Univerzita Hradec Králové
Fakulta informatiky a managementu
Katedra informačních technologií

Grafické karty a kryptoměny

Bakalářská práce

Autor: Martin Portych
Studijní obor: Aplikovaná informatika

Vedoucí práce: prof. RNDr. Peter Mikulecký, Ph.D.

Hradec Králové Duben 2024

Prohlášení:

Prohlašuji, že jsem bakalářskou práci zpracoval samostatně a s použitím uvedené literatury.

vlastnoruční podpis

V Hradci Králové dne 23.4.2024 Martin Portych

Poděkování:

Děkuji vedoucímu bakalářské práce prof. RNDr. Peter Mikulecký, Ph.D. za metodické vedení práce a jeho trpělivost, ochotu a podporu během celého procesu.

Abstrakt

Tato bakalářská práce poskytuje komplexní přehled problematiky těžby kryptoměn s využitím grafických karet. Cílem je analyzovat základní principy a různé typy těžby kryptoměn, přičemž se zaměřuje na výběr vhodných grafických karet pro tuto činnost. Práce rovněž identifikuje a hodnotí výhody a rizika spojená s jednotlivými typy těžby.

V první části práce jsou popsány základní pojmy a principy těžby kryptoměn, včetně algoritmů a vývoje těžebních technologií. Dále se jsou uvedeny různé typy těžby, těžebních zařízení, algoritmů a těžebních softwarů. Práce věnuje pozornost historii grafických karet v těžbě kryptoměn, jejich architektuře a specifikacím, technologickým inovacím a porovnání výkonu.

V další části je věnována pozornost stavbě těžební stanice, porovnávání grafických karet, testování grafické karty, výběru vhodného algoritmu a testování a porovnávání těžebních softwaru a operačních systémů.

V závěrečné části jsou shrnuty hlavní zjištění a výsledky práce, a jsou navržena doporučení pro investory a těžaře. Práce také nabízí pohled na aktuální stav kryptoměn a jejich vzájemné porovnání dle definovaných kritérií.

Tato bakalářská práce přispívá k lepšímu porozumění problematiky těžby kryptoměn a poskytuje užitečné informace pro ty, kteří se zajímají o tuto dynamickou oblast.

Abstract

Title: Graphic cards and cryptocurrencies

This bachelor thesis provides a comprehensive overview of cryptocurrency mining using graphics cards. The aim is to analyze the basic principles and various types of

cryptocurrency mining, with a focus on selecting suitable graphics cards for this activity. The thesis also identifies and evaluates the advantages and risks associated with different types of mining.

The first part of the thesis describes the basic concepts and principles of cryptocurrency mining, including algorithms and the development of mining technologies. It further introduces various types of mining, mining devices, algorithms, and mining software. The thesis pays attention to the history of graphics cards in cryptocurrency mining, their architecture and specifications, technological innovations, and performance comparison.

The next part focuses on building a mining rig, comparing graphics cards, testing graphic cards, selecting a suitable algorithm, and testing and comparing mining software and operating systems.

In the final section, the main findings and results of the thesis are summarized, and recommendations are proposed for investors and miners. The thesis also offers insights into the current state of cryptocurrencies and their mutual comparison according to defined criteria.

This bachelor thesis contributes to a better understanding of cryptocurrency mining issues and provides useful information for those interested in this dynamic field.

Klíčová slova: kryptoměna, těžba, kryptografie, blockchain, důkaz prací, Bitcoin

Key words: cryptocurrency, mining, cryptography, blockchain, proof of work, Bitcoin

Obsah

1 Úvod

S rozvojem digitálních technologií a růstem zájmu o decentralizované finanční systémy se kryptoměny staly v posledních letech středem pozornosti v oblasti ekonomiky a investic. Jednou z klíčových činností spojených s těmito digitálními aktivy je jejich těžba, proces, který nejenom vytváří nové jednotky kryptoměn, ale také zajišťuje bezpečnost a decentralizaci jejich transakčních sítí. V tomto kontextu se využívají různé technologie, přičemž grafické karty patří mezi jednu z nejrozšířenějších metod těžby.

Tato bakalářská práce se zaměřuje na komplexní analýzu problematiky těžby kryptoměn s důrazem na využití grafických karet. Účelem je přispět k porozumění základním principům a různým typům těžby kryptoměn, a to zejména s ohledem na výběr a efektivitu grafických karet pro tento účel. Dále se práce zabývá identifikací a hodnocením výhod a rizik spojených s jednotlivými metodami těžby.

V rámci této práce budou rozebírány základní pojmy a principy těžby kryptoměn, algoritmy využívané v tomto procesu a nejnovější technologické inovace v oblasti těžebních grafických karet. Dále je představena historie a architektura grafických karet ve vztahu k těžbě kryptoměn, a jsou provedeny porovnání výkonu a efektivity různých modelů.

