

Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačního inženýrství



Bakalářská práce

Těžba kryptoměny a její dopad na životní prostředí

František Váňa

© 2023 ČZU v Praze

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

František Váňa

Informatika

Název práce

Těžba kryptoměny a její dopad na životní prostředí

Název anglicky

Cryptocurrency Mining and it's Enviromental Impact

Cíle práce

Cílem teoretické část je představit kryptoměnu, popsat samotný proces těžení kryptoměny, jaké jsou k tomu využívány prostředky a jaký dopad má těžení na životní prostředí. Praktická část se zaměří na porovnání měn s ohledem na to, kolik elektrické energie spotřebují a zda je efektivní je těžit, jak z ekonomického hlediska, tak z hlediska dopadu na životní prostředí.

Metodika

Metodikou teoretické části bude studium a zpracování problematiky kryptoměn a procesů, které jsou používány k jejich těžbě formou literární rešerše za použití odborných zdrojů. Praktická část bude analyzovat spotřebu elektrické energie u jednotlivých kryptoměn. Na základě výsledků z porovnání bude určeno, které kryptoměny je efektivní těžit s ohledem na životní prostředí.

Doporučený rozsah práce

30 – 40 stran

Klíčová slova

kryptoměny, blockchain, těžba kryptoměny, elektrická energie, životní prostředí

Doporučené zdroje informací

CHOWDHURY, N. Inside Blockchain, Bitcoin, and Cryptocurrencies. Milton: Auerbach Publishers, Incorporated, 2019, 362 s. ISBN 9781138618152.

CHUEN, D.L.K. Handbook of Digital Currency : Bitcoin, Innovation, Financial Instruments, and Big Data. Elsevier Science & Technology, 2015, 612 s. ISBN 9780128021170.

LÁNSKÝ, J. *Kryptoměny*. V Praze: C.H. Beck, 2018. ISBN 978-80-7400-722-4.

Předběžný termín obhajoby

2022/23 LS – PEF

Vedoucí práce

Ing. David Buchtela, Ph.D.

Garantující pracoviště

Katedra informačního inženýrství

Elektronicky schváleno dne 7. 3. 2023

Ing. Martin Pelikán, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 13. 3. 2023

doc. Ing. Tomáš Šubrt, Ph.D.

Děkan

V Praze dne 15. 03. 2023

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Těžba kryptoměny a její dopad na životní prostředí" jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 15. 3. 2023

Poděkování

Rád bych touto cestou poděkoval Ing. Davidu Buchtelovi, Ph.D. za poskytnutí cenných rad a za odborné vedení této bakalářské práce.

Těžba kryptoměny a její dopad na životní prostředí

Abstrakt

Tato práce je zaměřena na zhodnocení těžby kryptoměn a její následný dopad na životní prostředí. Je zde vysvětlen pojem kryptoměna, spolu s její historií. Dále jsou popsány hlavní vlastnosti kryptoměny a jak je těchto vlastností dosaženo pomocí různých technologií a principů. Práce dále rozebírá samotný proces těžby kryptoměny a dále uvádí všechny náležitosti pro zahájení těžby jednotlivými způsoby. Nechybí ani vysvětlení podstaty uhlíkové stopy a jak je provázána s kryptoměnami.

Vlastní práce se věnuje popisu všech potřebných náležitostí pro provozování těžby, včetně nákupu vhodného těžebního vybavení a dalších nezbytných prostředků. Na základě součtu výdajů za těžební vybavení a spotřebovanou elektřinu je vypočítán potenciální čistý výdělek z těžby. Kromě výdajů za provozování těžby a potenciálního výdělku si práce klade za cíl zjistit velikost uhlíkové stopy, jakou těžba jednotlivých kryptoměn zanechává.

Dalším cílem této práce je porovnat jednotlivé kryptoměny z hlediska nákladů na těžbu, potenciálního zisku a také velikosti uhlíkové stopy, tedy jejich dopadu na životní prostředí.

Klíčová slova: kryptoměny, blockchain, těžba kryptoměny, elektrická energie, životní prostředí, uhlíková stopa, hash rate

Cryptocurrency mining and it's environmental impact

Abstract

This bachelor thesis focuses on the evaluation of cryptocurrency mining and its further impact on the environment. The term cryptocurrency is explained, along with its history. Furthermore, are described the main characteristics of cryptocurrency and how those characteristics are achieved through different technologies and principles. The thesis also examines the process of cryptocurrency mining itself and then lists all the essentials to start mining by each method. The nature of the carbon footprint and how it is intertwined with cryptocurrencies is also explained.

This thesis itself describes all the essentials needed to for the operation of mining, including the purchase of suitable mining equipment and other necessary resources. Based on the sum of the expenses for mining equipment and the electricity consumed, the potential net revenue from mining is calculated. In addition to the costs for operating the mining process and the potential earnings, the work aims to determine the size of the carbon footprint left by mining each cryptocurrency.

Another aim of this thesis is to compare the different cryptocurrencies in terms of mining costs, potential profit and also the size of their carbon footprint, i.e. their impact on the environment.

Keywords: cryptocurrencies, blockchain, cryptocurrency mining, electric energy, environment, carbon footprint, hash rate

Obsah

1 Úvod.....	10
2 Cíl práce a metodika	11
2.1 Cíl práce	11
2.2 Metodika	11
3 Teoretická část práce	12
3.1 Kryptoměna.....	12
3.1.1 Historie kryptoměn	12
3.1.2 Bitcoin.....	13
3.1.3 Kryptografie v kryptoměnách	14
3.1.4 Peer-to-peer síť	14
3.1.5 Blockchain	15
3.1.6 Transakce	16
3.1.7 Blok.....	17
3.1.8 Důkaz prací (Proof of work).....	17
3.1.9 Důkaz podílem (Proof of stake).....	18
3.2 Těžba kryptoměny.....	19
3.2.1 Hash rate	20
3.2.2 Evoluce těžby kryptoměny	20
3.2.3 Grafické karty (GPU).....	21
3.2.4 Programovatelná hradlová pole (FPGA)	22
3.2.5 ASIC (Application Specific Integrated Circuits).....	22
3.2.6 Sólo těžba (Solo mining)	23
3.2.7 Těžba ve skupině (Pool mining).....	24
3.3 Uhlíková stopa kryptoměn	25
4 Praktická část práce.....	27
4.1 Postup při analýze	27
4.2 Bitcoin.....	29
4.2.1 Výpočet nákladů pro těžbu	29
4.2.2 Potencionální výdělek.....	31
4.2.3 Uhlíková stopa	31
4.2.4 Zhodnocení a doporučení.....	31
4.3 Dogecoin (DOGE)	32
4.3.1 Výpočet nákladů pro těžbu	33
4.3.2 Potencionální výdělek.....	35

4.3.3	Uhlíková stopa	35
4.3.4	Zhodnocení a doporučení.....	36
4.4	Litecoin (LTC)	36
4.4.1	Výpočet nákladů pro těžbu	37
4.4.2	Potencionální výdělek.....	37
4.4.3	Uhlíková stopa	37
4.4.4	Zhodnocení a doporučení.....	37
4.5	Ethereum classic (ETC)	38
4.5.1	Výpočet nákladů pro těžbu	38
4.5.2	Potencionální výdělek.....	40
4.5.3	Uhlíková stopa	40
4.5.4	Zhodnocení a doporučení.....	40
5	Výsledky a diskuse	42
6	Závěr.....	44
7	Seznam použitých zdrojů	45
8	Seznam obrázků, tabulek a zkratk	48
8.1	Seznam obrázků	48
8.2	Seznam tabulek	48
8.3	Seznam použitých zkratk.....	48

1 Úvod

Kryptoměny jsou výrazným fenoménem posledních let, který nabyl na popularitě i mezi běžnou populací. Přilákaly díky své inovativnosti mnoho nadšenců, kteří se těžbě kryptoměn začali věnovat, a to jak z řad odborníků na informační technologie a jiných příbuzných oborů, tak i z řad laické veřejnosti. O kryptoměně bylo napsáno již mnoho odborných i populárně naučných publikací, většina z nich se ale věnuje obecnému popisu kryptoměn a principu jejich fungování. Podstatně menší pozornost je pak věnována stinným stránkám kryptoměn, jako jsou například dopady těžby na životní prostředí. Právě nedostatek pozornosti věnovaný těmto tématům dal podnět k napsání této bakalářské práce, s cílem vysvětlit podstatu kryptoměn a její přínos nových technologií, tak zároveň prozkoumat i negativní aspekty, kterými působí na životní prostředí.

Na začátku této práce je vymezen její cíl a použitá metodika. Dále se teoretická část zaměřujeme na popis kryptoměny, její historii a vývoj v průběhu let a také na vysvětlení principů, na kterých je postavena. Poté jsou popsány technologie a zařízení, které jsou při těžbě používány a je popsán samotný proces těžby.

Dále je praktická část práce zaměřena na rozbor čtyř kryptoměn, které využívají důkaz prací, konkrétně se jedná o Bitcoin, Dogecoin, Litecoin a Ethereum classic. V úvodu každé kapitoly, věnující se konkrétní kryptoměně, jsou uváděny základní informace týkající se dané kryptoměny a také seznam položek, které jsou pro těžbu nezbytné. Dále je vypočítáván potenciální výdělek a velikost uhlíkové stopy, kterou za sebou těžba zanechá. Na závěr každé kapitoly je shrnutí zjištěných poznatků a doporučení týkající se dané kryptoměny.

Práce je zakončena porovnáním výsledků z hlediska různých aspektů, jako například velikosti uhlíkové stopy, ekonomické výhodnosti a dalších. Samotný závěr je věnován zamyšlením se nad potenciálním budoucím výzkumem na toto téma.

2 Cíl práce a metodika

2.1 Cíl práce

Hlavním cílem této práce je zhodnotit těžbu jednotlivých kryptoměn a stanovit, jak tato těžba ovlivňuje životní prostředí. Cílem teoretické části je představit kryptoměnu, popsat samotný proces těžení kryptoměny, jaké jsou k tomu využívány prostředky a jaký dopad má těžení na životní prostředí. Praktická část se zaměří na porovnání měn s ohledem na to, kolik elektrické energie spotřebují a zda je efektivní je těžit, jak z ekonomického hlediska, tak z hlediska dopadu na životní prostředí.

2.2 Metodika

Metodikou teoretické části bude studium a zpracování problematiky kryptoměn a procesů, které jsou používány k jejich těžbě, a to formou literární rešerše za použití odborných zdrojů. V praktické části jsou vybrány 4 kryptoměny, které budou zkoumány. V jednotlivých kapitolách je popsán způsob, jakým jsou zajištěny podmínky pro možný provoz těžby dané kryptoměny. Pro těžbu je vybráno takové zařízení, které dosahuje největší efektivity. Na základě zajištění podmínek pro těžbu je dále vypočítána suma nákladů a pomocí vzorců je spočítána šance na vytěžení dané kryptoměny a jak velký je možný výdělek z takto provozované těžby. V každé kapitole věnující se jednotlivé kryptoměně jsou zhodnoceny výsledky a jsou uvedena doporučení zjištěná v průběhu zkoumání dané kryptoměny. Následně jsou všechny kryptoměny vzájemně porovnány na základě jejich uhlíkové stopy a potenciálního výdělku.

3 Teoretická část práce

Tato část práce je zaměřena na kryptoměnu a jak funguje těžba kryptoměny. Nejprve je popsána kryptoměna, její historie, vývoj v průběhu let a na jakých principech funguje. Dále jsou představeny technologie, které jsou využívány kryptoměnami a jaká zařízení jsou využívána na těžbu kryptoměn. Tato část dále rozebírá samostatnou těžbu a těžbu v poolu, v závěru je vysvětlena podstata uhlíkové stopy ve spojitosti s kryptoměnami.

3.1 Kryptoměna

Kryptoměna je digitální měna, která by se dala považovat za elektronickou verzi peněz (Chuen, 2015, s. 6-8) a je vydávána systémem kryptoměn (Pernice & Scott, 2021, s. 1). Pro bližší představu Lánský (2018, s. 3) definuje kryptoměnu tak, že splňuje následující podmínky:

- 1) Systém nepotřebuje žádnou centrální autoritu.
- 2) Je prokazováno vlastnictví kryptoměny kryptograficky.
- 3) Možnost vzniku nové jednotky měny je systémem definována. Pokud vznikají nové jednotky kryptoměny, je systémem definováno, za jakých okolností a jakým způsobem bude určeno vlastnictví těchto jednotek.
- 4) Systém je schopný uchovávat přehled o jednotkách kryptoměny a jejich vlastnictví.
- 5) Je systémem umožněno provádět transakce, kde dochází ke změně vlastnictví kryptoměny, pouze pokud je prokázáno aktuální vlastnictví těchto jednotek.
- 6) Při zadání dvou různých pokynů pro stejné jednotky kryptoměny, provede systém pouze jednu z nich – zabrání dvojitému utrácení.

