Gabriela, ed. Zkušenosti s virtuálními měnami - Bitcoin měna budoucnosti?: sborník z konference: Praha, 26. března 2014. Praha: Vysoká škola manažerské informatiky, ekonomiky a práva, 2014. s. 75 -76. ISBN 978-80-86847-71-9.
[56] SAMUELSON, Paul Anthony a NORDHAUS, William D. Ekonomie: 19. vydání. Vyd. 1. Praha: NS Svoboda, 2013. s. 667. ISBN 978-80-205-0629-0.

spíše jako nepravděpodobný, protože nastavený trend směřuje spíše k regulacím centrálními autoritami.

Směnný kurz není jednotkou statickou, ale v čase se vyvíjející a důvody tohoto vývoje lze jen stěží predikovat[57]. Ještě důležitější než kurz samotný je jeho vývoj v čase. Pokud výpočet rentability je spočítán ke konkrétnímu datu, nelze předpokládat že rentabilita bude stejná k datu jinému. Jelikož je volatilita směného kurzu vysoká je pro výpočet rentability těžby důležité toto hledisko zohledňovat, a to především v dlouhodobém horizontu těžby.

**Hashrate sítě (Nhsr)**

Je počet možných vytěžených bloků za časové období všemi těžaři, kteří se účastní těžby kryptoměny.

**HW hashrate (HWhsr)**

Je jednotka která určuje výkon HW samotného, který je využíván pro těžbu kryptoměn. Jeho základní jednotkou je 1 hash[58]. Tuto jednotku lze také vyjádřit jako potenciální možnost HW vytěžit určitý počet jednotek za předpokladu stálé funkčnosti.

**Obtížnost (D)**

Procentuální zastoupení z celkové hashrate sítě aplikované na náš těžební hardware. Tato jednotka nám udává míru možnosti objemu těžby na konkrétním HW. Níže uvedený výpočet vychází z dat k roku 2018. Základní jednotkou hashrate podílu sítě (D) je 1 H/s - Hash za sekundu.

[57] JEDLINSKÝ, Jakub. Jsou kryptoměny bublinou nebo mají význam pro světové hospodářství? In: HUJOVÁ, Gabriela, ed. Zkušenosti s virtuálními měnami - Bitcoin měna budoucnosti?: sborník z konference: Praha, 26. března 2014. Praha: Vysoká škola manažerské informatiky, ekonomiky a práva, 2014. s. 55. ISBN 978-80-86847-71-9.

[58] ROTHSTEIN, Adam. The End of Money The Story of bitcoin, cryptocurrencies and the blockchain revolution. London: Hodder & Stoughton General Division, 2017. p. 36-42. ISBN 978-1473-62953-0.

**Cena těžebního hardwaru (Pa, Phw)**

Pro vykonávání činnosti těžby kryptoměn je podmínkou vhodný HW a příslušenství k němu. HW v tomto smyslu je myšlen těžební počítač s příslušenstvím, tj. zejména klasické příslušenství k počítači, jako je monitor, kabely, klávesnice, myš atd. V některých případech sofistikovaného HW určeného výhradně pro těžbu kryptoměn může být zapotřebí další speciální příslušenství. Toto je však velmi individuální a kompletní popis vzhledem k možnostem lze uvést pouze na konkrétním příkladu viz následující kapitola.

Jelikož cena těžebního počítače a příslušenství je přímým nákladem, který ovlivňuje výpočet rentability těžby, je nutné ho do výpočtu zahrnout.

Největší podíl na ceně HW a příslušenství, tedy vstupním nákladu má grafická karta. Tento komponent přímo ovlivňuje výkon těžebního počítače, což má značný vliv na efektivitu těžby a zastoupení těžaře v na síti.

Z důvodu zvýšené poptávky po grafických kartách neboli grafických procesorech, se ceny grafických karet razantně zvýšily, a to z důvodu zvýšeného zájmu o těžbu kryptoměny.

## 2.3 Rozhodovací hlediska

### 2.3.1 Metoda těžby

Níže jsou popsány dvě metody těžby, a to metoda - těžba GPU a těžba ASIC. V rámci těžby kryptoměn, existují i další metody těžby např. pronájem podílu na těžebním poolu….. Základem těchto metod není těžba kryptoměn na vlastním HW, tedy se v nich nekalkuluje s pořizovacími náklady, stejně jako v popisovaných metodách, a proto tyto metody neleze s popisovanými relevantně srovnávat. Zvolení metody těžby musí předcházet samotnému pořízení těžebního HW. Výběrem metody si předem stanovíme, jaký těžební hardware bude odpovídat plánovanému záměru. Rozhodujícím kritériem pro zvolení metody těžby je rozsah pokrytí kryptoměn, které lze na zařízení těžit.[59]

[59] Top 10 Best Cryptocurrencies to Mine Using GPUs in 2021 - BlockSocial. BlockSocial - Your Guide to Understanding and Capitalizing on a Decentralized World [online].[cit. 23.04.2021]. Dostupné z: https://www.blocksocial.com/best-cryptocurrencies-to-mine-using-gpu/

**Metoda 1 - Těžba GPU[60]**

Jedná se o relativně levnou, ale zároveň efektivní metodu těžby pomocí GPU soustavy, tedy HW se všemi nezbytnými komponenty pro zajištění těžby. Standardně se skládá z procesoru, základní desky, chladiče, rámu a několika grafických karet. Nejdůležitějším komponentem pro tuto metodu těžby je grafická karta, u které je nejdůležitějším parametrem její výkon. Pořizovací cena HW pro těžbu dle této metody se pohybuje mezi 50 - 60 tis. Kč.[61]

Výhody:

**Rozsah těžby** - můžeme těžit jakoukoliv kryptoměnu
**Aktualizace** - vždy dostupné upgrady a aktualizace
**Dostupnost** - snadná dosažitelnost
**Likvidita** - použitý hardware lze prodat dál
**Nastavení** - v případě, že instalaci kompletní HW sestavy bude provádět osoba, znalá v oboru můžeme považovat instalaci sestavy za lehko proveditelnou a tím nastavení považovat za výhodu, jelikož lze přepokládat vhodnější kombinaci jednotlivých komponent sestavy určené přímo k těžbě a tím dosažení lepších výsledků

Nevýhody:

**Objem hardwaru** - HW se vyznačuje větším požadavkem na místo, tedy čím více se těžař kryptoměny vytěžit, tím více prostoru pro HW potřebuje. Tato nevýhoda se na první pohled může zdát jako zanedbatelná, ale u většího objemu těžby ji nelze opomíjet, protože s nutností většího mohou přicházet i zvýšené náklady např. pronájem prostor. Pro účely výpočtu rentability, v této práci s nimi kalkulováno.
**Nastavení** - sestavení a instalace HW do kompletní sestavy je obtížná a pro neinformovaného laika téměř nemožná. Pro správné sestavení a instalaci HW jsou vyžadovány znalosti v této

[60] GPU (Graphics Processing Unit) - grafický procesor dle: Funkce Výkon GPU. 301 Moved Permanently [online].[cit. 23.04.2021]. Dostupné z: https://helpx.adobe.com/cz/illustrator/kb/gpu-performance-preview-improvements.html
[61] How To Mine Cryptocurrency: Beginner's Guide To Crypto Mining. Best Online Courses to Kickstart Your Career: eLearning on BitDegree [online].[cit. 23.04.2021]. Dostupné z: https://www.bitdegree.org/crypto/tutorials/how-to-mine-cryptocurrency

oblasti. Toto se také může zdát z ekonomického pohledu zanedbatelné, ale opět u větších objemů těžby v souvislosti s touto skutečnosti, může dojít ke vzniku dodatečných nákladů (placená školení, čas strávený studiem, nákup služeb od odborníka z oblasti…).
**Spotřeba energie** - vyšší energetická náročnost v poměru s výkonem[62]