Další části práce se věnují konkrétním postupům stavby těžebních stanic, výběru vhodného hardwaru a softwaru pro těžbu, a testování jejich výkonu. Závěrečná část práce shrnuje hlavní zjištění, výsledky a doporučení pro investory a těžaře, a poskytuje pohled na aktuální stav a budoucí směry vývoje v oblasti těžby kryptoměn.

Tato bakalářská práce má za cíl přispět k lepšímu pochopení problematiky těžby kryptoměn a poskytnout užitečné informace pro ty, kteří se zajímají o tento dynamický a stále se rozvíjející obor.

2 Cíl a metodika práce

Cílem této práce je provést komplexní analýzu problematiky těžby kryptoměn, zejména s ohledem na využití grafických karet, a poskytnout užitečné informace a doporučení pro investory a těžaře.

Pro dosažení tohoto cíle jsou stanoveny následující kroky a metodologie.
Studium teoretických základů: Provést důkladný průzkum literatury a nastudovat základní pojmy, principy těžby kryptoměn, algoritmy, mechanismy konsenzu a ekologické aspekty.

Analýza historie a vývoje grafických karet. Zkoumat historický vývoj grafických karet v kontextu těžby kryptoměn, identifikovat klíčové inovace a technologické změny.

Vyhodnocení výkonu a efektivity grafických karet. Provést srovnání výkonu a efektivity různých modelů grafických karet.

Hodnocení těžebního softwaru. Posoudit různé typy těžebního softwaru, včetně jejich vlastností, funkcí a výkonu, a provést porovnání na základě konkrétních kritérií.

Testování výkonu a efektivity. Provést experimenty a testy s cílem zhodnotit výkon a efektivitu těžebních softwaru za různých podmínek a scénářů.

Shrnutí a formulace doporučení. Shrnutí hlavních zjištění, výsledků a doporučení pro investory a těžaře, a poskytnutí pohledu na aktuální stav a budoucí směry vývoje v oblasti těžby kryptoměn.

Metodologie práce spočívá v kombinaci teoretického výzkumu, experimentů a praktických testů, které mají za cíl poskytnout komplexní a relevantní informace pro zkoumanou problematiku.

3 Vymezení pojmů

V úvodní sekci bakalářské práce je nezbytné přesně vymezit klíčové termíny spojené s digitálním světem kryptoměn a jejich těžby. Mezi termíny, které je potřeba popsat patří:

Digitální měna

Digitální měna představuje formu peněz, která existuje pouze v elektronické podobě, což znamená, že nemá fyzickou reprezentaci. Je zaznamenána v elektronické databázi. Příkladem digitální měny v každodenním životě mohou být finanční prostředky uložené na bankovním účtu. (42)

Virtuální měna

Existuje pouze v elektronické nebo digitální podobě a nemá fyzickou reprezentaci. Virtuální měny jsou vydávány soukromými organizacemi nebo skupinami vývojářů a jsou většinou neregulované. Virtuální měny se snaží zvýšit rychlost transakcí odstraněním prostředníků z procesu (banka), ale jsou také náchylné k napadení a online podvodům. Mimo svou oblast působení ztrácí měna hodnotu. (44)

Kryptoměna

Kryptoměna je digitální měna, která nepotřebuje banku nebo centrální autoritu k ověření transakcí. K ověření transakcí využívá šifrování. Jedná se o peer-to-peer systém, který umožňuje komukoli, kdekoli posílat a přijímat platby. Transakce s kryptoměnami jsou prováděny prostřednictvím digitálních peněženek a kryptoměnových burz. Každý účastník této sítě má svou vlastní digitální peněženku. Když uživatel provede transakci s kryptoměnou, tato transakce je zapsána do transparentní a veřejně dostupné databáze. (43)

3.1 Blockchain

Blockchain je databáze transakcí, která je aktualizována a sdílena na mnoha počítačích (uzlech) v síti, což zajišťuje rovnoměrné rozložení informací a odolnost proti jednotlivým selháním. Pokaždé, když je přidána nová sada transakcí, nazývá se to „block“ - odtud pochází název blockchainu. Existují tři základní vlastnosti blockchainu. Zaprvé, databáze blockchainu musí být kryptograficky zabezpečená. To znamená, že k přístupu nebo přidání dat do databáze potřebujete veřejný klíč a soukromý klíč. Dále je blockchain digitálním záznamem nebo databází transakcí, což znamená, že probíhá zcela online. A konečně, blockchain je databáze, která je sdílena napříč veřejnou nebo privátní sítí. Jednou z nejznámějších veřejných blockchainových sítí je Bitcoin

blockchain. Kdokoli může otevřít Bitcoin peněženku nebo se stát uzlem v síti. Znamená to, že veřejné blockchainy umožňují každému přidávat, ale neodebírat data. Pokud by někdo chtěl změnit některé informace nebo podvádět systém, musel by to udělat na většině počítačů v síti. To je energeticky velmi náročné. To činí decentralizované blockchainy velmi bezpečnými. Původně vznikl jako technologický základ pro kryptoměny, jako je Bitcoin, ale blockchain má širší uplatnění. Lze ho využít například pro zabezpečení dodavatelských řetězců, hlasování, správu identit a mnoho dalších oblastí, kde je klíčová důvěra a transparentnost v transakcích. Jiné blockchainy mohou být soukromé sítě, které jsou relevantnější pro bankovnictví , kde lidé potřebují vědět přesně, kdo se účastní, kdo má přístup k datům a kdo má soukromý klíč k databázi.[34]