3.1.1 Historie kryptoměn

V komerční sféře používání kryptoměn začalo eCash systémem od společnosti DigiCash, Inc. z roku 1990, který umožňoval platby online i offline. Využíval kryptografických protokolů k zabránění dvojitému utrácení (double-spendingu) a chránil soukromí uživatele pomocí slepých podpisů (blind signatures). eCash byl centralizovaný systém dostupný v různých bankách a čipových kartách, používal se například ve Spojených státech amerických nebo ve Finsku. Po roce 1999 začal eCash systém společně s kryptoměnou ustupovat do pozadí, v této době byl také odkoupen firmou InfoSpace (Chuen, 2015, s. 8-9).

Termín kryptoměna začal postupně vstupovat do povědomí veřejnosti v říjnu roku 2008, a to poté, co Satoshi Nakamoto představil Bitcoin na své doméně bitcoin.org (Pernice & Scott, 2021, s. 1). Identita Satoshiho není dosud známá a není jisté, zda je Satoshi skupina nebo člověk. Satoshi začal Bitcoinový systém provozovat na svém počítači a dne 3. 1. 2009 vytvořil první blok, nazývaný také jako genesis block (základní blok). Nicméně se Bitcoinový systém rozběhl až po vytvoření druhého bloku, dne 9. 1. 2009. Postupem času se do Bitcoinového systému začalo zapojovat více osob, které se podílely na jeho vývoji nebo se snažily přicházet na nové způsoby, jak těžit Bitcoin ještě efektivněji. Začalo také vznikat spousta dalších kryptoměn, některé přímo kopírují zdrojový kód Bitcoinu pouze s tím rozdílem, že změní parametry jako je celkový počet jednotek nebo potvrzovací doba (Ong et al., 2015). Dne 22. 5. 2010 si programátor Laszlo Hancz nepřímo koupil dvě pizzy za 10 000 bitcoinů (Lánský, 2018, s. 4-8). Tento den je příznivci Bitcoinu dodnes pamatován a nazýván jako „Pizza day“. O pár měsíců později se Satoshi Nakamoto přestal podílet na vývoji Bitcoinu (Chowdury, 2019, s. 64). Rostoucí zájem o Bitcoin zapříčinil také vznik první Bitcoinové burzy nesoucí název Mt. Gox, kde byl první den kurz 20 bitcoinů za dolar. Zájem o Bitcoin stále více rostl, v roce 2015 se dokonce kryptoměny začaly studovat na vysokých školách. O dva roky později byl také přidán symbol pro Bitcoin do Unicode (Lánský, 2018, s. 4-8). Dle webu coinmarketcap.com je ke dni 25. 1. 2023 na trhu přes 22 300 různých kryptoměn.

3.1.2 Bitcoin

Bitcoin je virtuální měna vytvořená s použitím kryptografických principů a využívající blockchain a mechanismus důkaz prací (proof of work), který funguje v distribuované a decentralizované peer-to-peer síti. Tvůrce Bitcoinu, Satoshi Nakamoto, přišel s řešením problému dvojitého utrácení, a to pomocí distribuované účetní knihy (blockchain) pro přesun virtuální měny bez potřeby přítomnosti třetí strany, který dříve nebyl možný. Proto zůstává Bitcoin jako první na světě správně implementovanou kryptoměnou (Chowdhury, 2019, s. 61). Technologie Bitcoinů používá ve svém počítačovém softwaru kryptografický důkaz ke zpracování transakcí a ověření legitimacy bitcoinů, takže při zpracování plateb není potřeba třetí strany, jako např. banky (Nakamoto, 2008). Není tedy možné, aby vláda nebo jiný ústřední orgán mohl manipulovat s nabídkou bitcoinů (Chuen, 2015, s. 33-34). Konečná měnová základna je pevně stanovena na přibližně 21 milionů bitcoinů (Franco, 2014, s. 5)

z toho je aktuálně v oběhu 19 272 300 bitcoinů (Coinmarketcap.com). Předpokládá se, že v roce 2140 bude dosaženo maximálního množství bitcoinů v oběhu (Lánský, 2018, s. 9).

V Bitcoinovém systému se pro název Bitcoin používá velké B a bitcoin s malý b je použit pro jednotku měny nebo digitální adresu. Jiná běžně používaná varianta je také zkratka BTC (Chuen, 2015 s. 8-9).

3.1.3 Kryptografie v kryptoměnách

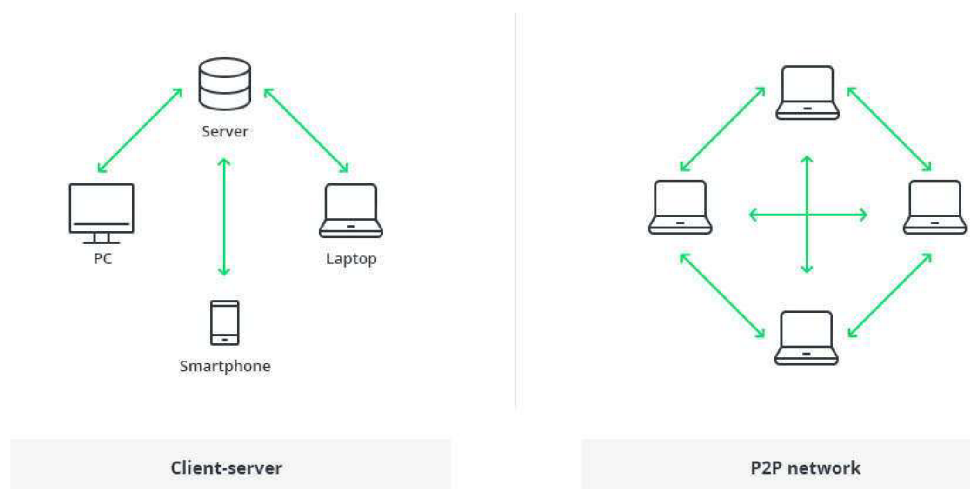
Jak bylo již zmíněno, vlastnictví jednotek kryptoměny je dokazováno kryptograficky. K tomu je využíván soukromý klíč, veřejný klíč a také hash. V případě Bitcoinu je soukromý klíč 256bitové číslo, které je generováno náhodně. Toto číslo je vytvořeno generátorem pseudonáhodných čísel (CSPRNG). Takto vytvořený soukromý klíč zabraňuje útočníkovi odvodit vygenerované číslo, ani pokud by znal část tohoto čísla. Pomocí soukromého klíče je prokazováno vlastnictví daných jednotek kryptoměny, proto by k soukromému klíči měla mít přístup pouze jedna osoba, aby nedošlo ke zneužití. Privátní klíč bývá obvykle uložen v elektronickém médiu, ztráta tohoto média by znamenala, že by vlastnictví kryptoměny nebylo možné ověřit (Lánský, 2018, s. 9).

Veřejný klíč je odvozen od soukromého klíče pomocí kryptografie eliptických křivek, kdy hash veřejného klíče slouží jako adresa. Z adresy však nelze zpětně odvodit soukromý či veřejný klíč, toto jednosměrné odvození je důvodem, proč je tento způsob bezpečný (Lánský, 2018, s.10).

3.1.4 Peer-to-peer síť

Peer-to-peer (P2P) síť je distribuovaný systém, ve kterém jsou účastníci rovnocenní a stejně privilegování. V ideální P2P síti zpřístupňují klienti část svých zdrojů, jako je výpočetní výkon, disková úložiště nebo šířku pásma sítě, přímo ostatním účastníkům sítě, aniž by potřebovali centrální koordinaci ze strany serverů nebo stabilních hostitelů. Toto uspořádání dělá z každého uzlu dodavatele i spotřebitele, na rozdíl od tradičního modelu klient–server, ve kterém je klient spotřebitelem a server působí jako zdroj a poskytovatel služeb (Chowdhury, 2019, s. 12-14). Pro lepší vysvětlení problematiky je model klient-server zobrazen jako obrázek 1.

Obrázek 1 Struktura klient-serveru a peer-to-peer sítě



Zdroj: Pardeshi, 2021

Peer-to-peer sítě lze dělit do dvou kategorií: nestrukturované nebo strukturované. Nestrukturované P2P sítě nekladou důraz na dodržování struktury při překrývání sítě, jsou tvořeny uzly, které mezi sebou náhodně vytvářejí spojení. Ve strukturovaných P2P sítích je překrytí organizováno do specifických struktur a protokol zajišťuje, že jakýkoli uzel může v síti efektivně vyhledávat soubory nebo zdroje bez ohledu na to, zda je zdroj extrémně vzácný (Chowdhury, 2019, s. 12-14).

3.1.5 Blockchain

Bitcoin je nejdiskutovanější aplikací technologie blockchain. Tato technologie pomohla vyřešit problém dvojího utrácení, její využití však přesahuje Bitcoin. Tato technologie může být použita v množství případů a mnoho stávajících aplikací by fungovalo díky blockchainu lépe. Dle Chowdhuryho (2019, s. 8) může být blockchain definován jako neměnná distribuovaná účetní kniha zabezpečená kryptografickými technikami a spravovaná decentralizovanou komunitou přes peer-to-peer.

Blockchain funguje na P2P síti a vykazuje mnoho vlastností zděděných z této síťové architektury. Jako distribuovaný systém je blockchain umístěn na stovkách tisíc uzlů a sdílí své zdroje, takže neexistuje žádná závislost na jediném serveru nebo uzlu. Demonstruje také základní atributy distribuovaných systémů, jako je potřeba konsenzu při přijímání klíčových rozhodnutí, odolnost vůči chybám a další (Chowdhury, 2019, s.13-14). Jako decentralizovaný systém demonstruje, že žádný uzel nedává pokyn jinému uzlu, co má dělat. Pokud budou existovat uzly, které se nebudou řídit předem stanovenými pravidly, zabrání

jim v tom distribuovaná povaha blockchainu tím, že si vynucuje konsenzus prostřednictvím důkazu práce nebo jiných typů důkazů (Chowdhury, 2019, s. 14).

Neexistuje žádná centralizovaná oficiální kopie dat a žádnému uživateli se v této architektuře nedůvěřuje více než kterémukoli jinému. S blockchainem jsou transakce vysílány do sítě a zprávy jsou doručovány na základě maximálního úsilí. Po příchodu nových transakcí uzly validátoru, známé jako těžaři, ověří a přidají je do bloku, který vytvářejí, a poté vysílají dokončený blok do dalších uzlů. Tato operace pokračuje až do konce životního cyklu blockchainu výměnou za malé odměny pro uzly, které se účastní procesu ověřování neboli těžby (Chowdhury, 2019, s. 14).

3.1.6 Transakce

Transakce slouží k převodu bitcoinů mezi uživateli. Každá transakce obsahuje vstupy a výstupy, kdy vstupem jsou vlastněné bitcoiny, které mají být převedeny a výstupem jsou adresy a množství bitcoinů, které jsou převáděny (Lánský, 2018, s. 10). Transakce jsou rozepisovány po bitcoinové síti a shromažďovány do bloků. V bloku lze najít všechny transakce, které do něj byly zaznamenány. Všechny transakce jsou tak zpětně dohledatelné v blockchainu, který je dostupný všem uživatelům v síti (Chowdhury, 2019, s. 73-74).

Účelem transakce je tedy distribuovat jednotky kryptoměny z jednoho nebo více starých výstupů tím, že jsou použity jako vstup v nových transakcích (Chowdhury, 2019, s. 75). Výstup může být využit jako vstup maximálně jednou (Lánský, 2018, s. 10). Pokud uživatel chce poslat určitou částku jinému uživateli, např. 8 BTC, musí do vstupu této transakce zahrnout tolik výstupů starých transakcí, aby součet těchto výstupů byl větší než množství, které má být převedeno, tedy větší než 8 BTC. Poté odesílatel pošle požadované množství bitcoinů spolu s transakčním poplatkem a zbývající bitcoiny jsou odeslány zpět odesílateli. Tento zbytek je nazýván jako neutracený výstup transakce (UTXO) (Chowdhury, 2019, s. 75). Výše transakčního poplatku není pevně stanovena, ale nesmí být záporná. Výši transakčního poplatku určuje sám odesílatel, čím větší bude transakční poplatek, tím je větší šance, že bude transakce zpracována. Pokud by je poplatek velmi nízký, nemusí být zpracován nikdy. Aby transakce mohla proběhnout, musí majitel podepsat svým soukromým klíčem všechny transakční vstupy. Tím dává souhlas k převodu bitcoinů ve prospěch transakčních výstupů (Lánský, 2018, s. 10).