**Metoda 2 - Těžba ASIC[63]**

Jde o metodu, která k těžbě využívá zařízení od společnosti ASIC. Těžební stroje od společnosti ASIC byly přímo vyvinuty a vyrobeny pro účely těžby kryptoměn, jedná se tedy o vysoce specializovaný HW, jehož jiné využití je značně omezené.[64] Pořizovací náklady se pohybují přibližně kolem 100 tis Kč.[65]

Výhody:

**Vysoký výkon** - Zařízení od společnosti ASIC jsou aktuálně jedny z nejvýhodnějších na trhu
**Nastavení** - nepotřebujeme žádné další HW komponenty ani technické znalosti
**Objem hardwaru** - úspora prostoru
**Spotřeba energie** - menší energetická náročnost v poměru s výkonem

Nevýhody:

**Pořizovací náklady** - vysoká cenová hladina
**Rozsah těžby** - nelze těžit všechny kryptoměny
**Aktualizace** - nelze upgradovat, ani aktualizovat
**Likvidita** - obtížnost dalšího prodeje[66]

[62] ASIC vs GPU Mining: Which Is Better in 2021?. cryptocoingossip.com: Simplifying Cryptos and Blockchain. [online].[cit. 27.04.2021]. Dostupné z: https://ccoingossip.com/asic-vs-gpu-mining/
[63] https://www.sigenics.com/blog/what-is-an-asic
ASIC (application-specific integrated circuit) - specializovaný procesor pro těžbu kryptoměn
[64] https://ccoingossip.com/asic-vs-gpu-mining/
[65] https://shop.bitmain.com/
[66] https://ccoingossip.com/asic-vs-gpu-mining/

Z výše uvedeného srovnání vyplývá, že rozhodnutí, zda použít pro těžbu kryptoměny metodu GPU nebo ASIC, vychází především z volby druhu kryptoměny, jelikož metodou ASIC nelze vytěžit všechny druhy kryptoměn. Do rozhodnutí, kterou zvolit metodu těžby, vstupují i další kritéria, která jsou však sekundárními kritérii.

### 2.3.2 Compliance náklady

Podstatným kritériem pro výpočet rentability jsou i legální aspekty. Pokud těžba v dané lokalitě není legální, nemůžeme začít uvažovat o zahájení a rentability z této činnosti např. Maroko.[67] V případě, že jsou aktivity spojené s kryptoměny striktně regulovány, lze očekávat, že rentabilita se bude snižovat. Můžeme se setkat se situací, kdy jsou regulovány jenom některé aktivity. Konkrétně se může jednat o to, že těžba je zakázána a obchodování taktéž, avšak držet ji lze[68]. Tento stav je nežádoucí a můžeme předpokládat, že z těchto důvodů bude rentabilita klesat. Můžeme setkat se stavem, kdy kryptoměny a aktivity s tím spojené nejsou regulované. Zde se dá předpokládat vyšší rentabilita než ve výše uvedených stavech. Legálnost a právní regulace kryptoměn s sebou nesou dodatečné náklady spojené se změnou právní úpravy, které by se daly zahrnout pod pojem compliance náklady[69], které se také zahrnují do transakčních nákladů[70]a mají významný vliv na výslednou rentability. Zahrnutí těchto nákladů do výpočtu rentability je problematické z následujících důvodů:

---

[67] **Maroko** - Tamní vláda považuje všechny aktivity spojené s kryptoměnami za nelegální činnosti. Např. Pokud se občan Maroka nachází na území České republiky, vztahují se na něj tamní zákony. Může zde legálně držet, obchodovat a těžit kryptoměnu. Pokud by však po překročení hranic Maroka stále držel kryptoměnu, kterou vytěžil na území České republiky, bude se dopouštět nelegální činnosti. https://www.sciencedirect.com/science/article/pii/S2590051X21000058

[68] **Čína** - Od roku 2018 se Čína podílela na vytěžení přibližně 60% kryptoměn z jejich celkového množství v oběhu. Podmínky pro těžbu v Číně jsou stále přísnější a každá z 23 čínských provincií těžbu, obchod a držení kryptoměn upravuje odlišně.
**Vnitřní Mongolsko (čínská provincie)**- Aktuálně vláda vydala návrh opatření na přerušení všech těžebních a obchodních operací s kryptoměnami, a to do konce dubna 2021. Důvodem je omezení v energeticky náročných průmyslových odvětvích. Momentálně je zde zákaz těžby a obchodování, držení je povoleno. https://supchina.com/2021/03/09/c/

[69] **Compliance náklady** – jsou náklady institucí a jednotlivců zapříčiněné aktivitami, které požaduje regulace, které by nebyly vyvolány, kdyby neexistovala. Blíže viz BAŽANTOVÁ, Ilona a kol. *Ekonomie regulace: soudobé trendy a compliance costs*. 1. vyd. Praha: Vladimír Lelek, 2011. s. 24 – 25. ISBN 978-80-904837-1-2.

[70] **Transakční náklady** – patří do tématů, kterými se zabývá institucionální ekonomie a lze definovat jako náklady, které je potřeba vynaložit k informování, vyjednávání, posuzování a rozhodování ohledně uzavíraného kontraktu a jeho realizací. Blíže viz BAŽANTOVÁ, Ilona a kol. *Ekonomie regulace: soudobé trendy a compliance costs*. 1. vyd. Praha: Vladimír Lelek, 2011. s. 32 - 33. ISBN 978-80-904837-1-2.

**Nepředvídatelnost** - tyto náklady jsou nepředvídatelné z pohledu, kdy se s nimi setkáme, tzn. může nastat situace, kdy v rámci již probíhajících aktivit začne platit nová regulace, která může ekonomickou výhodnost těžby, konkrétní kryptoměny, změnit. U regulace, která je dlouhodobě platná, tyto problémy odpadají a vyčíslitelnost nákladů z nich plynoucí je možná, ovšem tuto vlastnost regulace kryptoměn nemá, jelikož se jedná o nové regulace na téma, která jsou krátce probírána

**Výše** - jedná se o náklady u kterých se jejich výše nedá de facto předpokládat, i přesto, že například v České republice je pro tyto účely využívána RIA[71], náklady v praxi pro těžaře a obchodníky s kryptoměnami jsou jiné.

Z popsaných důvodů, zahrnutí těchto nákladů do výpočtu rentability nebude aplikováno. Výsledek rentability by mohl být zkreslený, a to z toho důvodu, že přesná data pro potřeby výpočtu, lze obtížně hledat a ověřovat.

### 2.3.3 Výběr a dostupnost těžebního HW

Jedním z nutných kroků před započetí těžby je nutnost vlastnit kryptoměnovou peněženku. Tato peněženka slouží k tomu, aby vytěžená jednotka kryptoměny byla připsána správnému vlastníkovy. Z tohoto důvodu vůbec SW systém nepovoluje zahájení těžby bez kryptoměnové peněženky. Na softwarovou peněženku je potřeba vyčlenit možné pořizovací náklady.