3.2 Kryptografie

Je to vědní obor, který se zabývá zabezpečením komunikace a informací pomocí matematických a algoritmických metod. Cílem kryptografie je zajistit, aby komunikace mezi dvěma stranami zůstala tajná a nedotčená třetími stranami. Zároveň se snaží ověřit pravost informací a zajistit, že nebyly změněny během přenosu.[19]

3.2.1 Symetrická

Jedná se o šifrovací systém, kde odesílatel a příjemce zprávy používají společný klíč k šifrování a dešifrování zpráv. Systémy se symetrickým klíčem jsou rychlejší a jednodušší, ale problémem je výměna klíče mezi odesílatelem a příjemcem zabezpečeným způsobem. Nejpopulárnějšími systémy symetrické kryptografie jsou Data Encryption System (DES) a Advanced Encryption System (AES) [20]

3.2.2 Asymetrická

Asymetrická kryptografie je šifrovací metoda, která využívá dva klíče: veřejný klíč pro šifrování a privátní klíč pro dešifrování. Veřejný klíč je sdílen s ostatními, zatímco privátní klíč zůstává tajný. [19] Tato technologie umožňuje bezpečnou komunikaci bez potřeby sdílení společného klíče. Nejznámějším asymetrickým algoritmem je RSA, často používaný v digitální komunikaci a vytváření digitálních podpisů.[21]

4 Kryptoměny

V této kapitole se věnuji detailní charakteristice vybraných kryptoměn, včetně jejich historie a principů fungování. Na začátku objasním, co je to alternativní měna a její typy. Poté se zaměřuji na nejpopulárnější kryptoměnu, Bitcoin a na zkoumání různých aspektů, jako je jeho ukládání, vlastnosti, zabezpečení a historický od jeho vytvoření. Následně představuji další klíčové kryptoměny, jako jsou Ethereum, Litecoin, RavenCoin, a poskytuji základní informace o jejich charakteristikách. Kromě toho se zaměřuji na vysvětlení důležité terminologie pro lepší porozumění tomuto tématu.

4.1 Altcoiny

Alternativní měna neboli "altcoin" je termín používaný pro všechny kryptoměny, které jsou alternativou k Bitcoinu. Bitcoin, jako první a nejznámější kryptoměna, položil základy pro vývoj celého odvětví digitálních měn. Altcoiny vznikly jako reakce na Bitcoin a často se snaží přinést inovace nebo řešit omezení, která jsou spojena s původním konceptem Bitcoinu.

Počátky altcoinů sahají do období několika let po vzniku Bitcoinu. Prvním známým altcoinem byl Namecoin, který byl spuštěn v dubnu 2011. Namecoin byl zaměřen na decentralizovaný systém pro registraci domén s koncovkou ".bit". Dalšími ranými altcoiny byly například Dogecoin nebo Litecoin, známý pro rychlejší časy potvrzení transakcí, tyto alcoiny vychází z open source kódu bitcoinu, který následně upraví. Existují další altcoiny, které mají vlastní kód, jako například Solana nebo Ethereum.

Budoucnost altcoinů závisí na schopnosti přinášet inovace, řešit aktuální nedostatky v kryptosvětě a udržet si uživatelskou základnu. S rychlým vývojem technologie blockchain a kryptoměn můžeme očekávat další rozmanité altcoiny, které přinesou nové příležitosti a výzvy pro ekosystém digitálních měn.

Existuje tisíce různých altcoinů, z nichž každý má své vlastní specifické vlastnosti a zaměření. [18] Některé z hlavních kategorií altcoinů zahrnují: stablecoins, mining based, utility tokens, security tokens. [26]

4.1.1 Stablecoins

Stablecoiny představují subtyp altcoinů, které jsou podloženy rezervou tradičních fiat měn, jako jsou americké dolary (USD), eura nebo jiné národní měny. Jejich hlavním cílem je poskytnout uživatelům stabilní a bezpečný způsob uchování hodnoty v rámci

kryptoměnového prostředí, které je obvykle charakterizováno výraznou volatilitou. Využívají se často na krypto burzách. Nejrozšířenějším je Tether neboli USDT. [26]