Dále ještě existuje speciální transakce, ke které nelze zpětně dohledat zdroj, z kterého byla vytvořena. Jelikož tato transakce je vždy vytvořena současně s novým blokem, je nazývána jako mincovorná (coinbase). Mincetvorná transakce je zaslána na adresu těžaře, který blok vytvořil, v kryptoměnovém světě je to bráno jako forma odměny pro těžaře. Množství jednotek kryptoměny v této transakci je určeno kryptoměnovým systémem. Původní odměna Bitcoinu byla 50 BTC za vytěžený blok, každých 210 tisíc bloků je tato hodnota snížena o polovinu, také nazýváno jako halving. To odpovídá přibližně 4 roků, než proběhne další snížení odměny. Tento proces bude opakován, dokud nebudou vytěženy všechny bitcoiny a odměna bude nulová (Chowdury, 2019, s. 65).

3.1.7 Blok

Jak bylo v předchozí kapitole zmíněno, blok obsahuje transakce. Počet transakcí, které může blok obsahovat je určen jeho velikostí. Maximální velikost bloku je jeden Megabajt (MB), aby bylo podpořeno rychlá distribuce a omezení odchylek (Chuen, 2015, s. 48). Hodnota transakčního poplatku je vydělena datovou velikostí transakce. Transakce s nejvyšší výslednou hodnotou bude poté zapsána do bloku. Velikost transakce je závislá na počtu vstupů a výstupů, je tedy obvyklé, že velké transakce musí mít větší transakční poplatek, aby mohly být zapsány do bloku. Jakmile je transakce zapsána do bloku, je považována za ověřenou (Lánský, 2018, s. 11).

Blok kromě transakcí obsahuje také blokovou hlavičku a hashový strom (Merkle tree). V hashovém stromu jsou ukládány transakce včetně i té mincovorné, hlavička slouží jako označení bloku. Hlavička je poté zašifrována hashovací funkcí, u bitcoinu to je funkcí SHA-256 (Chowdury, 2019, s. 67). Tato funkce z hlavičky vytvoří 256bitové číslo, nazývané jako haš hlavičky (Lánský, 2018, s. 11). Do haše hlavičky je také obsažen haš z předchozího bloku hlavičky, díky tomu je tvořen řetězec bloků neboli blockchain (Chowdury, 2019, s. 67).

3.1.8 Důkaz prací (Proof of work)

Bloky v kryptoměnách lze tvořit více způsoby, nejstarší kryptoměna Bitcoin využívá pro těžbu bloku důkaz práce (PoW). Cílem těžařů je za použití toho algoritmu nalézt vstup hashovací funkce, aby výsledek této funkce splňoval systémem dané omezení. Jelikož

výsledek hashovací funkce nelze předem předvídat, neexistuje lepší metoda než pokus a omyl (Lánský, 2018, s.23).

Pokud tedy má být vytvořen nový blok, nazývaný také jako kandidátský blok, je nejprve hlavička tohoto bloku zašifrována a výsledná hodnota haše musí být nižší než hodnota obtížnosti. Pokud haš hlavičky nesplňuje podmínku, musí být v hlavičce upravena hodnota nonce. Tento postup je opakován, dokud není splněna podmínka (Lánský, 2018, s.23-24). V momentu nalezení haše hlavičky, který je menší než hodnota obtížnosti, je blok sdílen v síti pro ověření ostatními. Jakmile je blok ověřen, je přidán do blockchainu a každý další blok musí navazovat na tento nově přidáný blok. V případě, že jsou dva bloky vytvořeny ve stejný moment, tvorba nových bloků se nezastavuje a potvrzen bude ten blok, na který bude navazovat další nově vytvořený blok, druhý blok se stane osiřelým (Chowdury, 2019, s. 83).

Obtížnost je stejně jako haš hlavičky 256bitové číslo, aby bylo možné je navzájem porovnat. Obecně je považováno za přijímaný fakt, že čím více nul obsahuje hodnota obtížnosti, tím se obtížnost zvyšuje. Měnící se výpočetní výkon v celé síti je hlavním důvodem, proč se obtížnost zvyšuje či snižuje. Nelze tedy ponechat konstantní hodnotu obtížnosti, jelikož větší výpočetní výkon znamená častější vytváření bloků, což způsobuje rozdíl mezi reálnou dobou těžení a formální dobou těžení. V případě Bitcoinu je po každých 2016 vytěžených bloků upravena obtížnost tak, aby průměrná doba těžby bloku odpovídala deseti minutám. V průměru je tedy obtížnost měněna každé dva týdny. (Lánský, 2018, s.24).

Těžař tedy k nalezení správného haše musí vynaložit velké úsilí v podobě spotřebované elektrické energie, aby mohl přidat svůj blok do blockchainu a dostat tak odměnu za vytěžený blok. Ověření nově přidávaného bloku je velmi jednoduché a nevyžaduje velký výpočetní výkon (Chowdury, 2019, s. 18).

3.1.9 Důkaz podílem (Proof of stake)

Přestože důkaz prací účinně odrazuje útočníky, bylo potřeba nalézt alternativní způsob k dosahování konsenzu, a to hlavně kvůli energetické náročnosti PoW. Jedním z pravděpodobně nejvíce používaných alternativních přístupů, jakým lze ověřovat nově přidávané bloky je důkaz podílem (PoS) (Chowdury, 2019, s. 19).

Důkaz podílem určuje, kdo bude mít právo přidat nový blok do blockchainu na základě počtu vlastněných jednotek kryptoměny. Pravděpodobnost, se kterou bude uživatel vybrán se zvyšuje s větším počtem vlastněných jednotek. Při tvorbě bloků se již nepoužívá výraz těžba bloku, nýbrž slévání bloku či ražení bloku. Slévání bloku neboli forging, se obvykle používá, pokud již nové jednotky kryptoměny nevznikají a ražení bloku (minting) je používáno u dalších kryptoměn, které implementují důkaz podílem (Lánský, 2018, s. 32).

Ražení nového bloku se od důkazu prací liší mnoha způsoby, např. místo porovnávání haše hlavičky s hodnotou obtížnosti se porovnává haš, který je tvořen z neutraceného výstupu transakce tvůrce bloku s hashem předchozího bloku a ten až porovnává s hodnotou obtížnosti. Obtížnost těžby je v tomto případě vypočítána jako násobek obecné obtížnosti těžby a specifického koeficientu pro danou adresu. Tento koeficient může zohledňovat různé faktory, jako je doba, po kterou byly jednotky kryptoměny drženy majitelem, nebo počet jednotek, které daná adresa vlastní. Dále PoS při tvorbě bloku neprovádí změnu nonce v bloku, takže výpočetní výkon uživatele zde nehraje žádnou roli (Lánský, 2018, s. 32).

Oproti PoW by se dal důkaz podílem považovat za zranitelnější vůči útokům. Některé kryptoměny se to pokoušejí eliminovat tak, že jednotky kryptoměny na dané adrese mohou být použity k vytvoření nového bloku pouze pokud nejsou na dané adrese déle, než je stanovená doba. I tak stále hrozí riziko, že bude vytvořen zcela nový řetězec od základního bloku, nebo také přepsání velkého úseku historie. Proto při využívání důkazu podílem bývá často pro zvýšení bezpečnosti použit i důkaz prací. (Lánský, 2018, s. 32-33).

3.2 Těžba kryptoměny

Těžba kryptoměn je metoda ověřování transakcí a přidávání záznamů do distribuované účetní knihy pro různé formy kryptoměn. Těžba se zvýšila, protože používání kryptoměn v posledních několika letech exponenciálně rostlo. Z těžby kryptoměn se stal prosperující průmysl, do kterého jsou vkládány obrovské investice a zahrnuje velké infrastruktury věnované jedinému úkolu – nalezení správné hodnoty haše (Chowdury, 2019, s. 219).

3.2.1 Hash rate

Haš je výstupem hashovací funkce. Schopnost generovat tyto haše rychle je pro těžaře považováno za nejdůležitější prvek při těžbě kryptoměny. Počet hashů, které je zařízení schopno provést za sekundu je uváděno jako hashrate. Pokud zařízení dosahuje výkonu 60 hashů za sekundu, znamená to, že mělo 60krát šanci nalézt správnou hodnotu pro sestavení bloku během jedné vteřiny. Jelikož se postupem času zvyšoval možný výkon těchto zařízení, začaly se u hashratu využívat stejné předpony jako u bajtů, tedy kilo-, mega – a další. Hashrate jednoho těžícího zařízení není konstantní pro všechny kryptoměny, jelikož každá kryptoměna využívá jiných algoritmů, což mění počet potřebných výpočetních operací k nalezení bloku (Chowdury, 2019, s. 222).

3.2.2 Evoluce těžby kryptoměny

Těžba kryptoměn je neustále se měnící proces, každých pár měsíců dojde v této oblasti k určitému vývoji. Všechno to začalo těžbou centrální procesorové jednotky (CPU) pomocí běžných stolních počítačů (Chowdury, 2019, s. 220), těžební výkon procesoru nebyl větší než 10 mega hashů za sekundu (MH/s) (Chuen, 2015, s. 54). Tento výkon byl během prvních dnů bitcoinu dostačující, brzy však těžaři přišli na to, že grafické karty jsou v hashování ještě výkonnější, proto se začali k těžení používat grafické procesory (GPU).

Těžení pomocí grafického procesoru bylo určitou dobu nejvýkonnější, dokud se nezačali používat programovatelné hradlové pole (FPGA), což jsou integrované obvody navržené tak, aby je bylo možné po výrobě nakonfigurovat podle potřeb zákazníka (Chowdury, 2019, s. 220). Výhodou těchto hradlových polí byla jejich schopnost pracovat s vysokými hashraty a zároveň s nízkou spotřebou energie (Chuen, 2015, s. 55).

Dny FPGA netrvaly dlouho, protože obtížnost těžby se zvyšovala a byl brzy nahrazen novou generací těžebních strojů ve formě integrovaných obvodů pro specifickou aplikaci neboli ASIC. Jedná se o specializované a účelové čipy určené pro hashování. Výrobci si rychle uvědomili, že z toho mohou sami profitovat, a tak začali budovat velké farmy určené k těžení, ve kterých bylo zaměstnáno větší množství těžařů. Někteří shromáždili těžaře po celém světě prostřednictvím cloudu, díky kterému můžou těžit bez vlastnění hardwaru pro těžbu. Vývoj těžby se tím nezastavil. Nebylo rentabilní těžit sám z domova v současném prostředí, hlavním důvodem byla spotřeba elektřiny a opotřebení počítače.

Koncept zvaný pool mining se stal trendem. Tento způsob spočívá v tom, že těžaři sdílejí svůj výpočetní výkon přes síť, aby vytvořili obří výpočetní platformu výhradně pro těžbu a později mezi ně pomocí různých metod rozdělili odměnu (Chowdury, 2019, s. 220).

3.2.3 Grafické karty (GPU)

Nejčastěji se pro těžbu pomocí grafických karet využívají tzv. těžařské rigy (mining rigs), na které je většinou umístěno od 6 do 12 grafických karet. Typický stolní počítač obvykle nabízí místo pro jednu nebo v některých případech i tři grafické karty. Těžařský rig, kromě již zmíněných GPU, obsahuje mnoho podobných komponentů jako má klasický stolní počítač, například základní desku, centrální procesor, operační paměť, napájecí zdroj, pevný disk, ventilátor a v neposlední řadě klávesnici, myš a monitor. Všechny tyto součásti jsou umístěny do speciálně upraveného rámu pro těžení kryptoměny. Ten na rozdíl od klasické PC skříně nabízí větší odvod tepla a dostatek prostoru pro umístění většího počtu grafických procesorů. Některé rámy nabízejí i možnost připojení dalšího rámu nebo namontování do racku počítačového serveru. Na obrázku 3 lze vidět vizuální příklad toho, jak vypadá těžební rig (Bain & Kent, 2022, s. 185-187).

Obrázek 2 Těžební rig



Zdroj: Joom, 2023

Základní deska je velmi důležitou součástí, která umožňuje zapojení všech součástí dohromady. Pro zapojení většího počtu grafických procesorů je potřeba základní deska

s větším počtem konektorů PCI-E, nebo redukční karta (Riser card), která umožňuje připojit grafické procesory k základní desce pomocí USB portu (Bain & Kent, 2022, s. 187-192).

Stěžejním bodem celé plošiny jsou grafické karty, které plní účel, ke kterému byla plošina vytvořena, tedy těžení kryptoměny. Je doporučeno, aby v jedné plošině byly využívány GPU stejného modelu, jelikož různé grafické karty mohou využívat jiné ovladače, což může vést k problému s kompatibilitou (Bain & Kent, 2022, s. 190).