Softwarová peněženka je dostupná okamžitě a její pořizovací náklady jsou výrazně nižší, až zanedbatelné. Peněženka je druh SW který široce dostupný. Přístup do peněženky je umožněn z jakéhokoliv počítače, který je připojený k internetu a je chráněn heslem. Nevýhodou je kontrola nad privátním klíčem, který je vlastněný společností, která daný SW poskytuje. To znamená, že riziko možného odcizení může být vysoké.[72] U hardwarové peněženky se pořizovací náklady pohybují v řádech jednotek tisíc korun. Jedná se o HW na kterém je

[71] RIA blíže viz Vláda ČR, 2016. Obecné zásady pro hodnocení dopadů regulace (RIA). [online]. [cit. 27.4.2021]. Dostupné z: https://ria.vlada.cz/wp-content/uploads/Obecn%C3%A9-z%C3%A1sady-pro-RIA-2016.pdf

[72] Krypto peněženka - Jaká je nejvíce bezpečná? » Finex.cz. Finanční magazín Finex.cz - Objektivní průvodce světem financí [online].[cit. 23.04.2021]. Dostupné z: https://finex.cz/rubrika/kryptomeny/penezenky/

umístěna peněženka včetně privátního klíče. Z hlediska bezpečnosti je hardwarová peněženka bezpečnější, protože přístup k privátnímu klíči má pouze vlastník peněženky. Míra rizika je nižší než u peněženek SW.[73]

Posuzovat vhodný výběr peněženky lze z hlediska pořizovacích nákladů, bezpečnosti, míry obtížnosti instalace, přenositelnosti či dostupnosti. Pořizovací náklady na peněženku jsou zahrnuty do výpočtu rentability.

K procesu zahájení těžby kryptoměny se využívají speciální softwarové aplikace. V závislosti na vybrané kryptoměně je nutné najít odpovídající těžební pool. Pro každou kryptoměnu se používá jiný těžební pool. Následuje stažení SW aplikace, která umožní samotnou těžbu. Samozřejmou podmínkou je nepřetržitá internetová konektivita. Ještě před stažením je nutné zadat parametry HW, který kryptoměnu bude těžit a to z důvodu, aby došlo ke stažení náležité verze SW. Nekompatibilní verze SW a HW pro těžbu nelze společně použít.

Těžař zpravidla hned po spuštění SW aplikace mění v příkazovém řádku adresu poolu, port, ssl připojení a defaultní číslo peněženky. Tímto krokem dochází ke správnému nastavení v SW aplikaci. Vytěžování jednotek kryptoměn probíhá na správné adrese těžebního poolu. Vytěžené kryptoměny ve stanovený čas převedou do peněženky skutečného vlastníka.

Na webu těžebního poolu pak můžeme těžař sledovat vlastní aktivitu. Automaticky se zobrazuje hodnota podílu výkonu GPU, hardware hashrate a očekávaný denní zisk. Zobrazování hodnot v uživatelském prostředí se může lišit dle nastavení a možností konkrétního těžebním poolu.[74]

[73] Tamtéž

[74] Těžte BTC doma pomocí GPU – návod pro začátečníky . PCTuning - Titulni stranka [online]. [cit. 27.4.2021]. Dostupné z: https://pctuning.tyden.cz/hardware/graficke-karty/61723-tezte-btc-doma-pomoci-gpu-navod-pro-zacatecniky?start=3

## 2.4 Výpočet rentability

### 2.4.1 Výpočet

Pod pojmem rentabilita je obecně myšlena schopnost dosáhnout zisku na základě vložených prostředků. Je tedy zásadním ukazatelem hospodářského výsledku ekonomické transakce. V souvislosti se stanovením rentability těžby kryptoměn se jeví jako vhodné použití rentability vlastního kapitálu (ROE), jejíž výpočet ukáže, nakolik je těžba kryptoměn výhodná či nevýhodná. Výsledný ukazatel je vyjádřen v procentech.

Vzhledem k nenulovým nákladům nezbytným pro zahájení konkurenceschopné těžby musí každý odpovědný investor znát rentabilitu vlastního kapitálu. Při rozhodování pak musí zohlednit i náklady obětované příležitosti.[75]

**Re (Revenue) – příjmy za sledované období**

$$Re = \left[\left(\frac{HWhsr}{Nhsr} * \frac{t}{Mt}\right) * (Rb + Rtr)\right] * R$$

Vstupní parametry (příjmy):

***HWhsr*** *= 13,5 Th/s*
***Nhsr*** **=** *14 923 656 Th/s*
***t*** *= 1 440 min*
***Mt*** *= 10 min*
***Rb*** *= 12,5 BTC*
***Rtr*** *= 3 BTC*
***R*** *= 13 465 $/BTC*

[75] Náklady obětované příležitosti – v rámci těžby kryptoměn lze vnímat náklady obětované příležitosti zejména jako ztrátu možnosti využití vlastní kapitálu, investovaného do těžebního HW, namísto investice do jiné činnosti, která má potencionálně vyšší rentabilitu.

$$Re = \left[\left(\frac{13{,}5}{14\ 923\ 656} * \frac{1\ 440}{10}\right) * (12{,}5\ +\ 3)\right] * 13\ 465$$

***Re = 27,19 $/den***

**Co (Costs) – výdaje za sledované období**

$$Co = (Pe * t * e) + \left[\frac{(Phw+Pa)}{Lhw}\right]$$

Vstupní parametry (výdaje):

***Pe** = 0,191 $/kWh*

***t** = 24 h*

***e** = 1,323 Wh = 1 323 kWh*

***Phw** = 2 320 $*

***Pa** = 180 $*

***Lhw** = 3,5 r = 1 460 d*

$$Co = (0{,}247 * 24 * 1{,}323) + \left[\frac{(2\ 320+180)}{1\ 460}\right]$$

***Co = 8,38 $/den***

**Re (Revenue) – příjmy za sledované období**

Tabulka 2 – vstupní data pro účely výpočtu Re

| Datum | Rb (BTC) | Rtr (BTC) | Mt (min) | t (min) | R ($/BTC) | HWhsr (Th/s) | Nhsr (Th/s) |
|---|---|---|---|---|---|---|---|
| 1.1.2018 | 12,5 | 3 | 10 | 1440 | 13465 | 13,5 | 14 923 656 |

**Co (Costs) – výdaje za sledované období**

Tabulka 3 – vstupní data pro účely výpočtu Co

| Datum | Phw ($) | Pa ($) | e (KWh) | Pe ($) | t (h) | Lhw (d) |
|---|---|---|---|---|---|---|
| 1.1.2018 | 2320 | 180 | 1,323 | 0,192 | 24 | 1460 |

Do výpočtu nám vstupují data k 1.1.2018, které budeme požívat jako data výchozí. Do příjmu nám vstupují následující parametry:

**Rb – příjem za vytěžený blok**, nebo také odměna, která je ve výpočtu konstantní jednotkou. Používáme hodnotu 12,5 BTC za vytěžený blok, pro lepší pochopení budeme tuto hodnotu považovat za konstantní, jelikož její volatilita je minimální.

**Rtr – příjem za transakci**, nebo-li odměna za transakci, která je připočítávána k odměně za vytěžený blok. V tomto příkladu je jednotka konstantou.

**Mt – doba vytěžení bloku** – počítáme 10 minut na vytěžení jednoho bloku, tato jednotka je neměnná a vstupuje jako konstanta.

**t – čas**, ve výpočtu je sledované období jeden den, resp. čas přepočítaný na minuty a hodiny za den, což je 1 440 minut nebo 24 hodin. V tomto případě je čas konstantní jednotkou.

**R – kurz**, aktuální směnný kurz k určitému datu je pro nás jednotkou proměnnou v čase. Ve výchozím příkladě je počítáno k určitému časovému úseku, tedy s hodnotou k danému dni. K jinému časovému úseku je nutné počítat s aktuální hodnotou viz níže.