4.1.2 Těžebně založené

Tato kategorie altcoinů je založena na procesu těžby, což je klíčový prvek vytváření nových jednotek digitální měny. Tyto altcoiny se těží pomocí speciálních hardwarových zařízení nebo grafických karet, a to prostřednictvím matematických algoritmů. Těžaři přispívají svým výpočetním výkonem k udržování bezpečnosti sítě a ověřování transakcí. [26]

4.1.3 Utility tokens

Altcoiny v kategorii utility tokens jsou navrženy tak, aby poskytovaly přístup nebo služby v rámci specifického ekosystému nebo platformy. Tyto tokeny mají praktický účel v rámci určité aplikace nebo systému a jsou často využívány pro financování projektů nebo společností. [26]

4.1.4 Security tokens

Security tokens jsou altcoiny, které reprezentují podíl nebo majetková práva a jsou podobné tradičním cenným papírům. Tyto tokeny podléhají regulacím a mohou být využity pro emitování digitálních akcií, dluhopisů nebo jiných finančních nástrojů. [26]

4.2 Bitcoin

Bitcoin, zavedený v roce 2009 pod tajemným pseudonymem Satoshi Nakamoto, představuje revoluční digitální měnu, která změnila pohled na finanční systémy. Jeho významné charakteristiky a decentralizovaná povaha přispěly k jeho celosvětové adopci.

Bitcoin operuje bez centrální autority či regulátora, což umožňuje přímé transakce mezi uživateli bez potřeby prostředníků. Záznam všech transakcí je uchováván v blockchainu, což zajišťuje transparentnost a bezpečnost transakcí. S limitovaným počtem bitcoinů, který může být vytěžen (21 milionů), je zabraňováno inflaci a vytváří se odolnost proti devalvaci měny. [14]

Bitcoinové transakce jsou ověřovány a nové bloky jsou vytvářeny prostřednictvím těžby, procesu, který zapojuje uživatele známé jako těžaři, kteří jsou odměňováni za svou účast. Těžební odměny jsou však dynamické a s určitou periodicitou dochází k události nazývané "halving". Během halvingu se odměny za nalezení nového bloku

automaticky snižují o polovinu, což má za následek zpomalení tempa tvorby nových bitcoinů a omezení jejich nabídky na trhu. [1]

Základní principy fungování Bitcoinu spočívají v používání unikátních bitcoinových adres, které umožňují uživatelům provádět transakce s touto měnou. Tyto transakce jsou ověřovány pomocí kombinace veřejných a soukromých klíčů, což zajišťuje bezpečnost a důvěryhodnost procesu. Každý účet v síti Bitcoin má svůj unikátní veřejný a privátní klíč. Veřejný klíč slouží jako adresa, na kterou mohou ostatní uživatelé posílat bitcoiny. Privátní klíč je tajný klíč, který umožňuje odesílat bitcoiny z dané adresy. Potvrzené transakce jsou pak seskupovány do bloků a následně přidávány do blockchainu, což je decentralizovaný a neustále se rozšiřující systém zaznamenávající veškeré transakce provedené s Bitcoiny. Legitimitu transakcí kontrolují těžaři, kteří je přidávají do blockchainu a kontrolují pomocí algoritmu SHA-256. [35]

Bitcoin je využíván pro různé účely, od provedení transakcí až po investice a uchovávání hodnoty. Všechny transakce jsou veřejné a samotná identita uživatelů zůstává většinou anonymní. Cena bitcoinu je považována za velmi volatilní, což odráží jeho citlivost na tržní poptávku a nabídku. Přestože jeho přínosy jsou mnohé, je třeba brát v úvahu i výzvy spojené s vysokou volatilitou. [14]

4.2.1 Uchovávání bitcoinu

Bitcoin, podobně jako běžný bankovní účet nebo peněženka, vyžaduje pečlivou ochranu a správu pro minimalizaci rizika krádeže. Uživatelé mají k dispozici různé metody uchování svých bitcoinů, které jim umožňují efektivně chránit své digitální bohatství.

První možností je uchovávat své bitcoiny přímo na osobních počítačích nebo mobilních zařízeních. Tato metoda poskytuje uživatelům přímý přístup k jejich bitcoinům a umožňuje jim spravovat své finance přímo z jejich zařízení.

Jednou z dalších možností jsou hardwarové peněženky, jako je Trezor nebo Ledger. Tyto fyzické zařízení jsou koncipována pro bezpečné uchovávání digitálních měn mimo online prostředí. Uživatelé s nimi získávají veškerou kontrolu nad svými bitcoiny a minimalizují tak riziko zneužití nebo odcizení.