Při těžbě kryptoměn využívajících archivní blockchain (kopii blockchainu, který uchovává všechna historická data), je potřeba pevný disk s několika terabajtovou pamětí. Pokud je těžební plošina využívána v poolu, není zapotřebí pevného disku s velkou pamětí, jelikož těžařovi stačí nainstalovat pouze operační systém, žádná další velká data nebude potřeba ukládat. Těžební plošina také nevyžaduje velkou operační paměť, obvykle je potřeba k provozu plošiny 4 GB až 16 GB operační paměti (Bain & Kent, 2022, s. 193-194).

I když GPU a centrální procesor jsou vybaveny vlastními ventilátory pro chlazení, bývají plošiny ještě vybaveny externími ventilátory, jelikož při dlouhodobém výkonu hrozí riziko přehřátí. To navyšuje spotřebu elektrické energie a musí být použito napájecí zařízení, které poskytne dostatečnou elektrickou energii pro všechny komponenty těžební plošiny (Bain & Kent, 2022, s. 193-194).

3.2.4 Programovatelná hradlová pole (FPGA)

FPGA je integrovaný obvod, který lze po výrobě přizpůsobit potřebám uživatelů. Pokud tedy chce těžař začít těžit jinou kryptoměnu, má možnost FPGA přeprogramovat. Těžaři bitcoinů využívali tyto čipy k podpoře těžby, protože mohou pracovat s vysokými hashraty s nízkou spotřebou energie. Těžba pomocí FPGA nějakou dobu dominovala na trhu pro svou snadnou implementaci a dnes je stále využívána, jen v mnohem menším měřítku. Poté však byla nahrazena ASIC zařízeními, jelikož je potřeba několik FPGA obvodů, aby se vyrovnaly výkonu ASIC.

3.2.5 ASIC (Application Specific Integrated Circuits)

ASIC je zařízení, které je sestaveno pro specifické účely, v tomto případě je vyráběno za účelem těžení kryptoměn. Oproti GPU je mnohem snazší na instalaci i použití. Aby bylo možné využívat více ASIC minerů najednou, jsou vyráběny regály umožňující umístění několika ASIC minerů vedle sebe, viz obrázek 3. Stejně jako stolní počítač potřebuje ASIC

miner napájecí zdroj. Dalším příslušenstvím je PDU, tedy jednotka pro distribuování elektřiny. Využívá se hlavně v regálech, ve kterých se nachází více ASIC minérů. Aby zařízení mohlo těžit kryptoměnu, musí být připojené k internetu. Tento problém je řešen pomocí ethernet portu, do kterého lze zapojit UTP kabel. Ovládat ASIC zařízení lze pomocí počítače, notebooku nebo chytrého telefonu, jedinou podmínkou je, aby zařízení bylo připojené na stejné LAN síti jako ASIC (Bain & Kent, 2022, s. 175-181).

Obrázek 3 Regál plný ASIC minérů těžících Bitcoin



Zdroj: Casey, 2021

Každý ASIC miner je určen pro těžbu pouze jednoho algoritmu, to značně omezuje počet kryptoměn, které je možné těžit (Tardi, 2022). Například Bitcoin Miner S19 XP Hyd od firmy Bitmain je určen pro algoritmus SHA-256, takže je schopen těžit kryptoměny jako je Bitcoin, BitcoinCash, Nicehash, Peercoin a LitecoinCash (Whattomine.com, 2023). Díky tomuto jednoznačnému zaměření dosahují lepších výkonů než těžení pomocí GPU, a to navíc při menší spotřebě elektrické energie (Tardi, 2022).

3.2.6 Sólo těžba (Solo mining)

Během let 2009 až 2011 byla velká šance vytěžit nový blok bitcoinu. Od té doby ale šance výrazně klesla, přesto se někteří těžaři stále rozhodují pro sólo těžbu a rozhodli se podstoupit větší riziko v souvislosti s nižší šancí na nalezení bloku. Tyto malé šance často kompenzují velkými investicemi do svého těžařského vybavení pro zvýšení hash ratu.

Těžba se stala nákladnou a komplikovanou, proto sólo těžba dnes není doporučovaná pro začínající těžaře. Aby těžaři mohli konkurovat, potřebují stále více těžebního zařízení, jehož cena výrazně stoupla. Dalším faktorem je hluk, který přístroje na těžbu produkují, proto je potřeba i více prostoru, a to nejen kvůli hluku, ale i kvůli potřebě chlazení. Proto se většina amatérských těžařů rozhodla připojovat do těžebních poolů (Bain & Kent, 2022, s. 79-80).

3.2.7 Těžba ve skupině (Pool mining)

Zvyšující se náročnost těžby dala podnět k vytváření těžebních poolů. Je to přístup k těžbě, kdy se na vytváření bloku podílí více těžařů a odměna za blok je rozdělena podle výpočetního výkonu, kterým přispěl každý člen v poolu (Chowdury, 2019, s. 225). To zajišťuje skupinovým těžařům pravidelné menší odměny za jejich vykonanou práci, místo jedné velké odměny za neurčitou dobu, někdy i několik desítek let při sólo těžbě (Lánský, 2018, s. 14). Každý pool se vyznačuje odlišnými vlastnostmi, jako je jeho velikost a systém odměn. Čím je pool větší, tím jsou výdělků konzistentnější a mají menší rozptyl od očekávaného zisku. Malé fondy se vyznačují větším rozptylem a méně častými většími platbami, ale pomáhají zmenšovat koncentraci hashovací síly. Pokud by totiž jeden pool vlastnil 51 procent výpočetní sítě, mohl významně poškodit síť kryptoměny tím, že by tvořil řetězec bloků rychleji, než by ho distribuoval a tím narušil decentralizaci a důvěryhodnost kryptoměny (Chuen, 2015, s. 58-63).

Je mnoho způsobů, kterými pool rozděluje odměny mezi své těžaře. Mezi nejčastější způsoby patří platba za podíl, úplná platba za podíl a platba za poslední počet podílů (Skorjanc, 2019). Platba za podíl (PPS) je způsob, kdy pool nabízí výplatu ze svého stávajícího zůstatku, která může být okamžitě vyplacena, aniž by musel klient čekat na vyřešení nebo potvrzení bloku (Chowdury, 2019, s. 228). Těžáři tak stačí předložit podíl o vykonané práci a následně dostane svou výplatu (Chuen, 2015, 2015, s. 60). Tato metoda přináší co nejmenší odchylku pro těžaře a zároveň přenáší veškeré riziko na provozovatele poolu (Chowdury, 2019, s. 228).

Úplná platba za podíl (FPPS) je přístup představený poolem BTC.com, jehož cílem je těžit z vysokých transakčních poplatků. Vypočítá standardní transakční poplatek ve stanoveném období, přidá jej do odměn za bloky a následně rozdělí celkovou částku těžařům

podle režimu platby za podíl. Tato metoda zachovává výhody PPS a pro těžaře je výhodnější, jelikož zahrnuje i výtěžky z transakčních poplatků (Chowdury, 2019, s. 228).

Platba za poslední počet podílů (PPLNS) je systém, odměňuje těžaře pouze v případě, že pool nalezne blok. Pool vypočítá výplatu pro těžaře tak, že se „vrátí v čase“ a zkontroluje platné podíly, které podíleli na vytěžení bloku. Tento časový úsek je nazýván časovým oknem. Výplata těžařů tak odpovídá podílům, které odeslali v daném časovém okně. Těžaři se tak nevyplatí měnit pool, pokud se odpojí dříve, než bude blok nalezen (Skorjanc, 2019).

3.3 Uhlíková stopa kryptoměn

Eckley (2022) definuje uhlíkovou stopu jako množství emisí oxidu uhličitého (CO₂) spojených se všemi činnostmi vykonávané osobami nebo jinými subjekty (např. budovy, korporace, země atd.). Emise lze rozdělit do tří kategorií, a to na přímé emise z činností, produktů a procesů, na nepřímé emise energie (nakoupené vytápění a elektřina) a na kategorii zahrnující jakékoli další nepřímé emise). Koncept uhlíkové stopy nezahrnuje pouze emise oxidu uhličitého, ale také emise dalších skleníkových plynů, jako je metan, oxid dusný nebo chlorfluoruhlodíky (Geneidy a spol. 2021).

Koncepce uhlíkové stopy souvisí se starší myšlenkou ekologické stopy, ze které se vyvinula a která říká, že ekologická stopa je celková plocha půdy potřebná k udržení činnosti nebo populace. Naproti tomu uhlíková stopa se obvykle vyjadřuje jako míra hmotnosti, například v tunách CO₂ nebo ekvivalentu CO₂ za rok (Eckley, 2022).

V minulém století došlo k nárůstu úrovně atmosférických skleníkových plynů (GHG) na téměř 584 gigatun CO₂ z fosilních paliv. Od roku 1960 do roku 2020 se množství oxidu uhličitého v ovzduší zvýšilo z 250 ppm (částic z milionu) na 400 ppm a současné trendy ukazují nárůst přírodních katastrof způsobených vysokými teplotami a obdobími sucha (Sharma a spol.). Vzhledem k distribuované síti kryptoměn je obtížné získat informace o tom, jaká těžební zařízení jsou používána k těžbě a také přesný podíl obnovitelných a neobnovitelných zdrojů energie. Zatímco některé studie tvrdí, že hlavním zdrojem energie pro kryptoměny jsou obnovitelné zdroje s téměř 80% podílem, 3. GCBS ukazuje 61% závislost na neobnovitelných zdrojích energie. Statistiky těžby kryptoměn v Číně ukazují, že podle nedávné studie je rozdělení výroby energie na 58 % z vodní energie a 42 % výroby

elektřiny z těžkého uhlí. Výzkum odhadl emisní faktor pro Čínu na 550 g/kWh s ohledem na vážený průměr provincií S'-čchuan a Vnitřní Mongolsko bohatých na vodu a uhlí. Vezmeme-li v úvahu, že přibližně 46 % hash ratu Bitcoinové sítě se nachází v Číně a předpověď 130 megatun CO₂ bitcoinové sítě do roku 2021 jen v Číně, spolu s pokračujícím využíváním fosilních paliv, existuje skutečná hrozba pro životní prostředí, což učiní očekávaný nárůst o 2 °C, kterým přispěje Bitcoin během několika příštích desetiletí (Kohli a kol., 2022). Stránka ccaf.io odhaduje spotřebu Bitcoinu na 118 Twh za rok. Pro srovnání Nizozemsko spotřebuje 113 Twh ročně a Argentina 126 Twh. Samotné emise Bitcoinu jsou považovány jako hrozba pro zmírnění emisí skleníkových plynů, aby byla splněna Pařížská dohoda (Wendl a spol., 2023).

4 Praktická část práce

V této části práce bude prováděn rozbor čtyř kryptoměn, které využívají důkaz prací. U každé kryptoměny budou uvedeny krátké základní údaje a poté bude vytvořen seznam všech položek, které bude potřeba pořídit pro těžbu kryptoměny. Dalším bodem bude výpočet potencionálního výdělku a velikosti uhlíkové stopy, na závěr bude u každé kryptoměny shrnutí a doporučení. Kryptoměny jsou vybrány na základě největšího tržního kapitálu ke dni 21.2. 2023. Dle stránky coinmarketcap.com jsou čtyřmi největšími kryptoměnami využívající PoW Bitcoin, Dogecoin, Litecoin a Ethereum classic. Vybrány jsou kryptoměny využívající důkaz prací, jelikož ten způsobuje velkou spotřebu elektřiny při těžbě. Aby bylo zajištěno zkoumání za stejných podmínek, je stanoveno, že celková cena nákladů nepřesáhne 1 milion korun českých. Doba těžby bude stanovena na základě toho, za jak dlouho se bude měnit obtížnost Bitcoinu, jelikož ten má největší tržní kapitál. Dále bude provozována sólo těžba, a to z toho důvodu, že získat přístup k informacím o tom, jak daný pool dělí zisk mezi těžaře je bez aktivního podílení se na těžbě nemožné. Z důvodu, že se celkový výkon sítě neustále mění a nelze ho předvídat, bude použita jeho průměrná hodnota.

4.1 Postup při analýze

V první části analýzy je cílem zjistit hodnotu nákladů, které těžba kryptoměny obnáší. Nejprve je nalezeno vhodné těžební zařízení, které dosahuje nejlepších výsledků v poměru hash rate na spotřebovanou elektřinu. Poté je zjištěna cena dalších nezbytných prostředků k tomu, aby bylo možné využívat těžební zařízení k těžbě dané kryptoměny. Na základě celkového příkonu, který budou nakoupená zařízení vytvářet, bude vypočítána spotřeba elektřiny. Suma všech uvedených položek vyčíslí částku, která bude potřebná pro provozování těžby dané kryptoměny.