**HWhrs – hashrate hardwaru**, resp. výkon těžebního počítače. V tomto příkladě uvažujeme těžbu na těžebním počítači Bitmain Antminer S9, který má výkon 13,5 Th/s. V průběhu času se jeho výkon může snižovat, v tomto případě však počítáme s jeho výkonem, jako s konstantní jednotkou.

**Nhsr – hashrate sítě,** nebo obtížnost těžby je proměnnou jednotkou a k výchozímu datu byla ve výši 14 923 656 (Th/s). Ve výchozím příkladu počítáme s touto hodnotou, dále se budeme zabývat proměnou této jednotky v čase.

**Phw – cena těžebního HW**, je v tomto případě 2 320 $. Uvažujeme, že se těžba zahájila k výchozímu datu a bereme v potaz dostupný HW i tržní ceny k tomuto datu. V příkladu je s cenou těžebního HW počítáno jako s konstantní jednotkou.

**Pa – cena HW příslušenství**, je v tomto případě vypočítána na 180 $. Jedná se o síťový kabel, zdroj a o ostatní příslušenství kompatibilní s Bitmain Antminerem S9. V tomto případě se jedná o konstantní jednotku.

**e – spotřeba elektřiny**, což je spotřeba elektřiny těžebního zařízení Bitmain Antmineru S9, která je 1,323 KWh. V tomto případě se jedná o konstantní jednotku.

**Pe – cena elektřiny**, je vyjádřena v amerických dolarech. V našem případě se jedná o průměrnou cenu elektřiny v daném roce těžby. K výchozímu datu zahájení těžby byla průměrná cena v roce 2018 ve výši 0,192. V našem případě do příkladu bude vstupovat jako proměnná jednotka, která se bude měnit meziročně.

**Lhw - životnost hardwaru**, v našem případě počítáme uvažujeme životnost těžebního HW na 3,5 roku od pořízení. Do příkladu vstupuje jako konstantní jednotka přepočítaná na počet dní životnosti, což vychází na 1460 dní.

**Interpretace výsledků**

Tabulka 4 – interpretace výsledků Re, Co

| Datum | Re ($) | Co ($) | Re-Co ($) |
|---|---|---|---|
| 1.1.2018 | 27,19 | 7,81 | 19,38 |

K výchozímu datu je denní příjem ve výši 27, 19 $ a denní výdaj ve výši 7, 81 $. Rozdíl mezi příjmem a výdajem, tedy zisk před zdaněním, vychází ve výši 19, 38 $.

Opravdové vypovídající hodnoty dosáhneme pouze v čase, kde uvažujeme určité vstupy jako proměnné jednotky. K výchozímu datu je těžba Bitcoinu výhodná, ale jelikož se jedná o velice proměnný trh, den následující tomu už tak být nemusí. Je tedy nezbytné těžbu počítat v čase. V následujícím příkladě je sledované období těžby od 1.1.2018 – 30.4.2021 a proměnnými jednotky jsou **Nhsr, R a Pe.** Ve sledovaném období bude zjišťováno, kolik bude denní zisk/ztráta před zdaněním, ale také ukazatel rentability vlastního kapitálu.

**ROE (Return Of Equity)** - rentabilita vlastního kapitálu

$$ROE = \frac{Re - Co - T}{Phw + Pa} * 100$$

Vstupní parametry:

***Re*** *= 27,19 $/den*
***Co*** *= 7, 81 $/den*
***T*** *= 15%*
***Phw*** *= 2 320 $*
***Pa*** *= 180 $*

$$ROE = \frac{27{,}19 - 10{,}13 - (19{,}38 * 0{,}15)}{2\ 500} * 100$$

$$\boldsymbol{ROE = 0{,}61\%}$$

Tabulka 5 – vstupní data pro výpočet ROE a interpretace výsledků

| Re | Co | Re-Co | T (15%) | ROE (%) |
|---|---|---|---|---|
| 27,19 | 7,81 | 19,38 | 4,08 | 0,61 |

Pro potřeby našeho výchozího výpočtu je sledované období 24 hodin, výpočet vychází z dat k 1.1.2018. V tomto výpočtu je použit typ těžebního HW Bitmain Antminer S9 a je zde použita cena elektřiny v České republice. Náklady jsou udávány v jednotce fiat měny, pro naše potřeby je využívána výchozí jednotka americký dolar.

Ve výchozím příkladu jsme si nejprve vypočítali celkový příjem z vytěžené kryptoměny za den, kde chceme obecně dosáhnout co nejvyšší hodnoty. Dále jsme si vypočítali celkové výdaje na všechny vytěžené kryptoměny za den, kde chceme obecně dosáhnout co nejnižší hodnoty.

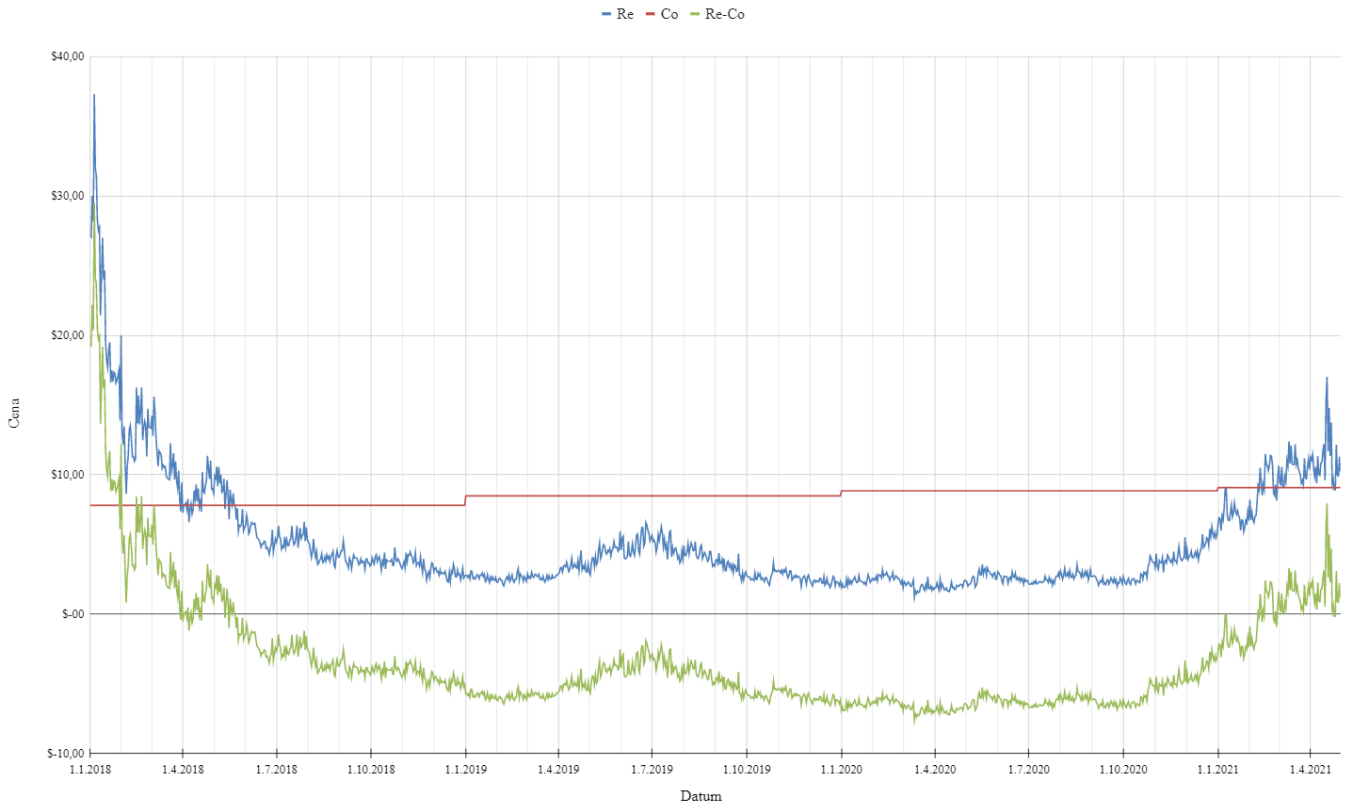
V našem případě vyšly příjmy = 27,19 $/den a výdaje = 8,38 $/den, rozdílem je tedy zisk před zdaněním = 19,38 $. Můžeme tedy zhodnotit, že jsme k fixnímu datu, resp. ke určitému dni v roce 2018 vykazovali zisk.