Alternativou k hardwarovým peněženkám jsou online peněženky. Tyto internetové externí služby poskytují online úložiště pro digitální měny. umožňují uživatelům přistupovat ke svým bitcoinům z libovolného zařízení připojeného k internetu, což zvyšuje jejich pohodlí, ale zároveň vyžaduje důvěru v poskytovatele služby.[2]

4.2.2 Anonymita

I přes některé mýty o úplné anonymitě Bitcoinu, každá transakce vytváří identifikovatelný záznam. Transparentnost blockchainu umožňuje sledování transakcí. Pro dosažení vyšší úrovně anonymity lze pravidelně vytvářet nové Bitcoinové adresy. Ty jsou složeny z unikátních řetězců a umožňují uživatelům anonymní transakce. Bitcoin Mixer, známý také jako Tumbler, poskytuje službu míchání transakcí. To pomáhá zakrýt cestu k původní Bitcoin adrese, tato technika často slouží k nelegálním účelům. [36]

4.2.3 Historie Bitcoinu

2008

V roce 2008 byl Bitcoin poprvé navržen a popsán osobou nebo skupinou osob známou pod pseudonymem Satoshi Nakamoto. Byl zveřejněn bílý papír s názvem "Bitcoin: A Peer-to-Peer Electronic Cash System" na stránce "Bitcoin.org", ten popisoval koncept první decentralizované digitální měny. [2]

2009

První Bitcoinový blok, nazývaný "Genesis Block", byl vytvořen 3. ledna 2009. Tím začala oficiální historie Bitcoinu. Bitcoinová síť byla spuštěna, a lidé mohli začít těžit a obchodovat s touto digitální měnou. První transakce proběhla v tomto období. Na adresu „1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa“ bylo zasláno 50 bitcoinů, které jsou do dnes na stejné adrese. [2]

2010

V roce 2010 vznikla první webová stránka nazvaná „The Bitcoin Market“, která umožňovala provádět platby v Bitcoinu. Tuto novinku představil uživatel s přezdívkou „dwdollar“. Během tohoto období se Bitcoin poprvé setkal s významnou výzvou, kdy hacker vytvořil měnu v hodnotě 184 miliard Bitcoinů. Nicméně tato chyba byla rychle odstraněna díky promptní reakci ze strany Satoshiho. Avšak skutečný zlom se stal na fóru bitcointalk.org, kde někdo nabídl 10 000 bitcoinů za 2 velké pizzy, tato transakce byla provedena. [2]

2011

Rok 2011 přivedl rozšíření platby pomocí Bitcoinu do fyzického světa. Bitcoin se začal objevovat v běžných obchodech, na nejrůznějších online platformách, a dokonce i na nelegálních internetových stránkách, kde byl využíván díky nízkému riziku odhalení.

Některé internetové stránky byly dostupné jedině na darkwebu pomocí neregulovaného internetového prohlížeče „Tor“, což zvyšovalo anonymitu uživatelů. [2]

2012-2013

Se zvyšujícím se zájmem začali vznikat prvotní Bitcoin bankomaty. San Diego (Kalifornie) bylo prvním městem, kde jste mohli směňovat Bitcoiny za reálné peníze. Postupem času začal Bitcoin přitahovat pozornost daňových autorit, což vedlo k začlenění této digitální měny do daňové regulace, ačkoliv byl původně vnímán spíše jako alternativní forma aktiv. [2]

2014–2016

Rok 2014 přinesl největší problém v historii Bitcoinu s kolapsem burzy Mt. Gox, což mělo důsledky pro důvěru v digitální měnu. Následující léta byla obdobím stabilizace, získávání důvěry a postupné akceptace od obchodníků.

2017–2019

Rok 2017 byl poznamenán ohromujícím růstem ceny Bitcoinu na více než 20 000 USD, což přitáhlo nejen pozornost médií, ale i institucionálních investorů. Následovala však korekce trhu v roce 2018, provázená regulačními změnami. Rok 2019 přinesl nárůst institucionálního zájmu a přijetí Bitcoinu jako "digitálního zlata".

2020–2023

Zvýšený zájem institucí a korporací přinesl nové výzvy a možnosti. Rok 2021 byl zaznamenán novými rekordy v ceně bitcoinu a dalším přijetím. Před rokem 2023, bylo v digitálním světě stále více očekávání a nadšení z dalšího vývoje Bitcoinu, současný vývoj ještě nelze plně hodnotit. [16]

4.3 Ethereum

Ethereum je jeden z nejúspěšnějších altcoinů, představuje decentralizovanou globální open source softwarovou platformu poháněnou blockchain technologií. Její nejznámější součástí je vlastní kryptoměna ether (ETH). Na rozdíl od Bitcoinu má Ethereum širší funkčnost než pouhá digitální měna. Slouží jako otevřená platforma pro každého, kdo chce vytvořit bezpečné digitální technologie. Zatímco má svou vlastní tokenovou měnu pro podporu blockchain operací, účastníci mohou Ethereum také používat k platbě za hmatatelné zboží a služby, pokud je přijímáno.