V další části bude spočítán potencionální výdělek, který s vybraným zařízením bude možné dosáhnout. Pro zjištění výdělku je potřeba znát obtížnost sítě, celkový hash rate sítě, hash rate využívaného těžebního zařízení, cenu elektřiny, cenu za jednotku kryptoměny a kolik jednotek kryptoměny je získáno při vytěžení bloku. Jelikož se všechny tyto hodnoty v průběhu dne neustále mění, budou použita historická data získaná z internetových stránek v časovém úseku od 7.2. 2023 do 20.2. 2023, a ty budou následně zprůměrovány. Ze stránky coinmarketcap.com bude vybrána nejnižší a nejvyšší cena, které kryptoměna dosahovala

v daný den. Z těchto hodnot bude spočítána průměrná nejnižší a nejvyšší cena za 14 dní, po zprůměrování nejnižší a nejvyšší ceny bude známa průměrná cena za jednotku. Dále stránka minerstat.com uvádí průměrný hash rate a obtížnost za daný den. Aby bylo dosaženo jedné konstantní hodnoty, bude uváděn průměr hodnot, bude pomocí vzorce:

$$T = \frac{D \times 2^{32}}{V}, \quad (1)$$

kde

T je čas na spočítání bloku v sekundách;

D je obtížnost sítě;

V je výpočetní výkon (hash rate) v hashích za sekundu.

Vypočítán čas na vytěžení jednoho bloku. Nejprve bude spočítán čas s hash ratem kryptoměnové sítě a poté čas s hash ratem nakoupeného těžebního zařízení. Na základě těchto dvou získaných časů bude spočítána šance na vytěžení bloku pomocí nakoupeného těžebního zařízení. Šanci na vytěžení lze definovat jako následující vztah:

$$X = \frac{T_s}{T_x}, \quad (2)$$

kde

T_s je čas sítě na spočítání bloku;

T_x je čas těžebního zařízení na spočítání bloku;

X je část bloku, které těžební zařízení dokáže spočítat.

Šance bude poté vynásobena počtem bloků, který bude za dobu provozované těžby vytěžen. Tím bude získán přibližný odhad, jak velká bude šance najít blok s vybraným těžebním zařízením. Aby bylo možné zjistit velikost finanční obnosu při vytěžení bloku, bude použita již zmíněná průměrná cena za jednotku kryptoměny, která bude vynásobena odměnou za blok, bez transakčních poplatků. Rozdíl tohoto finančního obnosu a cena spotřebované elektřiny bude určovat, zda byla těžba zisková, či ztrátová.

Dále bude vypočítáno, jak velká uhlíková byla při těžbě vytvořena. Stránka ourworldindata.org uvádí, kolik gramů oxidu uhličitého vytvoří jedna kW hodina při spotřebování elektřiny v ČR, vynásobením tohoto počtu gramů CO₂ se spotřebovanou elektřinou je získána výsledná uhlíková stopa, která byla při těžbě způsobena.

V poslední části analýzy budou zhodnoceny všechny výsledky, ke kterým bylo dospěno. V této části budou také zmíněny různé poznatky či doporučení autora související problematikou těžby. Na závěr této kapitoly bude uveden autorův osobní názor na to, zda by těžbu konkrétních kryptoměn doporučil.

4.2 Bitcoin

Bitcoin jakožto nejstarší kryptoměna stále dosahuje nejvyšší ceny na trhu za jednu jednotku, a to i navzdory tomu, že je jeho cena velice proměnlivá, během dne lze pozorovat změny až o tisíce amerických dolarů. Průměrná cena za jeden Bitcoin je tedy 23 075,12 USD, to odpovídá přibližně 511 446,17 Kč. Ke dni 21.2. 2023 je již vytěženo přibližně 92 % jednotek Bitcoinu, které mohou být v oběhu. Odměna za blok už byla celkem třikrát snížena, a to přesně o polovinu, to se děje přibližně každé 4 roky, nyní je odměna 6,25 BTC. Obtížnost těžby Bitcoinu se mění každých 2016 bloků, ke dni 21.2. 2023 je aktuální obtížnost 39 156 400 059 293, s průměrným hash ratem 308,09 EH/s může být předpokládáno, že další změna nastane za 12 dní a 17 hodin. Proto bude těžba provozována po tuto dobu, aby byla simulována těžba za aktuální obtížnosti (Whattomine, 2020; Minerstat, 2023).

4.2.1 Výpočet nákladů pro těžbu

Největší podíl nákladu při těžbě kryptoměny bude tvořit cena těžebního zařízení, proto je vybráno takové zařízení, které bude dosahovat vysokého výkonu při co nejmenší spotřebě. Největší podíl nákladu při těžbě kryptoměny bude tvořit cena těžebního zařízení, proto je vybráno takové zařízení, které bude dosahovat vysokého výpočetního výkonu při co nejmenší spotřebě elektrické energie. Byla prozkoumána nabídka zařízení pro těžbu pomocí algoritmu SHA-256, který využívá Bitcoin. Zařízení byly řazena podle poměru výpočetního výkonu v jednotkách Terahashů za sekundu na spotřebované Watty za hodinu. Nejlepších výsledků dosahoval Antminer S 19 XP od firmy Bitmain. Dalším faktorem, který ovlivní náklady, bude příslušenství a ostatní prostředky, potřebné k provozu Antminer S 19 XP. Jelikož je pozornost věnována hlavně nákladům přímo k těžebnímu zařízení, nebude zahrnuta cena prostor, ve které bude těžba provozována a nebude ani zahrnuta cena zařízení, kterým bude těžba ovládána. Všechny prostředky potřebné k těžbě jsou shrnuty níže, v tabulce 1.

Tabulka 1 Seznam nakoupených prostředků pro těžbu Bitcoinu

Název položky	Cena za kus (Kč)	Počet kusů	Celková cena (Kč)
Antminer S 19 XP	143 758	6	862 548
Třífázový jistič 32 A	552	1	552
Jednopolový jistič 16 A	85	7	595
Instalační vypínač 32 A	530	1	530
Proudový chránič 40 A	1462	1	1462
24 modulová rozvodnice	1149	1	1149
Propojovací lišta	783	1	783
Kabely CYKY (1,5 mm)	21	14	294
Dvozásuvka	119	7	833
UTP kabel (2 m)	25	7	175
Regál pro ASIC zařízení	775	1	775
Napájecí kabel 10 A	129	12	1 548
Přepínač 8 port	269	1	269

Zdroj: Vlastní zpracování, KVeлектро, CZC, hornbach, bitmain

Aby bylo možné zapojit nakoupené těžební zařízení, je potřeba zajistit dostatečně silnou elektrickou síť. Výrobce uvádí, že příkon Antmineru S 19 XP se pohybuje v průměru 3030 W. To znamená, že celkový příkon bude 18 180 W a požadovaný elektrický proud bude přibližně 76 ampérů. Je tedy třeba nainstalovat 32 ampérový třífázový jistič, který poskytne dostatečný proud. Dále bude proud distribuován z třífázového jističe jednopólovými jističi do zásuvky pomocí kabelů CYKY. Jističe budou vzájemně propojeny propojovací lištou. Pro jeden Antminer S 19 XP je potřeba dvou 10 ampérových napájecích kabelů. Proudový chránič slouží k ochraně při porušení obvodu a hlavní vypínač pro možnost vypnout přívod elektrického proudu.

Suma všech položek v tabulce 1 je rovna 871 513 Kč. Do celkových nákladů potřebných pro započítání těžby je třeba ještě zahrnout cenu připojení k elektrické síti, která bude činit přibližně 20 160 Kč (egd.cz) a internetové připojení v hodnotě 299 Kč na měsíc, po přičtení těchto dodatečných hodnot budou vstupní náklady pro těžbu přibližně 891 972 Kč.

Elektrina spotřebovaná při těžbě je dalším faktorem, který je potřeba zahrnout do nákladů. Největší část spotřebované energie bude tvořit hlavně těžba pomocí ASIC zařízení, výrobce uvádí průměrnou spotřebu 3010 W za hodinu. Celková spotřeba elektriny tedy bude přibližně 18 060 W za hodinu. Pokud bude těžba provozována 12 dní a 17 hodin, bude za tuto dobu spotřebováno 5 544,9 kWh. Při ceně 3,89 Kč za kWh pro domácnosti v České

republice (kurzy.cz), zvýší to náklady o 21 619 Kč. bude těžba která byla nalezena který bude spotřebována při těžbě. Náklady na pořízení vybavení a na samotný provoz těžby budou dosahovat až 915 788 korun českých.

4.2.2 Potencionální výdělek

Nyní bude zjištěno, jaká šance s výše uvedeným vybavením je na vytěžení Bitcoinu. Výpočetní výkon ASIC minérů bude dosahovat 840 TH/s. Průměrná obtížnost Bitcoinu je aktuálně 39 156 400 059 293. Jak dlouho zabere vybranému vybavení spočítání jednoho bloku bude vypočítáno pomocí vzorce 1 pro výpočet času na jeden blok.

Dosažením do vzorce je čas roven 200 208 878 vteřinám. Stejný vzorec byl použit pro zjištění, jak dlouho trvá celé Bitcoinové síti s hash ratem 308 094 357,1 TH/s. Bitcoinové síti zabere výpočet jednoho bloku 9 minut a 5 sekund. Po vydělení času na blok zvoleným zařízením a času Bitcoinové sítě, je získána hodnota 0,00027264 %, která uvádí, jakou část bloku stihne nakoupené zařízení spočítat. Šance na vytěžení se bude zvyšovat, čím déle bude těžba provozována, po 12 dnech a 17 hodinách by tedy šance na vytěžení Bitcoinu byla 0,54965 %.

Cena 1 BTC za posledních 14 dní se v průměru pohybovala kolem 511 146 Kč. Aktuální odměna za vytěžení bloku je 6,25 BTC, potencionální „výhra“ je tedy 3 196 538 CZK, to je 3,5krát větší finanční obnos, než který byl potřeba investovat.

4.2.3 Uhlíková stopa

Dosažený výpočetní výkon 840 TH/s spotřebovává 18 180 W za hodinu, která je odebírána z elektrické sítě, v tomto případě elektrické sítě v České republice, dle stránky ourworldindata.org za rok 2022 byly emise při spotřebě elektřiny 415 gramů oxidu uhličitého na 1 kilowatt hodinu. Odhadovaná těžba Bitcoinu po dobu 12 dní a 17 hodin by tudíž emitovala 2 535,02 Kg oxidu uhličitého.

4.2.4 Zhodnocení a doporučení

Výsledky ukazují velmi malou šanci na vytěžení Bitcoinu při sólo těžbě, pokud bude brán v potaz kapitál, který je potřebný pro započítání těžby s takovou to šancí, není dle mého názoru doporučeno v takových to podmínkách s těžbou začínat. Aby bylo možné vůbec obstát

v tomto kompetitivním prostředí a vytěžit Bitcoin, bylo by nutné zvýšit výpočetní výkon a minimalizovat elektřinu spotřebovanou k těžbě. V tomto případě by to však vedlo k značnému zvýšení nákladů za spotřebovanou elektřinu a také mnohem větší vstupní náklady. Pokud by se obtížnost nezměnila následujících 365 dní a ostatní podmínky by zůstaly stejné, hodnota spotřebované elektřiny by dosahovala 616 629,75 Kč. Šance na vytěžení by se tím také zvedla, až na necelých 15,75 %, ale stále to nezajišťuje zaručený úspěch. Navíc nelze predikovat, zda se nezvýší celkový hash rate sítě, který nejvíce ovlivní šanci na vytěžení Bitcoinu. Také velkou roli hraje stát, ve kterém těžíme, pokud bychom provozovali těžbu např. v Číně, v přepočtu na českou měnu by byla cena za kWh 1,751 CZK (globalpetrolprices.com). To by významně snížilo náklady na těžbu a bylo by možné těžit delší dobu s šancí na větší výdělek. Výhodou Bitcoinu je vysoká peněžní hodnota, která by byla získána při jeho vytěžení, jelikož tato hodnota dosahuje až 3 196 538 Kč, tudíž pokud by cena za spotřebu elektřiny byla 3 miliony korun českých a opravdu by se podařilo vytěžit blok Bitcoinu, stále by bylo profitováno 196 538 Kč.

Vhodným řešením, jak ušetřit za náklady spojené s elektrickou energií a jak snížit uhlíkovou stopu by také bylo těžit kryptoměnu za využívání obnovitelných zdrojů, např. solární či větrnou energií. Další možností je využít odpadní teplo, které produkují těžební zařízení. Pokud by se dalo efektivně vytápět těžbou kryptoměny, bylo by možné snížit uhlíkovou stopu tím, že by nebyl používán plynový či uhelný kotel k vytápění obytných zařízení nebo ohřevu vody.