Ukazatel rentability vlastního kapitálu vychází na 0,61 %, což v tomto případě značí, že se náš vložený kapitál zhodnotil za tento daný den o 0,61 %. V tento konkrétní den lze označit výsledek těžby, jako pozitivní, ovšem o výhodnosti lze hovořit až s větším množstvím dat. Pro zhodnocení výhodnosti nebo nevýhodnosti těžby kryptoměny prostřednictvím rentability vlastního kapitálu jsou důležité vstupní proměnné, které budou do příkladu zaneseny viz další kapitoly. Vstupními proměnnými jsou čas, směnný kurz a celkový Hashrate sítě. Tyto vstupní

proměnné totiž ovlivňují hodnoty v čase. Na základě předchozího výsledku nelze totiž odhadnout, zda po celou dobu výkonu činnosti se bude vyvíjet trend v čase tímto směrem.[76]

K výchozímu datu nám vychází ukazatel 0,61%, tzn. že v tento den by došlo ke zhodnocení vlastního kapitálu o 0,61%. Nicméně k jednomu dni, z celé těžby nelze přisuzovat významnost, tudíž opět zde budeme počítat s ukazatelem ROE v celém sledovaném období.

Obrázek 4 – vývoj Re, Co, Re-Co ve sledovaném období od 1.1.2018 do 30.4.2021




Dne 1.1.2018 by bylo výhodné těžit kryptoměnu Bitcoin, za těchto podmínek. Obtížnost těžby nebyla tolik náročná v porovnání s rokem 2021 a byla tím pádem vyšší pravděpodobnost dosažení úspěšného vytěžení bloku. Dalším aspektem kladného výsledku je vstupní cena

[76] Podobně také HEISSLER, Herbert a kol. Ekonomie bitcoinu: analýza a modelování bitcoinu v rozvinutém stadiu. Vydání první. Praha: Vysoká škola finanční a správní, o.p.s., 2014. s. 69. ISBN 978-80-7408-104-0.

elektřiny, která byla z hlediska sledovaného období nejnižší. Nejpodstatnějším vstupem je směnný kurz, který se pohyboval k tomuto datu kolem 13 tis. amerických dolarů.

Nejzásadnějším vstupem, který může značně ovlivnit celkový výsledek je Hashrate Sítě, který se na začátku roku 2018 pohyboval kolem 15 000 000 Th/s. Na základě hodnoty Hashrate sítě je možné si vypočítat vlastní podíl na síti, který je v tomto případě neměnný, to znamená, že čím větší bude hodnota Hashrate sítě, tím nižší bude pravděpodobnost dosažení jednoho bloku.

Z grafu je patrné. Že tento vstup hraje zásadní roli na příjmech, které z vytěženého bloku plynou. Na začátku období se pohyboval kurz Bitcoinu kolem 13 tis. amerických dolarů a na konci sledovaného období je kurz čtyř až pětinásobně vyšší, respektive se pohybuje kolem 60 tis. amerických dolarů. Na první pohled se může jevit, že by mělo dojít automaticky k vyššímu příjmu z těžby než na začátku období, ale není tomu tak. Jak již bylo zmíněno, kritickým vstupem je Hashrate sítě. Na konci sledovaného období je až jedenáctkrát vyšší než na začátku sledovaného období, aby mohlo dojít alespoň k přibližným výsledkům příjmů z těžby, musel by mít Hashrate sítě stejnou tendenci růstu, jako kurz Bitcoinu.

Na začátku a na konci sledovaného období, dochází k zisku především. V mezidobý jsou výsledky spíše ztrátové, což zapříčiňuje především pokles kurzu Bitcoinu. Lze tedy tvrdit, že kurz Bitcoinu je nejdůležitějším vstupem, k tomu, abychom mohli uvažovat o výhodnosti. Jeho vývoj je ale velice nepředvídatelný a nelze odhadnout, jak se bude v budoucích letech chovat. Kdyby se kurz Bitcoinu držel ve stejných hodnotách a rostl podobně rychle, jako Hashrate sítě, mohli bychom předpokládat, že výsledky těžby by mohli mít podobný trend, jako na konci sledovaného období. Tuto jistotu však mít nemůžeme. Jedná se o mimořádně volatilní trh a ze dne na den, může kurz Bitcoinu významně poklesnout, což by mělo kritický dopad na výsledky těžby.

# Závěr

Hlavním cílem této práce bylo zhodnotit jednotlivé možnosti těžby kryptoměn a spočítat jejich rentabilitu vlastního kapitálu. Mezi dalšími cíli bylo definovat kryptoměny a jejich ekosystém, popsat základní principy kryptografie a další s těžbou kryptoměn související aspekty.

Vytyčené cíle se podařilo splnit, přičemž během zpracování zvolené tématiky se ukázalo, že pro splnění cíle hlavního je nutné některé aspekty problematiky hlouběji specifikovat a jiné naopak upozadit.

Při zpracování tématu bylo čerpáno z mnoha vědeckých i nevědeckých zdrojů. Mezi primárními zdroji byly zanalyzovány především data týkající se směnného kurzu vybraných kryptoměn, cen elektřiny ve vybraných zemích a hashrate sítě. Jako sekundární zdroj byla použita tuzemská i zahraniční odborná literatura, především vědecké monografie. S ohledem na rychlost vývoje tématu bylo nezbytné čerpat i z nevědeckých zdrojů, které často obsahují aktuální a relevantní údaje. V rámci posuzování proveditelnosti těžby byly dále analyzovány i právní předpisy týkající se zejména legálnosti podnikání v oblasti těžby kryptoměn a jejího zdanění.

Co se týká metodiky zkoumání, sekundární zdroje byly podrobeny literární rešerši, na jejímž základě byly definovány základní atributy týkající se těžby kryptoměn. Primární zdroje byly analyzovány a použity jako podklady pro výpočty v praktické části.

Práce se skládá ze dvou částí, a to části teoretické a části praktické. Hlavním těžištěm práce je část praktická, která obsahuje metodiku, výpočtové vzorce, jejich proměnné, resp. vstupy, a další hlediska, která jsou nutná pro hlavní cíl práce, kterým je ekonomické zhodnocení těžby kryptoměn. V teoretické části jsou pak zmíněny důležité aspekty, které obsahují doplňující informace vztahující se k hlavnímu cíli práce.