Navrženo s ohledem na škálovatelnost, programovatelnost, bezpečnost a decentralizaci, Ethereum se stalo preferovaným blockchainem pro vývojáře a podniky, kteří chtějí transformovat různé odvětví a každodenní život. Jednou z jeho klíčových

funkcí je podpora Smart Contracts, klíčových nástrojů za decentralizovanými aplikacemi, často používanými v oblasti decentralizovaných financí (DeFi). [28]

Smart Contracts

Chytré smlouvy jsou automatizované programy, které běží na blockchainu a provádějí akce, když jsou splněny určité podmínky. Tato funkce je jedním z klíčových prvků blockchainu Ethereum a rozšiřuje možnosti kryptoměny nad jednoduchý převod hodnoty. Chytré smlouvy jsou napsány pomocí programovacího jazyka, který definuje podmínky a akce, které mají být provedeny. Chytré smlouvy na Ethereum jsou nerozlišující a nezávislé, což znamená, že každý k nim má stejný přístup a mohou být spuštěny kdykoli.

Chytré smlouvy mají širokou škálu aplikací, včetně automatizovaných financí (DeFi), digitálních uměleckých děl (NFT), smluvního pojištění a mnoho dalšího. Tyto smlouvy přidávají vrstvu programovatelnosti a autonomie k blockchainu, umožňující vytváření komplexních a decentralizovaných ekosystémů. [25]

4.3.1 Ether

Slouží jako palivo pro provádění operací na Ethereum platformě. Kromě toho umožňuje vývojářům vyvíjet a spouštět decentralizované aplikace (DApps) na Ethereum blockchainu. DApps jsou aplikace, které běží na decentralizovaném a distribuovaném síti, což zajišťuje bezpečnost a nedostupnost třetím stranám.[49]

4.3.2 Ethereum 2.0

Ethereum 2.0, také nazývané Eth2 nebo Serenity, představuje důležitou aktualizaci Ethereum, která přechází na nový konsensuální mechanismus známý jako proof-of-stake (PoS). Tato aktualizace má za cíl snížit cenu poplatků, zvýšit škálovatelnost, bezpečnost a udržitelnost sítě Ethereum. [13]

4.3.3 Historie

Vývoj Ethereum začal v roce 2013 pod vedením Vitalika Buterina, kanadského programátora a spisovatele. V roce 2015 byla spuštěna první verze Ethereum s názvem „Frontier“. Následně byly vydány aktualizace, včetně „Homestead“, „Metropolis“ a „Constantinople“, aby se zlepšila efektivita, bezpečnost a škálovatelnost sítě. [28]

4.4 Litecoin

Jedná se o alternativní kryptoměnu vytvořenou z otevřeného zdrojového kódu Bitcoinu, avšak s několika úpravami. Stejně jako Bitcoin, i Litecoin je založen na decentralizované globální platební síti, kterou nespravuje žádný centrální orgán. Litecoin se liší od Bitcoinu v aspektech jako je rychlejší tvorba bloků za použití algoritmu Scrypt, díky němu je poskytnout uživatelům snadný způsob provádění rychlých a levných transakcí. Toho je dosaženo díky menším finančním nákladům na transakce a převody prováděné uvnitř sítě. Stejně jako Bitcoin má i Litecoin maximální počet LTC pevně stanoven. Nikdy nebude více než 84 milionů litecoinů v oběhu. Každých 2,5 minuty síť Litecoinu generuje nový blok (Bitcoin generuje blok každých 10 minut). Litecoinová nadace odhaduje, že kolem roku 2142, bude vytěžen maximálního počet litecoinů.

Litecoin je považován za jeden z prvních altcoinů. Původně byl silným konkurentem Bitcoinu. Avšak s nasycením a zvýšenou konkurencí na trhu s kryptoměnami se popularita Litecoinu poněkud snížila. [33]

4.4.1 Historie

Historie Litecoinu sahá až do roku 2011, kdy byl poprvé představen jako open-source projekt pod pseudonymem „Satoshilite“ Charliem Leem. V tomto období byly vidět počátky nové alternativy k Bitcoinu, s cílem řešit některé jeho nedostatky, jako je rychlost transakcí a náklady na těžbu.

V roce 2013 Litecoin zažil rapidní nárůst, kdy jeho cena vystoupala téměř na úroveň 50 dolarů. Tento výrazný zájem investorů a těžařů posílil jeho popularitu a rozšíření, což naznačuje obrovský potenciál této digitální měny.

Avšak počátek roku 2014 přinesl výzvy, kdy těžba Litecoinu pomocí grafických karet byla náhle zastíněna příchodem ASIC zařízení. Tento vývoj vedl k postupnému úbytku menších těžařů a k poklesu hodnoty této měny, což naznačovalo i možné slabiny v decentralizovanosti této kryptoměny.