4.3 Dogecoin (DOGE)

Kryptoměna je pojmenována po velmi populárním internetovém vtípku, ve kterém je název „Doge“ přiřazen k plemenu psa Shiba inu. Fotka, která je s tímto vtípem spojována, je zobrazena i v logu této kryptoměny, viz obrázek 4. Samotný autor uvedl, že Dogecoin byl vytvořen s hlavním účelem pro pobavení kryptoměnové komunity. Dogecoin vznikl v roce 2013 odvozením od Litecoinu a funguje na stejných principech jako Bitcoin, na peer-to-peer

síť a s open-source zdrojovým kódem. Jelikož byl Litecoin odvozen z Bitcoinu. Dogecoin je decentralizovaný, využívá technologii blockchain a algoritmus Scrypt (Dogecoin, 2023).

Obrázek 4 Logo Dogecoinu



Zdroj: Wikipedia, 2023

Dogecoin nelimituje počet tokenů v oběhu, takže ho lze neustále těžit. Průměrná obtížnost je 10 870 733 a průměrný hash rate síť dosahuje 731,97 TH/s. Za každý vytěžený blok je odměna 10 tisíc DOGE, průměrný čas na vytěžení bloku je 1 minuta a 3 sekundy (whattomine.com). Je tedy jasné, že s neomezenou zásobou Dogecoinů, kterou lze neustále těžit nebude cena tak vysoká jako u Bitcoinu. Cena bude stanovena stejně jako v předchozí kapitole u Bitcoinu, zprůměrováním za posledních 14 dní, jeden DOGE tedy vychází na 1,9069 Kč. Momentálně je v oběhu 132,6 miliard Dogecoinů a hodnota tržního kapitálu činí necelých 11,5 miliard USD (Minerstat, 2023).

4.3.1 Výpočet nákladů pro těžbu

Pro těžbu je vybíráno ASIC zařízení operující na algoritmu Scrypt. Nejvhodnějším kandidátem je Litecoin Miner L7 od firmy Bitmain, který dosahuje nejlepších výsledků v efektivitě těžby. Koupě tohoto zařízení přímo od výrobce by vyšla v přepočtu českou měnu na 193 939 Kč. Litecoin Miner L7 dosahuje výkonu 8 800 MH/s při spotřebě 3 168 W. Aby rozpočet na těžbu kryptoměny nepřekročil milion korun českých, bude těžba provozována pouze se 4 kusy ASIC zařízení, jelikož další prostředky potřebné k těžbě by překročily tuto hranici rozpočtu. Jelikož celkový příkon těchto 4 zařízení se bude pohybovat kolem 12 672 W a výrobce uvádí, že napětí těchto zařízení se pohybuje mezi 200 až 240 V, je potřeba třířázkový jistič s 25 A. Pro ochranu při narušení celého obvodu, se použije 25 A Proudový chránič, k tomu i Instalační vypínač o stejných ampérech, aby mohl být

přívod elektřiny ovládn. Z jednopólových jističů o 16 A, bude elektřina pomocí kabelů CYKY vedena do zásuvek s dvěma zdírkami. Všechna ASIC zařízení bude pak možné připojit k tomuto obvodu přes dvojici napájecích kabelů, jelikož jeden Litecoin Miner L7 obsahuje dva napájecí zdroje. Pro 4 Litecoin Minery L7 je dostačující regál s dvěma policemi, na spodní polici lze umístit všechny 4 minery vedle sebe a lze nechávat mezi nimi mezery, pro lepší cirkulaci vzduchu a na horní polici lze umístit router a switch pro připojení ASIC zařízení k internetu přes UTP kabely. Zbylý prostor na horní polici lze využít pro umístění notebooku, aby mohl být ASIC rig ovládn přímo na místě. Ceny všech výše uvedených položek jsou shrnuty v tabulce 2.

Tabulka 2 Seznam nakoupených prostředků pro těžbu Dogecoinu

Název položky	Cena za kus (Kč)	Počet kusů	Celková cena (Kč)
Litecoin Miner L7	193 939	4	775 754
Třífázový jistič 25 A	433	1	433
Jednopólový jistič 16 A	85	5	425
Instalační vypínač 25 A	564	1	564
Proudový chránič 25 A	934	1	934
24 modulová rozvodnice	1 149	1	1 149
Propojovací lišta	783	1	783
Kabely CYKY (1,5mm)	21	10	210
Dvoj zásuvka	119	5	595
UTP kabel (2 m)	25	5	125
Regál pro ASIC zařízení	775	1	775
Napájecí kabel 10 A	129	8	1 032
Přepínač (5 port)	219	1	219

Zdroj: Vlastní zpracování, KVeлектро, CZC, hornbach, bitmain

Poslední náklady, které ještě zbývá zahrnout je cena internetu, zapojení našeho jističe k elektrické síti a následná těžba Dogecoinu po dobu 12 dní a 17 hodin. Po prozkoumání nabídky internetového připojení na trhu, byla nalezena výhodná nabídka, kdy za 299 Kč měsíčně dostaneme rychlost 100 Mb/s a router od společnosti nej.cz. Na stránce egd.cz lze nalézt jakou cenu máme očekávat za připojení k elektrické síti na základě požadovaného příkonu, v případě třífázového jističe s hodnotou 25 ampér to činí 15 750 Kč. Za 12 dní a 17 hodin spotřebujeme jen za těžbu 4 435 kWh elektřiny, budeme-li brát v úvahu stejnou cenu elektřiny jako při těžbě Bitcoinu (3,899 Kč/kWh), navýší to náklady 15 069,85 Kč. Sečtením všech uvedených cen, dostaneme sumu 813 870 Kč.

4.3.2 Potencionální výdělek

Dogecoin upravuje obtížnost po každém vytěženém bloku, tak aby čas na blok (block time) odpovídal jedné minutě. Je tedy velmi obtížné určit šanci, s kterou lze tuto kryptoměnu těžit. Proto budeme používat průměrnou obtížnost za posledních 14 dní, k tomu také průměrný hash rate sítě za posledních 14 dní. Se čtyřmi Litecoin minery L7 bude jejich celkový výpočetní výkon kolem 35 200 MH/s. Pro výpočet bude použit stejný postup jako při počítání šance na vytěžení Bitcoinu.

Nejprve je potřeba převést výpočetní výkon na pouhé hashe za sekundu, 35 200 bude vynásobeno 10^6 , průměrná obtížnost je 10 870 733. Dosazením hodnot do vzorce 1 pro výpočet obtížnosti je získán potřebný čas, který potřebuje těžební zařízení na vypočtení jednoho bloku. Ten se rovná 13 26 404 vteřin, pro lepší představu lze převést na 368,4 hodin. Použití stejné rovnice lze spočítat i čas celé sítě na jeden blok, jelikož hash rate sítě je 731,96613 TH/s, vynásobením 10^{12} a dosazením do rovnice i s obtížností se výsledná hodnota rovná 63,786 vteřinám.

Dále je potřeba spočítat šanci na vytěžení bloku, dosazením do vzorce 1, je získána hodnota 0,00004809, to se rovná 0,004809 %. To znamená, že za 63,79 vteřin spočítá vybrané těžební zařízení 0,004809 % bloku. Doba těžby bude trvat 12 dní a 17 hodin, to znamená, že za tuto dobu se vytěží přibližně 17 213krát. Pokud máme šanci 0,004809 % a 17 213 pokusů vytěžit blok, máme asi 82,78% šanci na vytěžení bloku. Jak bylo již zmíněno, odměna za blok je 10 000 dogecoinů, převedením na českou měnu a zaokrouhlením na dvě desetinná místa se dostáváme na potencionální výdělek v hodnotě 19 069,85 korun českých. Pokud by byly ignorovány náklady za nakoupené zařízení k těžbě a byla by odečtena pouze spotřebovaná elektřina, je velmi velká šance, že bude získán výdělek v hodnotě 4 000,75 Kč.

4.3.3 Uhlíková stopa

Jelikož při těžbě Dogecoinu byly použity pouze čtyři ASIC zařízení, které mají obdobný příkon jako ASIC zařízení použitá pro těžbu Bitcoinu, lze očekávat, že uhlíková stopa Dogecoinu bude menší. Použita budou stejná data pro změření uhlíkové stopy, což je 415 gramů na jeden kWh elektřiny, za dobu 12 dní a 17 hodin. Výsledkem je 1 603,958 kilogramů oxidu uhličitého, který byl vytvořen při těžbě Dogecoinu.

4.3.4 Zhodnocení a doporučení

Velkou výhodou Dogecoinu je, že při vytěžení bloku získáme této kryptoměny velké množství. V našem případě se šance na vytěžení pohybuje na velmi vysoké úrovni, a to na 91 %. Oproti Bitcoinu má Dogecoin výhodu v tom, že počet mincí, který dostane za vytěžení, je mnohonásobně vyšší. Další výhodou je častější přidávání bloků, tudíž za stejný časový úsek má každý těžař Dogecoinu 10krát větší šanci, že najde blok. Dle mého názoru, je ideálnější těžit tuto kryptoměnu s menší hash ratem při malé spotřebě elektřiny po co nejdéle dobu. Stále zde ale hraje roli proměnná v podobě celkového hash ratu sítě, která může negativně ovlivnit naši šanci na vytěžení. Jako hlavní nevýhodu považuji nízkou tržní cenu Dogecoinu, pokud bude bráno v potaz, že je třeba 798 801 Kč pro nakoupení příslušenství pro těžbu Dogecoinu a po 14 dnech těžby je dosaženo skoro 91 % šance na výdělek 4 000,75 Kč. Může být uvažováno, že během 12 dní a 17 hodin se podaří vytěžit dva bloky, tudíž se výdělek zdvojnásobí.

Opět se zde vyskytuje problém poměrně vysoké ceny elektřiny, která zapříčiňuje malý výdělek z těžby. Možným řešením by bylo těžit pouze pomocí dvou ASIC minérů Litecoin Miner L7 a ušetřené peníze využít k nainstalování solárních panelů, či jiného obnovitelného zdroje pro vyrábění elektrické energie, tím by se dalo těžit dlouhodobě za nízkých nákladů za spotřebu elektřiny.

4.4 Litecoin (LTC)

Litecoin si za svůj cíl klade, aby poskytoval bezpečné platby za nízké ceny, s využitím jedinečných vlastností blockchainu. Způsob, jakým udržuje nízké ceny jsou malé transakční poplatky, jeho hlavní využití je právě při mikrotransakcích. Jak bylo již zmíněno u Dogecoinu, Litecoin vychází z Bitcoinu, tudíž mají mnoho podobných vlastností, např. obtížnost se mění po 2016 blocích a bloky se přidávají pomocí důkazu práce. Oproti Bitcoinu má 4krát menší čas na blok, v průměru 2,5 minuty a jeho maximální počet v oběhu je zastropován až na 84 milionů jednotek, což je 4krát více než je tomu u Bitcoinu. Momentálně je již 86 % z tohoto celkového objemu vytěženo a odměna za blok je 12,5 LTC. Každých 840,000 bloků se tato hodnota odměny sníží přesně o polovinu, a to až do té doby, dokud je vytěžen maximální počet jednotek. Litecoin funguje na stejném algoritmu jako Dogecoin, na Scryptu (Litecoin, 2023).

4.4.1 Výpočet nákladů pro těžbu

Jelikož Litecoin a Dogecoin lze těžit pomocí stejných zařízení, budou použity stejné prostředky a náklady na těžbu jako u Dogecoinu uvedené v kapitole 4.3.1. Tudíž jsou již známy celkové náklady a stačí pouze vyčíslit potencionální zisk z těžby Litecoinu. Suma vstupních nákladů tedy činí 813 870 Kč, z toho 15 069,85 Kč tvoří spotřeba elektřiny při těžbě za 12 dní a 17 hodin (305 hodin).

4.4.2 Potencionální výdělek

Průměrná cena za 1 LTC v přepočtu na českou měnu činí 2 145 Kč. Jelikož je použito stejných prostředků jako při těžbě Dogecoinu, je již znám výpočetní výkon, který dosahuje 35 200 MH/s. Dále použijeme vzorec pro výpočet času na vytěžení bloku. Při výpočetním výkonu sítě 686,40 TH/s je průměrný čas na blok 2 minuty a 24 sekund. Čas vybraného těžebního zařízení při hash ratu 35 200 MH/s je 781,41 hodin na jeden blok. Po převedení času na sekundy a vydělením s časem sítě lze uvažovat s tím, že za dobu, kdy stihne síť vytěžit blok, stihne vybrané těžební zařízení spočítat 0,005128 % tohoto samého bloku. Může být předpokládáno, že za celou dobu těžby bude vytěženo přibližně 7 611 bloků, tudíž šance na vytěžení se tím zvyšuje o počet těchto bloků. Tím lze po 12 dnech a 17 hodinách těžení očekávat 39,03% šanci na nalezení bloku v hodnotě 26 817,44 Kč. To by znamenalo výdělek v hodnotě 10 216,31 Kč.