V prvních kapitolách práce je vysvětlen pojem kryptoměny, vč. jejích vlastností. Dále je navázáno popisem jednotlivých druhů kryptoměn a jejich možných dělení. V těchto částech bylo popsáno, co se pod pojmem kryptoměna skrývá a z vysvětlení jejich vlastností pak vyplynulo, co kryptoměnou je a není v komparaci s definicí samotnou. V souladu s hlavním cílem práce je i seznámení se s kryptoměnami, o kterých jsou známa historická data, která mohou být podstatná pro zjištění výhodnosti těžby.

V následujících kapitolách pak došlo k vysvětlení vybraných důležitých aspektů ekosystému kryptoměn, jelikož je pro jejich existenci nezbytný a vykazuje například oproti fiat měnám

významné odlišnosti. Dále je zde popsán princip těžby kryptoměn a vysvětleny důležité kroky, které je nezbytné znát a splnit, aby bylo možné kryptoměnu těžit.

V závěrečných kapitolách teoretické části jsou popsány i další možnosti získání kryptoměn, což je nezbytné pro povědomí fungování obchodu a dále pak legální hledisko těžby kryptoměn, které sice není tradičním ekonomickým ukazatelem, ale přesto může výhodnost těžby kryptoměn významně ovlivnit a nelze je tedy opomenout.

Po části teoretické následuje část praktická, která je stěžejní pro hlavní cíl práce, jelikož nabízí čtenáři výpočtové vzorce, které mu mohou odpovědět na otázku, zda je kryptoměny výhodné těžit. Začátek praktické části se zabývá metodikou, ve které jsou popsány vzorce pro výpočet ukazatele rentability vlastního kapitálu. V této souvislosti jsou přehledně vysvětleny jednotlivé parametry a způsob, jak byl celý vzorec stanoven, vč. dílčích výpočtů pro srozumitelnost.

Následuje pak popis rozhodovacích hledisek a metod těžby, jež jsou stěžejním kritériem pro rozhodnutí vhodné metody těžby. Nebyly opomenuty ani dílčí compliance náklady.

Posléze je věnována pozornost i dostupnosti a výběru těžebního hardwaru, který je pro pro proces a udržitelnost těžby zásadní. V následující kapitole je proveden výpočet rentability na kryptoměně Bitcoin v určeném časovém horizontu.

V závěru práce jsou zhodnoceny výsledky výpočtu v průběhu sledovaného období, na kterém je demonstrováno, kdy bylo kryptoměnu těžit výhodné a kdy naopak. Z výsledku výpočtu vyplynulo, že důležitými prvky, které mohou značně ovlivnit výsledek těžby, jsou směnný kurz kryptoměny, hashrate sítě a cena elektřiny. Nelze však opomenout ani stabilitu jednotlivých kryptoměn, kterou lze vypozorovat z dosavadního vývoje jejich směnného kurzu, jeho volatility. V neposlední řadě je pak třeba zvážit i reputaci samotných kryptoměn, která může být ovlivněna politickou situací, resp. mírou jejich regulace a zákazů v různých státech světa. Závěrem lze konstatovat, že v rámci zkoumání tématu došlo k naplnění cílů práce. Příklad je demonstrován na referenční kryptoměně Bitcoin, nicméně použité vzorce a závěry lze jen s nepatrnými úpravami aplikovat i na jiné kryptoměny a zjistit jejich rentabilitu.

# Seznam použitých zdrojů

## Tištěné zdroje


ANTONOPOULOS, Andreas M. Mastering Bitcoin: programming the open blockchain. Second edition. Sebastopol, CA: O'Reilly, 2017. ISBN 9781491954386.

BAŽANTOVÁ, Ilona a kol. Ekonomie regulace: soudobé trendy a compliance costs. 1. vyd. Praha: Vladimír Lelek, 2011. 111 s. ISBN 978-80-904837-1-2.

BIANCJI, Daniele and BABIAK, Mykola. On the Performance of Cryptocurrency Funds Working paper series – 672. Prague: Charles University, Center for Economic Research and Graduate Education, 2020. 54 s. ISBN 978-80-7343-479-3.

HARTMAN, Ondřej. Začínáme na burze: jak uspět při obchodování na finančních trzích - akcie, komodity a forex. Brno: BizBooks, 2013. ISBN 9788026500339

HEISSLER, Herbert a kol. Ekonomie bitcoinu: analýza a modelování bitcoinu v rozvinutém stadiu. Vydání první. Praha: Vysoká škola finanční a správní, o.p.s., 2014. 94 s. ISBN 978-80-7408-104-0.

HUJOVÁ, Gabriela, ed. Zkušenosti s virtuálními měnami - Bitcoin měna budoucnosti?: sborník z konference: Praha, 26. března 2014. Praha: Vysoká škola manažerské informatiky, ekonomiky a práva, 2014. 149 s. ISBN 978-80-86847-71-9.

KALISKÝ, Boris. Bitcoin a ti druzí: nepostradatelný průvodce světem kryptoměn. [Praha]: IFP Publishing, 2018. 133 stran. ISBN 978-80-87383-71-1

KALOUDA, František. Finanční a cost-benefit analýza podniku. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2019. 236 s. ISBN 978-80-7380-778-8.

LÁNSKÝ, Jan. Kryptoměny. Vydání první. V Praze: C.H. Beck, 2018. 144 s. ISBN 978-80-7400-722-4.

POPPER, Nathaniel. Digital gold: bitcoin and the inside story of the misfits and millionaires trying to reinvent money. New York: Harper, 2016. ISBN 9780062362506.

ROTHSTEIN, Adam. The End of Money The Story of bitcoin, cryptocurrencies and the blockchain revolution. London: Hodder & Stoughton General Division, 2017. 240 p. ISBN 978-1473-62953-0.

ROTHBARD, Murray Newton. Peníze v rukou státu: jak vláda zničila naše peníze. Praha: Liberální institut, 2001. s. 144

SAMUELSON, Paul Anthony a NORDHAUS, William D. Ekonomie: 19. vydání. Vyd. 1. Praha: NS Svoboda, 2013. 715 s. ISBN 978-80-205-0629-0.

STROUKAL, Dominik a SKALICKÝ, Jan. Bitcoin a jiné kryptopeníze budoucnosti: historie, ekonomie a technologie kryptoměn, stručná příručka pro úplné začátečníky. 2., rozšířené vydání. Praha: Grada Publishing, 2018. 195 s. ISBN 978-80-271-0742-1.

URBAN, Jan. Teorie národního hospodářství. 2., dopl. a rozš. vyd. Praha: ASPI, 2006. 515 s. ISBN 80-7357-188-9.

## Elektronické zdroje


ASIC vs GPU Mining: Which Is Better in 2021?. cryptocoingossip.com: Simplifying Cryptos and Blockchain. [online].[cit. 27.04.2021]. Dostupné z: https://ccoingossip.com/asic-vs-gpu-mining/

Attention Required! | Cloudflare. Attention Required! | Cloudflare [online].[cit. 23.04.2021]. Dostupné z: https://www.etoro.com/crypto/why-bitcoin-fluctuates/

BITCOIN - Kurz BTC/Bitcoin [online].[cit. 27.4.2021]. Dostupné z: http://www.kurzy.cz/bitcoin/

Bitcoin Cash - aktuální a historické ceny kryptoměny [online]. [cit. 23.04.2019]. Dostupné z: http://www.kurzy.cz/komodity/bitcoin-cash-graf-vyvoje-ceny/usd-3-roky?