V roce 2017 zažil Litecoin období obnoveného zájmu, kdy nové technologie jako SegWit. SegWit byl poprvé navržen pro Bitcoin v roce 2015 s cílem zvýšit škálovatelnost sítě Bitcoin. SegWit funguje tím, že "segreguje" digitální signálová data (tzv. "svědectví") mimo základní blok v blockchainu. V roce 2017 Litecoin přijal SegWit a kvůli podobnosti s Bitcoinem fungoval jako testovací plocha pro ověření životaschopnosti SegWitu na větší síti Bitcoinu. Test byl úspěšný, a Bitcoin následně

přijal SegWit. SegWit pomáhá zvýšit kapacitu bloku a zlepšit efektivitu transakcí. Paralelně s tím byla vyvinuta druhá vrstva, Lightning Networks. Lightning Network je druhá vrstva technologie pro Bitcoin, která využívá mikroplatební kanály k škálování schopností blockchainu a k provádění transakcí. Podobně jako v případě SegWit byla implementace Lightning Network na litecoinu testována, aby se ověřila možnost inovací na Bitcoinu. Lightning network výrazně zlepšila rychlost a efektivitu transakcí v blockchainu.(33)

4.4.2 RavenCoin

Ravencoin je kryptoměna, která byla spuštěna v lednu 2018 jako open-source projekt. Hlavním cílem Ravencoinu je umožnit uživatelům vytvářet a obchodovat s digitálními aktivy na decentralizované blockchainové síti.

Jednou z hlavních inovací Ravencoinu je jeho zaměření na tokenizaci aktiv. To znamená, že uživatelé mohou vytvářet vlastní digitální tokeny, reprezentující různé aktiva, jako jsou například akcie, nemovitosti, umění nebo dokonce jiné kryptoměny. Tato funkcionalita dělá z Ravencoinu platformu pro digitální aktiva s důrazem na decentralizaci, bezpečnost a transparentnost.

Jednou z dalších výhod Ravencoinu je jeho finanční návratnost při těžbě pomocí grafických karet. Díky svému algoritmu KAWPOW, což umožňuje širší účast ve těžbě a podporuje decentralizaci sítě. Tím se odlišuje od některých jiných kryptoměn, které se staly závislými na specializovaném hardwaru (ASICs), což může vést k centralizaci těžby.

Tato vlastnost Ravencoinu přitahuje těžaře, kteří chtějí využít své existujících GPU pro těžbu kryptoměn a dosáhnout solidního výnosu. Díky decentralizovanosti těžby, kterou podporuje použití GPU, mohou těžaři konkurovat s velkými těžebními farmami a přispívat k rovnoměrnější distribuci těžební moci v síti.(32)

5 Těžba kryptoměn

Těžba kryptoměny je proces, při kterém se vytvářejí nové jednotky digitální měny a současně jsou ověřovány a zaznamenávány transakce v blockchainu. Tento klíčový proces je základní pro fungování kryptoměnových sítí a zajišťuje jejich bezpečnost a decentralizaci. V tomto průvodci si přiblížíme základy těžby kryptoměny a seznámíme se s hlavními koncepty a postupy spojenými s touto činností.

5.1 Měření rychlosti těžby

Rychlost těžby, často označované jako hashrate, představuje klíčový prvek v oblasti kryptoměn a blockchainu. Tento ukazatel vyjadřuje výpočetní sílu, která je vynakládána na těžbu kryptoměn nebo ověřování transakcí v blockchainu. Hash je matematická funkce, která převádí vstup libovolné délky na zašifrovaný výstup pevné délky. Bez ohledu na velikost vstupních dat, výsledný hash bude mít vždy stejnou délku. [15]Navíc se hashe nedají použít k "zpětnému inženýrství" vstupu z hashovaného výstupu, protože hashovací funkce jsou "jednosměrné" (jako masový mlýnek; nemůžete vložit mleté maso zpět do steaku).[15] Nicméně, pokud takovou funkci použijete na stejná data, jejich hash bude identický, takže můžete ověřit, že data jsou stejná, pokud znáte jejich hash. Hashrate je měřen v jednotkách hashů za sekundu (H/s) nebo v násobcích této jednotky, jako jsou KH/s, MH/s, GH/s, TH/s, PH/s nebo EH/s.

Vyšší hashrate znamená, že těžební zařízení nebo síť je schopna provádět více hashovacích operací za sekundu, což zvyšuje šanci na úspěšné řešení těžebních úkolů a získání odměny v podobě nově těžených kryptoměn nebo transakčních poplatků. Těžební zařízení s vyšším hashratem mají v rámci sítě konkurenční výhodu. Tato metrika je klíčová při určování těžební obtížnosti blockchainové sítě a slouží jako ukazatel její bezpečnosti.