4.4.3 Uhlíková stopa

Uhlíková stopa způsobená těžbou Litecoinu bude stejně velká jako při těžbě Dogecoinu, která je popsána v kapitole 4.3.3. Hodnota oxidu uhličitého, která bude emitována do ovzduší činí 1 603,958 kg.

4.4.4 Zhodnocení a doporučení

Z výsledků je zřejmé, že je možné si vybrat, zda bude těžen Litecoin s menší šancí na vytěžení, konkrétně s šancí 39,03 %, ale za to s vyšším výdělkem při úspěšném vytěžení, který by činil 10 216,31 Kč. Další možností je těžit Dogecoin s větší jistotou výdělku, jelikož se zde vyskytuje 82,78% šance na vytěžení, ale při menší finanční hodnotě, a to 4 000,38 Kč. Z tohoto důvodu může být doporučeno začít těžit Litecoin, pokud je disponováno větším

hash ratem, jelikož by se šance na vytěžení Litecoinu zvýšila, a naopak při malém výpočetním výkonu těžit pouze Dogecoin.

Jelikož byla použita stejná těžební sestava, lze to považovat jako alternativní možnost, jak při poklesu ceny jedné kryptoměny lze přejít v krátkém čase na těžbu druhé kryptoměny. Tím zde může vznikat větší jistota, že bude těžena výhodná kryptoměna.

Je zde na místě zvážit, zda by těžba Litecoinu nebyla výhodnější v těžařském poolu. Jelikož při těžbě v poolu je těžké odhadovat výdělky, bylo by vhodné otestovat, zda by se tato těžba v poolu ukázala jako výhodnější než samostatná těžba Dogecoinu. Na základě výsledků by pak byla zvolena výhodnější alternativa.

4.5 Ethereum classic (ETC)

Jak je již možné z názvu této kryptoměny poznat, tato kryptoměna je odvozená od Etherea, které sice funguje na systému důkazu podílem, ale protože tvůrci Etherea classic chtěli, aby se tato nová verze kryptoměny od Etherea co nejvíce lišila, je Ethereum classic velmi modifikováno. Hlavním rozdílem je využívání systému důkazu prací a přechod na algoritmus ETChash (Ethereumclassic, 2023).

Průměrná cena Etherea classic, po převedení na českou měnu, dosahuje hodnoty 484,61 Kč. Odměna za blok je snižována po 5 milionech vytěžených blocích o 20 % a ke dni 21.2. 2023 je odměna za blok 2,48 ETC. Vytěžení jednoho bloku by tedy znamenalo výdělek v hodnotě 1 201,83 Kč. Průměrný hash rate je 125,52 TH/s při obtížnosti 1 659 071 428 milionů. Systém se snaží udržovat průměrný čas na vytěžení bloku na 15 sekund (Minerstat, 2023).

4.5.1 Výpočet nákladů pro těžbu

Pro Ethereum classic bude nejvýhodnější využít ASIC miner Jasminer X16-Q, ze všech dostupných zařízení dosahoval ohledně efektivity nejlepších výsledků. Cena uvedená výrobcem je 3 599 \$, bude tedy uváděna cena 79 770 Kč za kus. Jeden Jasminer X16-Q je schopen výkonu 1 845 MH/s při příkonu 630 W za hodinu. Těchto zařízení bude nakoupeno 12 a každé je vysoké 482 mm, široké 134 mm a dlouhé 360 mm. Proto budou umístěny do regálu s 4 policemi, kde bude také umístěn router a přepínač pro zajištění internetového připojení pomocí UTP kabelů. Regál bude umístěn v dostatečné vzdálenosti od dvojzásuvek,

aby bylo možné připojit každé těžební zařízení k elektrickému obvodu pomocí napájecí kabelu. Jelikož každý Jasminer X16-Q vyžaduje pouze jeden napájecí kabel, budou dvě těžební zařízení zapojena do jedné dvojjásovk, která je připojena k jednomu jednopólovému 16 ampérovému jističi. Ve 24 modulové rozvodnici jsou všechny komponenty vzájemně propojeny pomocí propojovací lišty. V rozvodnici je nainstalován proudový chránič, instalační vypínač, třífázový jistič a všechny jednopólové jističe. Jelikož nejsou známy rozměry budovy, ve které bude provozována těžba, bude na každou zásuvku odhadovány 2 metry CYKY kabelů. V tabulce 3 jsou vyčteny všechny položky, které budou nakoupeny i s cenami.

Tabulka 3 Seznam nakoupených prostředků pro těžbu Etherea classic

Název položky	Cena za kus (Kč)	Počet kusů	Celková cena (Kč)
Jasminer X16-Q	79 770	12	957 236
Třífázový jistič 16 A	375	1	375
Jednopólový jistič 10 A	88	7	616
Instalační vypínač 16 A	889	1	889
Proudový chránič 25 A	914	1	914
24 modulová rozvodnice	1 149	1	1 149
Propojovací lišta	537	1	537
Kabely CYKY (1,5mm)	21	12	252
Dvojjásovk	119	7	833
UTP kabel (2 m)	25	12	300
Regál pro ASIC zařízení	920	1	920
Přepínač (16 port)	1 899	1	1 899
Napájecí kabel 10 A	129	12	1 548

Zdroj: Vlastní zpracování, KVeлектро, CZC, Hornbach, Jasminer

Zajištění internetového připojení bude činit 299 Kč za měsíc, poskytovatel připojení v této ceně zahrnuje i router, tudíž nebude zahrnut v nákladech. Připojení k elektrické síti je odhadováno na 10 080 Kč, stránka edg.cz uvádí, že reálná cena zapojení se může lišit, dále však bude pracováno s touto hodnotou. Spotřeba elektřiny při těžbě po dobu 12 dnů a 17 hodin bude 9 010,36 Kč, při ceně elektřiny 3,89 Kč za kWh od Quantum a.s. Suma všech uvedených nákladů je rovna 986 857 Kč.

4.5.2 Potencionální výtěžek

Těžba s 12 zařízeními Jasminer X16-Q bude schopná produkovat hash rate o 22 140 MH za sekundu. Průměrný výpočetní výkon sítě Ethereum classic dosahuje 125,52 TH/s a průměrná obtížnost je 1 659 071 428,5 milionů. Na rozdíl od předchozích kryptoměn je u ETC počítán čas na blok pouze tak, že obtížnost je vydělena hash rate. Tudíž čas na blok sítě je 13,218 sekund a čas nakoupeného těžebního zařízení je 20 hodin a 48 minut na blok. Pro výpočet šance na vytěžení je použit vzorec zmíněný v kapitole 4.1. Po převedení výsledku na procenta je šance na vytěžení rovna 0,0176391 % každých 13,218 sekund. Jelikož těžba bude probíhat 12 dní a 17 hodin, bude možné vytěžit až 14 bloků ETC. To je způsobeno velmi malým časem na blok a menší obtížnosti na těžbu. Při odměně za blok 2,48 ETC může být za dobu těžby vytěženo Ethereum classic v hodnotě 16 825,61 Kč. Po odečtení ceny za spotřebovanou elektřinu je získána částka 7 815,26 Kč, která může být považována za celkový výtěžek.

4.5.3 Uhlíková stopa

Ke zjištění uhlíkové stopy vybraného těžebního zařízení při těžbě Etherea classic bude následovat stejný postup výpočtu jako u předchozích kryptoměn. Hodnota 415 gramů oxidu uhličitého na jednu kilowatt hodinu bude vynásobena počtem spotřebované elektřiny za dobu 12 dní a 17 hodin. Provozováním těžby této kryptoměny s využíváním elektrické sítě v České republice bude způsobena emise celkem 959,04 Kg oxidu uhličitého do ovzduší.

4.5.4 Zhodnocení a doporučení

Čas na vytěžení bloku u kryptoměna Ethereum classic, je velmi nízký, zároveň odměna za blok je také poměrně malá, konkrétně 1 201,82 Kč. Pokud by mělo být dosaženo navrácení investice, musela by být těžba provozována po dobu nejméně 1445 dní, a to při neměnné obtížnosti a za stejných okolností.

Při těžbě Etherea classic lze pozorovat poměrně malé náklady na spotřebu elektřiny, to dává možnost těžit s menším rizikem ztráty při nenalezení bloku. Výhodou těžby této kryptoměny je malý příkon jednoho zařízení Jasminer X16-Q, jelikož by bylo možné jej zapojit do stejné elektrické sítě, která je potřeba pro běžné domácí spotřebiče. Je tedy na místě úvaha, zda by nebylo možné využít Jasminer X16-Q jako domácí spotřebič jak pro

těžbu kryptoměny, tak zároveň pro ohřev vody či místnosti. Problémem je však hluk, který zařízení produkuje, tudíž by bylo potřeba vyhradit na toto zařízení samostatný prostor. Autor této práce by také doporučil využívání menšího počtu těžebních zařízení, jelikož by bylo dosaženo dřívějšího vrácení investice, pokud by nebylo potřeba zvětšovat infrastrukturu elektrické sítě v místě zapojení.

Ethereum classic má oproti předchozím kryptoměnám poměrně malou spotřebu elektřiny. Podle autorova mínění existuje možnost, že veškerá elektrická energie potřebná pro těžbu Etherea classic by mohla být vytvořena pouze z obnovitelných zdrojů. Pokud by těžba u ostatních kryptoměn splňovala tyto předpoklady, zvýšila by se tím šance, že těžba kryptoměn by nezvyšovala uhlíkovou stopu.

5 Výsledky a diskuse

V této kapitole jsou porovnány výsledky, ke kterým se dospělo v praktické části. Kryptoměny jsou zde porovnány dle jejich ekonomických a ekologických vlastností. Závěr této kapitoly je věnován diskusi.

Z výsledků lze vyčíst, že největšího možného výtěžku je dosahováno právě při těžbě Bitcoinu, a to 3 174 918,97 Kč. Vysoká odměna za vytěžení je však velmi nepravděpodobná, jelikož existuje pouze 0,55% šance, že po 12 dní a 17 hodinách těžby bude této odměny dosaženo. Druhý největší výtěžek lze zaznamenat u Litecoinu, kde za stejnou dobu těžby je možné získat 10 216,31 Kč. Na rozdíl od Bitcoinu existuje mnohem větší šance na získání této částky, tato šance je odhadována na 39 %. Dogecoin má ještě menší výtěžek, 4 000,37 Kč, za to však opět s vyšší šancí na úspěch při těžbě činí 82,78 %. Lze zde pozorovat trend, že s menším výtěžkem se zvyšuje šance na reálné získání odměny za blok. Výjimkou je Ethereum classic, u kterého tento trend neplatí, jelikož zde existuje stoprocentní šance na vytěžení 14 bloků, čímž vzniká čistý výtěžek v hodnotě 7 815,26 Kč.

Pokud bude věnována pozornost největšímu výtěžku, který nacházíme u Bitcoinu, je nutné také uvažovat nejen s malou šancí na vydělání velké sumy, ale také s nejvyšší uhlíkovou stopou, která při těžbě této kryptoměny vznikne, a to přesně 2 301,13 kilogramů CO₂. To je o 697,18 kg víc, než kolik emituje Dogecoin či Litecoin. Uhlíková stopa Etherea classic je dokonce o 1 342,09 kilogramů oxidu uhličitého menší. Toto zjištění je ale v kontrastu s tím, že po vypočtení profitu za kilogram CO₂ se Bitcoin s výtěžkem 1 379,72 Kč na kilogram CO₂ může zdát jako nejšetrnější kryptoměna pro životní prostředí, a to i v porovnání s Etherem classic, které má sice nejmenší uhlíkovou stopu, ale výtěžek pouze 8,97 Kč na kilogram CO₂. Z těchto zjištění naopak vyplývá, že Bitcoin je z hlediska šetrnosti k životnímu prostředí nejvhodnější. Pokud však bude do úvah zahrnut fakt, že šance na vytěžení Bitcoinu je pouhých 0,55 %, dojdeme k závěru, že označení Bitcoinu jako nejšetrnější kryptoměny není tak jednoznačné. Existuje zde totiž reálná šance, že mnozí těžaři výtěžku ani nedosáhnou. Tudíž by během těžby docházelo k produkovaní emisí, avšak bez jakéhokoli výtěžku.