Bitcoin mining is still huge in China despite new ban in Inner Mongolia – SupChina. SupChina | Reporting on China without fear or favor [online].[cit. 23.04.2021]. Dostupné z: https://supchina.com/2021/03/09/bitcoin-mining-is-still-huge-in-china-despite-new-ban-in-inner-mongolia/

Bitcoin Volatility Index (0.69%) | Bitcoin Volatility Explained (2021 Updated). 99Bitcoins - How to Buy Bitcoin in 2021 | Best Bitcoin Wallets & Exchanges [online].[cit. 23.04.2021]. Dostupné z: https://99bitcoins.com/bitcoin/historical-price/volatility/

Bitcoinmat [online].[cit. 23.04.2021]. Dostupné z: https://bitcomat.com/

Buy ASIC Bitcoin Miners & Bitcoin Mining Equipment - Bitmain. Wayback Machine [online]..[cit. 23.04.2021]. Dostupné z: http://web.archive.org/web/20180104105846/https://shop.bitmain.com/

Crypto Exchange Hacks: The Mt. Gox Scandal and More | Gemini. Cryptocurrency Exchange to Buy Bitcoin and Ether | Gemini [online]. [cit. 20.04.2021]. Dostupné z: https://www.gemini.com/cryptopedia/mt-gox-bitcoin-exchange-hacked

Dash - DASH/Dash kurz [online].[cit. 23.04.2019]. Dostupné z: http://www.kurzy.cz/dash/

Difference between Private key and Public key - GeeksforGeeks. GeeksforGeeks | A computer science portal for geeks [online].[cit. 23.04.2019]. Dostupné z: https://www.geeksforgeeks.org/difference-between-private-key-and-public-key/

Funkce Výkon GPU. 301 Moved Permanently [online].[cit. 23.04.2021]. Dostupné z: https://helpx.adobe.com/cz/illustrator/kb/gpu-performance-preview-improvements.html

Handbook of blockchain, digital finance, and inclusion. Volume 1, Cryptocurrency, finTech, insurTech, and regulation [online]. London, England: Academic Press, 2018, ©2018 [cit. 2021-05-10]. ISBN 978-0-12-810442-2. Dostupné z: https://ebookcentral.proquest.com/lib/natl-ebooks/detail.action?docID=4939374

How does Ethereum work, anyway?. Introduction | by Preethi Kasireddy | Medium. Preethi Kasireddy – Medium [online]. [cit. 23.04.2019]. Dostupné z: https://preethikasireddy.medium.com/how-does-ethereum-work-anyway-22d1df506369

How To Mine Cryptocurrency: Beginner's Guide To Crypto Mining. Best Online Courses to Kickstart Your Career: eLearning on BitDegree [online].[cit. 23.04.2021]. Dostupné z: https://www.bitdegree.org/crypto/tutorials/how-to-mine-cryptocurrency

Jak funguje Bitcoin? [online].[cit. 27.4.2021]. Dostupné z: http://kryptostart.cz/kryptomeny/bitcoin/

Jak na zdanění digitálních měn - Služby a podnikání. Vzdělávací a rekvalifikační kurzy Praha [online].[cit. 23.04.2021]. Dostupné z: https://www.sluzbyapodnikani.cz/jak-na-zdaneni-digitalnich-men/

Krypto peněženka - Jaká je nejvíce bezpečná? » Finex.cz. Finanční magazín Finex.cz - Objektivní průvodce světem financí [online].[cit. 23.04.2021]. Dostupné z: https://finex.cz/rubrika/kryptomeny/penezenky/

Kryptoměnová burza Bittrex – recenze, zkušenosti, návod na obchodování, poplatky. Investice a spoření | InvestPlus [online].[cit. 23.04.2021]. Dostupné z: https://investplus.cz/investice/kryptomenova-burza-bittrex-recenze-zkusenosti-navod-na-obchodovani-poplatky/

Kryptoměny a Bitcoin. Kam investovat? Vzdělávej se a propoj s odborníky [online]. [cit. 27.4.2021]. Dostupné z: https://investree.cz/category/kryptomeny/

KRYPTOMĚNY a DANĚ - Jak na to? Návod [Aktuální 2021]. Finanční magazín Finex.cz - Objektivní průvodce světem financí [online].[cit. 23.04.2021]. Dostupné z: https://finex.cz/zdaneni-kryptomen-kompletni-navod/

Kurzy.cz, spol. s. r. o., AliaWeb, spol. s.r.o.[online]. [cit. 23.04.2019]. Dostupné z: https://bitcoinblog.cz/

LISTINA ZÁKLADNÍCH PRÁV A SVOBOD [online].[cit. 23.04.2021]. Dostupné z: http://www.psp.cz/docs/laws/listina.html

MARTINÁK, Tomáš a kol. Bezhotovostní peníze versus elektronické peníze. 1. vydání. Olomouc: Iuridicum Olomoucense, s.r.o., ve spolupráci s Právnickou fakultou Univerzity Palackého v Olomouci, 2015. 188 stran. Acta iuridica Olomucensia. Monografie a studie. ISBN 978-80-87382-74-5

Mining - Dash. Dash - Dash is Digital Cash You Can Spend Anywhere [online].[cit. 23.04.2019]. Dostupné z: https://www.dash.org/mining/

Mining for nil-transaction blocks only - gaming the incentive scheme by rogue miners / consortium? - Bitcoin Stack Exchange. Bitcoin Stack Exchange [online].[cit. 23.04.2021]. Dostupné z: https://bitcoin.stackexchange.com/questions/41411/mining-for-nil-transaction-blocks-only-gaming-the-incentive-scheme-by-rogue-mi

Nonce [online].[cit. 23.04.2019]. Dostupné z: https://academy.binance.com/en/glossary/nonce

Nonce | Binance Academy. [online]. [cit. 27.4.2021]. Dostupné z: https://academy.binance.com/en/glossary/nonce

OZORA, Ogino: PROOF-OF-STAKE (POS) [online].[cit. 27.4.2021]. Dostupné z: https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/

RIA blíže viz Vláda ČR, 2016. Obecné zásady pro hodnocení dopadů regulace (RIA). [online]. [cit. 27.4.2021]. Dostupné z: https://ria.vlada.cz/wp-content/uploads/Obecn%C3%A9-z%C3%A1sady-pro-RIA-2016.pdf

Software wallet [online].[cit. 23.04.2021]. Dostupné z: https://btcdirect.eu/en-gb/software-wallet

Těžba kryptoměn - Jak těžit Bitcoin a jiné krypto? » Finex.cz. Finanční magazín Finex.cz - Objektivní průvodce světem financí [online].[cit. 23.04.2021]. Dostupné z: https://finex.cz/rubrika/kryptomeny/tezba/

Těžba kryptoměn - návod a tipy jak na to | E15.cz. E15.cz - Byznys, politika, ekonomika, finance, události [online].[cit. 23.04.2021]. Dostupné z: https://www.e15.cz/tezba-kryptomen

Těžte BTC doma pomocí GPU – návod pro začátečníky . PCTuning - Titulni stranka [online]. [cit. 27.4.2021]. Dostupné z: https://pctuning.tyden.cz/hardware/graficke-karty/61723-tezte-btc-doma-pomoci-gpu-navod-pro-zacatecniky?start=3

Thailand electricity prices, September 2020 | GlobalPetrolPrices.com. Gasoline and diesel prices by country | GlobalPetrolPrices.com [online].[cit. 23.04.2021]. Dostupné z: https://www.globalpetrolprices.com/Thailand/electricity_prices/

The Bitmain Antminer E9 is the world's most powerful Etherium mining ASIC - NotebookCheck.net News. Notebook / Laptop Reviews and News - NotebookCheck.net [online].[cit. 23.04.2021]. Dostupné z: https://www.notebookcheck.net/The-Bitmain-Antminer-E9-is-the-world-s-most-powerful-Ethereum-mining-ASIC.535225.0.html

The status of cryptocurrency in Morocco - ScienceDirect. ScienceDirect.com | Science, health and medical journals, full text articles and books. [online].[cit. 23.04.2021]. Dostupné z: https://www.sciencedirect.com/science/article/pii/S2590051X21000058

Top 10 Best Cryptocurrencies to Mine Using GPUs in 2021 - BlockSocial. BlockSocial - Your Guide to Understanding and Capitalizing on a Decentralized World [online].[cit. 23.04.2021]. Dostupné z: https://www.blocksocial.com/best-cryptocurrencies-to-mine-using-gpu/

Trezor [online].[cit. 23.04.2019]. Dostupné z: https://trezor.io/

VIX Index - vše co je nutné vědět o indexu volatility [2020]. Broker LYNX | Investujte s výhodami [online].[cit. 23.04.2021]. Dostupné z: https://www.lynxbroker.cz/vzdelavani/vix-index-vse-co-je-nutne-vedet-o-indexu-volatility/

Vláda ČR, 2016. Obecné zásady pro hodnocení dopadů regulace (RIA). [online]. [cit. 27.4.2021]. Dostupné z: https://ria.vlada.cz/wp-content/uploads/Obecn%C3%A9-z%C3%A1sady-pro-RIA-2016.pdf

# Seznam tabulek a obrázků

## Seznam použitých zkratek a značek

| | |
|---|---|
| BCH | Bitcoin Cash |
| BTC | Bitcoin |
| Co | (Costs) výdaje za sledované období |
| D | (Difficulty) - obtížnost |
| DASH | Dash |
| e | (Electricity) - spotřeba elektřiny těžebního hardwaru |
| EAT | (Earnings after Taxes) - zisk po zdanění |
| EBT | (Earnings Before Taxes) - zisk před zdaněním |
| Eq | (Equity) – vlastní vložený kapitál |
| ETH | Ethereum |
| FO | fyzická osoba |
| HSRhw | (Hardware Hashrate) - Hashrate hardwaru |
| HSRn | (Network Hashrate) - Hashrate sítě |
| HW | Hardware |
| Lhw | (Hardware Lifetime) - životnost hardwaru |
| MB | Megabyte |
| mil. | milion |
| Mt | (Time Per One Mined Block) - doba vytěžení bloku |
| NM | (Total Network Mined Block) - celkem vytěžených bloků na síti |
| Pa | (Accessories Price) - cena hardwarového příslušenství |
| Pe | (Price Electricity) - cena elektřiny |
| Phw | (Hardware Price) - cena těžebního hardwaru |
| PO | právnická osoba |
| R | (Rate) - směnný kurz |
| Rb | (Revenue Per Block) - příjem za vytěžený blok |
| Re | (Revenue) - příjmy za sledované období |
| Re | (Revenue) – příjmy za sledované období |
| ROE | (Return Of Equity) - rentabilita vlastního kapitálu |

| | |
|---|---|
| Rtr | (Revenue Per Transaction) - příjem za potvrzení transakce |
| SW | Software |
| T | (Taxes) – daně |
| t | (Time) – čas |
| TPhw | (Total Hardware Price) - celková cena těžebního HW |
| TR | (Total Revenue) - příjmy za těžbu celkem |
| TRns | (Total Revenue Per Network Share) - příjmy za těžbu podílu na síti |

## Abstrakt

DAVÍDKOVÁ, Lenka. *Kryptoměny, ekonomické zhodnocení výhodnosti těžby* (Bachelor Thesis). Univeristy of West Bohemia, Faculty of Economics.

**Klíčová slova:** kryptoměny, těžba, blockchain, ekosystém, právní úprava, vstupy

Práce se skládá ze dvou částí, a to teoretické části a praktické části. Hlavním těžištěm práce je část praktická, která obsahuje metodiku, vstupy, a další hlediska, které jsou nutné pro hlavní cíl práce, kterým je ekonomické zhodnocení těžby kryptoměn. Praktická část je přímo závislá na teoretické části, jelikož ji doplňuje o nutný kontext, který je nezbytný pro širší pochopení celé tématiky. Teoretická část se zaměřuje zejména na vysvětlení principu těžby kryptoměn a fungování celého jeho ekosystému. V prvních kapitolách teoretické části je definován přímo pojem kryptoměna, a to z různých úhlů pohledu. Neméně důležité je také zmínka o dělení a druzích kryptoměn, abychom viděli odlišnost mezi nimi, protože současný trend nasvědčuje tomu, že kryptoměn bude přibývat a správný výběr kryptoměny může ovlivnit výhodnost těžby.

Při zhodnocení jednotlivých možností těžby a porovnání jejich výhodnosti je nutné zohlednit celou řadu proměnných vstupů při čemž je nejzásadnějšími vstupy jsou směnný kurz kryptoměny, hashrate sítě a cena elektřiny které vykazují nejvyšší míru volatility. Dalšími pak jsou, cena těžebního HW a jeho příslušenství, spotřeba elektřiny, životnost těžebního HW, výkon těžebního HW, čas vytěžení jednoho bloku, odměna za transakci, odměna za vytěžený blok, které do výpočtu vstupují jako konstantní jednotky.

Každý zmíněný vstup je v širší či užší míře vysvětlen, definován a popsán, což je důležité pro správné pochopení jeho významu pro konečný výpočet. Výsledkem analýzy vycházející z výsledků praktické části vyplývá, že výhodnost těžby kryptoměn vykazuje vysokou míru volatility v čase, a proto je nutné před jejím zahájením vyhledat všechny jednotlivé vstupy, které mohou konečnou výhodnost ovlivnit a vypočítat relevantní ekonomický ukazatel, z nějž je výhodnost těžby patrná.

## Abstract

DAVÍDKOVÁ, Lenka. *Cryptocurrency, economic analysis of mining*
(Bachelor Thesis). Univeristy of West Bohemia, Faculty of Economics.

**Key words:** cryptocurrencies, mining, blockchain, ecosystem, legal regulation, inputs

The work consists of two parts, the theoretical part and the practical part. The core of the work is the practical part, that contains methodology, inputs and other aspects, which are necessary for the main scope of the work, the scope being the economic evaluation of cryptocurrency mining. The practical part is directly dependent on the theoretical part, as it complements the necessary context, which is necessary for a broader understanding of the whole topic. The theoretical part is focused mainly on explaining the principle of cryptocurrency mining and the functioning of its entire ecosystem. In the first chapters of the theoretical part, the term cryptocurrency is directly defined from various angles of view. Equally important is also specification of the division and types of cryptocurrencies in order to see the difference among them, as the current trend suggests that the types of cryptocurrencies will increase and the correct choice of cryptocurrency may affect the advantage of mining.

When evaluating individual mining options and comparing their benefits, it is necessary to take into account a number of variable inputs, the most fundamental being the cryptocurrency exchange rate, hashrate network and the price of electricity, these having the highest degree of volatility. The other inputs are the price of mining HW and its accessories, electricity consumption, lifespan of mining HW, performance of mining HW, extraction time of one block, reward for the transaction, reward for the extracted block, which enter into the calculation as constant units.

Each of the mentioned inputs is explained in a broader or narrower extent, defined and described, that being important for a correct understanding of their significance for the final calculation. The result of the analysis, based on the results of the practical part, shows that the profitability of cryptocurrency mining has a high degree of volatility over time and therefore it is necessary to find all individual inputs that may affect the final result and calculate a relevant economic indicator from which the advantage of mining is visible.