Při interpretaci výsledků je třeba brát v potaz, že výpočty byly prováděny s neměnnými hodnotami obtížnosti a hash ratu sítě. To může výsledky značně zkreslit, oproti výsledkům dosažených při provozování těžby v reálném prostředí. Nelze tak zaručit, že při

zrealizování námi představené těžby, bude dosaženo vypočítaného výdělku. Dalším faktorem ovlivňující výpočet je aktuální cena elektřiny, pokud by byl výzkum proveden v jiném státu, výsledky by se lišily. Při určování uhlíkové stopy musí být bráno v potaz, že každá země generuje elektřinu použitím jiných zdrojů, pokud by tedy stát využíval k vytváření elektřiny 90 % obnovitelných zdrojů, bude uhlíková stopa výrazně menší. To stejné by platilo i v případě, že by těžař pro těžební zařízení využíval svůj vlastní obnovitelný zdroj elektřiny. Dalším aspektem, na který se lze zaměřit je nalezení alternativního využití ASIC minerů. Pokud by těžař využíval odpadní teplo z těžby kryptoměn například pro ohřev vody nebo vytápění místnosti, mohl by snížit své náklady za celkovou spotřebu elektřiny.

6 Závěr

Cílem této práce bylo zhodnotit těžbu jednotlivých kryptoměn a stanovit, jak tato těžba ovlivňuje životní prostředí. Dále byla kryptoměna popsána společně s jejími vlastnostmi a principy na kterých funguje. Společně s kryptoměnou také představit způsoby jakými je kryptoměna těžena a jaké prostředky jsou k tomu zapotřebí. Práce byla dále zaměřena na to, zda je těžba kryptoměn výhodná z ekonomického hlediska a jak ovlivňuje životní prostředí.

V teoretické části byl nejprve definován pojem kryptoměna a její vznik byl přiblížen na nejstarší kryptoměně nazývané Bitcoin. Dále byly popsány kryptografické principy, které kryptoměny využívají k zabezpečení a jsou pomocí peer-to-peer sítě distribuovány. Byla vysvětlena technologie blockchain, která je s kryptoměnami často spojována a bylo popsáno, jakou roli zde hraje. Dále byly přiblíženy důležité prvky v kryptoměnách jako jsou transakce či bloky. V následujících kapitolách byla také popsána těžba kryptoměny společně s prostředky k tomu využívanými. Závěrem teoretické části bylo zasazení uhlíkové stopy do kontextu kryptoměn.

V praktické části byly popsány čtyři kryptoměny využívající důkaz prací. U každé této kryptoměny byla vypočítána šance na vytěžení a to, jak velký výdělek lze očekávat. Dále byla určena velikost emisí oxidu uhličitého při těžbě dané kryptoměny na základě spotřebované elektřiny. Výsledky byly nadále porovnány z ekonomického a ekologického hlediska, kde z ekonomického hlediska lze považovat těžbu Bitcoinu jako možnost největšího potenciálního výdělku. Z ekologického hlediska bylo zjištěno, že Ethereum classic se z těchto čtyř kryptoměn jeví jako nejmenší hrozba pro životní prostředí.

Byl tedy představen nový typ měny, která může fungovat bez třetí strany a pouze v digitálním formátu. Tato práce potvrdila, že při těžbě kryptoměn nelze garantovat výdělek. Právě kvůli nejistotě výdělku se dá těžba kryptoměny přirovnat k loterii, kdy úspěch znamená výrazný ekonomický zisk a neúspěch může znamenat pravý opak. Nezávisle na zisku nebo ztrátě dochází k negativnímu působení na životní prostředí. Nelze opomenout, že kryptoměna přinesla nové technologie, které mohou přinést další inovace. Je nutné brát v potaz, že v dnešní době ještě nejsou známy všechny možné alternativy využití těžby kryptoměn.

7 Seznam použitých zdrojů

Bain, T. & Kent, P., 2022. *Cryptocurrency Mining for Dummies* 2. vydání, New Jersey: John Wiley & Sons, Incorporated. [online]. Dostupné z: <https://ebookcentral.proquest.com/lib/czup/detail.action?docID=7008421&query=cryptocurrency%20for%20dummies> [Cit. 22.1.2023].

Bitmain, 2022. bitmain.com. [online]. Dostupné z: <https://shop.bitmain.com/> [Cit. 23. února, 2023].

Casey, M. J., 2021. *Crypto Needs More Than Code to Beat the ASIC Mining Threat*. Coindesk.com. [obrázek, online]. Dostupné z: <https://www.coindesk.com/markets/2018/05/01/crypto-needs-more-than-code-to-beat-the-asic-mining-threat/> [Cit. 30. ledna, 2023].

Coinmarketcap, 2023. coinmarketcap.com. [online]. Dostupné z: <https://coinmarketcap.com/> [Cit. 27. ledna, 2023].

CZC, 2023. Czc.cz. [online]. Dostupné z: https://www.czc.cz/prislusenstvi_2/kategorie [Cit. 23. února, 2023].

Dogecoin, 2023. *What is Dogecoin?* dogecoin.com. [online]. Dostupné z: <https://dogecoin.com/dogepedia/articles/what-is-dogecoin/> [Cit. 21. února, 2023].

Egd, 2023. *Výpočet podílu žadatele na oprávněných nákladech*. egd.com [online]. Dostupné z: <https://www.egd.cz/vypocet-podilu-zadatele-na-opravnemych-nakladech> [Cit. 22. února, 2023].

El Geneidy a kol, 2021. *The carbon footprint of a knowledge organization and emission scenarios for a post-COVID-19 world*. Environmental impact assessment review. 91. vydání. [online]. Dostupné z: <https://doi.org/10.1016/j.eiar.2021.106645> [Cit. 1. února, 2023].

Ethereum classic, 2022. *Mining Resources*. ethereumclassic.org. [online]. Dostupné z: <https://ethereumclassic.org/mining> [Cit. 21. února, 2023].

Franco, P., 2014. *Understanding Bitcoin: Cryptography, Engineering and Economics*. Velká Británie: John Wiley & Sons, Incorporated. [online]. Dostupné z: <https://ebookcentral.proquest.com/lib/czup/detail.action?docID=1823060&query=Understanding+Bitcoin> [Cit. 17. ledna, 2023].

Globalpetrolprices, 2023. *Electricity prices*. globalpetrolprices.org. [online]. Dostupné z: https://www.globalpetrolprices.com/electricity_prices/ [Cit. 25. února, 2023].

Hornbach, 2023. Hornbach.cz [online]. Dostupné z: <https://www.hornbach.cz/> [Cit. 24. února, 2023].

Chowdhury, N. 2019. *Inside Blockchain, Bitcoin, and Cryptocurrencies*. Auerbach Publishers, Incorporated Milton. ISBN 9781138618152.

Chuen, D.L.K. *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data*. Elsevier Science & Technology, 2015, 612 s. ISBN 9780128021170.

Jasminer, 2022. jasminer.com. [online]. Dostupné z: <https://www.jasminer.com/#/productDetail/908ad3781bff473ba9155276caa84456> [Cit. 23. února, 2023].

Joom, 2023. *Dual Power Hard Disk 8 GPU Open Air Mining Rig Bitcoin Frame Case Stackable + USB Switch For ETH ZEC*, joom.com. [obrázek, online]. Dostupné z: https://www.joom.com/en/products/1516777446541101049-125-1-39131-2903071453?variant_id=1516777446541498025-126-4-39131-2282866744 [Cit. 28. ledna, 2023].

K&V Elektro, 2023. *Elektroinstalační materiál*, kvelektro.cz. [online]. Dostupné z: <https://www.kvelektro.cz/> [Cit. 23. února, 2023].

Kohli, a kol., 2022. *An analysis of energy consumption and carbon footprints of cryptocurrencies and possible solutions*, Digital Communications and Networks, 9. vydání. <https://www.sciencedirect.com/science/article/pii/S235286482200139> [Cit. 1. února, 2023].

Kurzy, 2023. *Elektrina – ceny a grafy elektriny*. kurzy.cz. [online]. Dostupné z: <https://www.kurzy.cz/komodity/cena-elekriny-graf-vyvoje-ceny/> [Cit. 23. února, 2023].

Lánský, J., 2018. *Kryptoměny*, Praha: C. H. Beck. ISBN 9788074007224.

Litecoin, 2023. *What is litecoin?* litecoin.org. [online]. Dostupné z: <https://litecoin.org/> [Cit. 21. února, 2023].

Minerstat, 2023. minerstat.com. [online]. Dostupné z: <https://minerstat.com/> [Cit. 23. února, 2023].

Nakamoto, S., 2008. *Bitcoin: Peer-to-Peer systém elektronických peněz*. Bitcoin.org. [online]. Dostupné z: https://bitcoin.org/files/bitcoin-paper/bitcoin_cz.pdf [Cit. 18. ledna, 2023].

Ourworldindata, 2023. *Carbon intensity of electricity, 2000 to 2022*. ourworldindata.org. [online]. Dostupné z: <https://ourworldindata.org/grapher/carbon-intensity-electricity?tab=chart®ion=Europe&country=~CZE> [Cit. 25. února, 2023].

Pernice, I.G.A. & Scott, B., 2021. *Cryptocurrency*. Internet Policy Review: Glossary of decentralised technosocial systems, 10(2), p.9. [online]. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3899258 [Cit. 15. ledna, 2023].

Selin, N. Eckley, 2022. *carbon footprint*. Encyclopedia Britannica. <https://www.britannica.com/science/carbon-footprint> [Cit. 1. února, 2023].

Sharma A. a kol, 2023. *An extended approach to appraise electricity distribution and carbon footprint of bitcoin in a smart city*. *Frontiers in big data*, 6. vydání. [online]. 1082113. <https://doi.org/10.3389/fdata.2023.1082113> [Cit. 1. února, 2023].

Skorjanc, M., 2019. *How mining pools distribute rewards? PPS vs FPPS vs PPLNS*. Nicehash.com. [online]. Dostupné z: <https://www.nicehash.com/blog/post/how-mining-pools-distribute-rewards-pps-vs-fpps-vs-pplns> [Cit. 24. ledna, 2023].

Tardi, C., *Application-Specific Integrated Circuit (ASIC) Miner*. Investopedia.com. Dostupné z: <https://www.investopedia.com/terms/a/asic.asp> [Cit. 22. ledna, 2023].

Pardeshi, K., 2021. *Review of blockchain architecture a survey*. *Jac: a journal of composition theory*. 13. vydání. [obrázek, online]. Dostupné z: https://www.researchgate.net/figure/Client-Server-Vs-P2P-network-Source_fig1_352213267 [Cit. 24. ledna, 2023].

Wendl, M., Doan, M. H., & Sassen, R., 2023. *The environmental impact of cryptocurrencies using proof of work and proof of stake consensus algorithms: A systematic review*. *Journal of environmental management*, 326. vydání. <https://doi.org/10.1016/j.jenvman.2022.116530> [Cit. 1. února, 2023].

Whattomine, 2020. Whattomine.com. [online]. Dostupné z: <https://whattomine.com/coins> [Cit. 21. února, 2023].

Wikipedia, 2023. *Dogecoin*. Wikipedia.org. [obrázek, online]. Dostupné z: <https://en.wikipedia.org/wiki/Dogecoin> [Cit. 25. února, 2023].

8 Seznam obrázků, tabulek a zkratk

8.1 Seznam obrázků

Obrázek 1	Struktura klient-serveru a peer-to-peer sítě	15
Obrázek 2	Těžební rig	21
Obrázek 3	Regál plný ASIC minerů těžících Bitcoin	23
Obrázek 4	Logo Dogecoinu	33

8.2 Seznam tabulek

Tabulka 1	Seznam nakoupených prostředků pro těžbu Bitcoinu.....	30
Tabulka 2	Seznam nakoupených prostředků pro těžbu Dogecoinu.....	34
Tabulka 3	Seznam nakoupených prostředků pro těžbu Etherea classic	39

8.3 Seznam použitých zkratk

A – Ampér

BTC – Bitcoin

CO₂ – Oxid uhličitý

CZK – Česká koruna

ČR – Česká republika

CYKY – pevné silové kabely

EH/s – Exahash za sekundu

FPGA – Field Programmable Gate Array

FPPS – Full Pay Per Share

GB – Gigabajt

GPU – Graphics processing unit

Kč – koruna česká

kW – kilowatt

kWh – kilowatthodina

LAN – Local Area Network

Mb/s – Megabit za sekundu

MH – Megahash
P2P – Peer-to-peer
PDU – Power distribution unit
PoS – Proof of stake
PoW – Proof of work
PPLNS – Pay Per Last N Share
Ppm – particles per milion
PPS – Pay per share
SHA-256 – Secure Hash Algorithm 256
TH/s – Terahash za sekundu
TWh – Terawatthodina
UTP – Unshielded twisted pair
USB – Universal Serial Bus
UTXO – Unspent transaction output
V – Volt
W – Watt