Pro hodnocení výkonu těžebního hardwaru se používá Benchmark, což je soubor testů, které měří rychlost a efektivitu těžebních zařízení. Cílem benchmarku je poskytnout uživatelům objektivní data pro optimalizaci svého těžebního hardwaru. Testy Benchmarku zahrnují spuštění definovaných těžebních operací a sledování, jak rychle a efektivně dané zařízení tyto operace zpracovává. [47]

5.1.1 Testování GPU

Testování neboli benchmarking u GPU se provádí pomocí speciálních nástrojů, jako je GPUScore, které měří rychlost, výkon a efektivitu GPU v různých zařízeních. Těmito nástroji se spouští zátěžové testy, které simulují náročné úlohy, například herní obsah s náročnou grafikou. Výsledkem je numerické skóre, které umožňuje porovnávat výkon GPU mezi různými zařízeními. [45]

5.2 Mechanismy koncensu

Existují dva hlavní mechanismy, které utvářejí základní strukturu těžby a zajišťují konsensus v blockchainových sítích. Tyto mechanismy jsou Proof of Work (PoW) a Proof of Stake (PoS).

5.2.1 Proof of Work

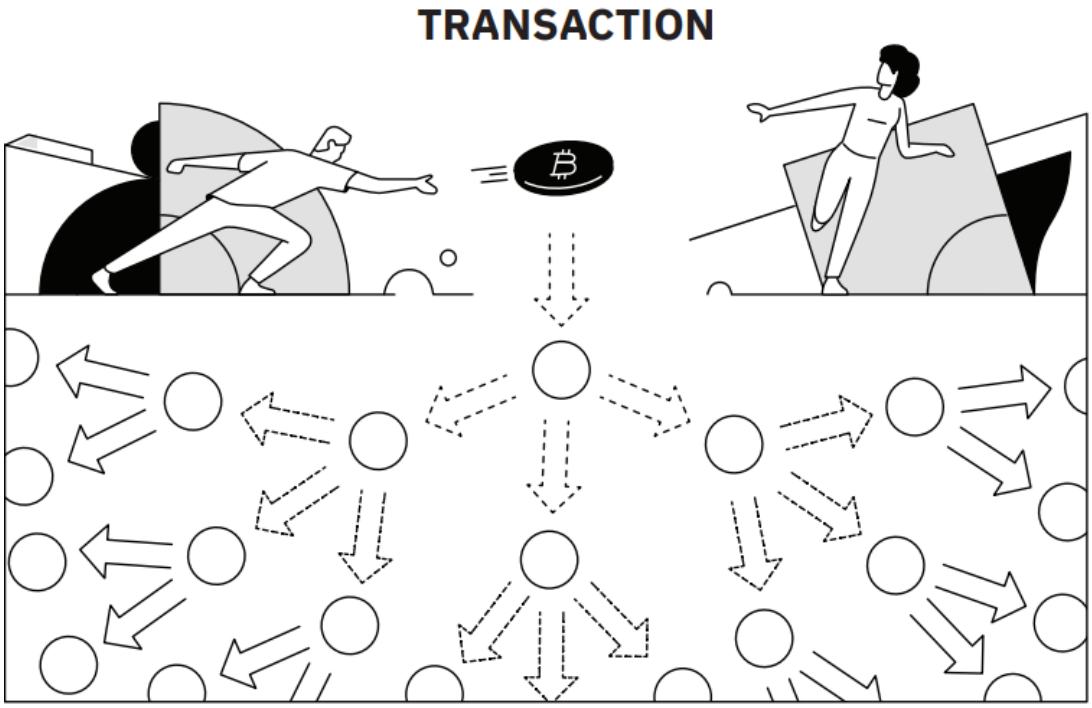
Proof of Work (často zkracováno jako PoW) představuje mechanismus, který slouží k prevenci dvojitých útrat, ke kterým dochází, když jsou stejné prostředky utraceny víc než jednou. PoW je využíván většinou dominantních kryptoměn. Tuto metodu také označujeme jako algoritmus konsenzu(dohody), který zajišťuje bezpečnost účetní knihy dané kryptoměny.

Proof of Work je prováděn pomocí procesu známého jako těžba, kde účastníci sítě, nazývaní těžaři, soutěží o právo na potvrzování transakcí. Klíčovým prvkem tohoto mechanismu je vynucování výpočetní práce, které zahrnuje proces generování hashů, nikoli řešení složitých matematických problémů, jak se často mylně uvádí. Těžaři vytvářejí nové bloky do blockchainu pomocí speciálních počítačových zařízení, která jsou optimalizována pro rychlé výpočty hashů. Vyšší hashrate, tedy více hashů za sekundu, znamená vyšší pravděpodobnost úspěchu při těžbě. Pokud je hodnota hashů nižší než obtížnost sítě, těžař, který navrhl blok, vyhrává. V opačném případě těžař pokračuje v dalších výpočtech hashů. Úspěšný blok je pak přidán do blockchainu a těžař je odměněn nově vydanými bitcoiny za svou práci.

Cílem Proof of Work je zajistit, že většina těžební síly v síti pracuje na potvrzování platných transakcí a zároveň brání potenciálním útočníkům v manipulaci s blockchainem. Tímto způsobem přispívá k bezpečnosti a důvěryhodnosti kryptoměnové sítě. [10]

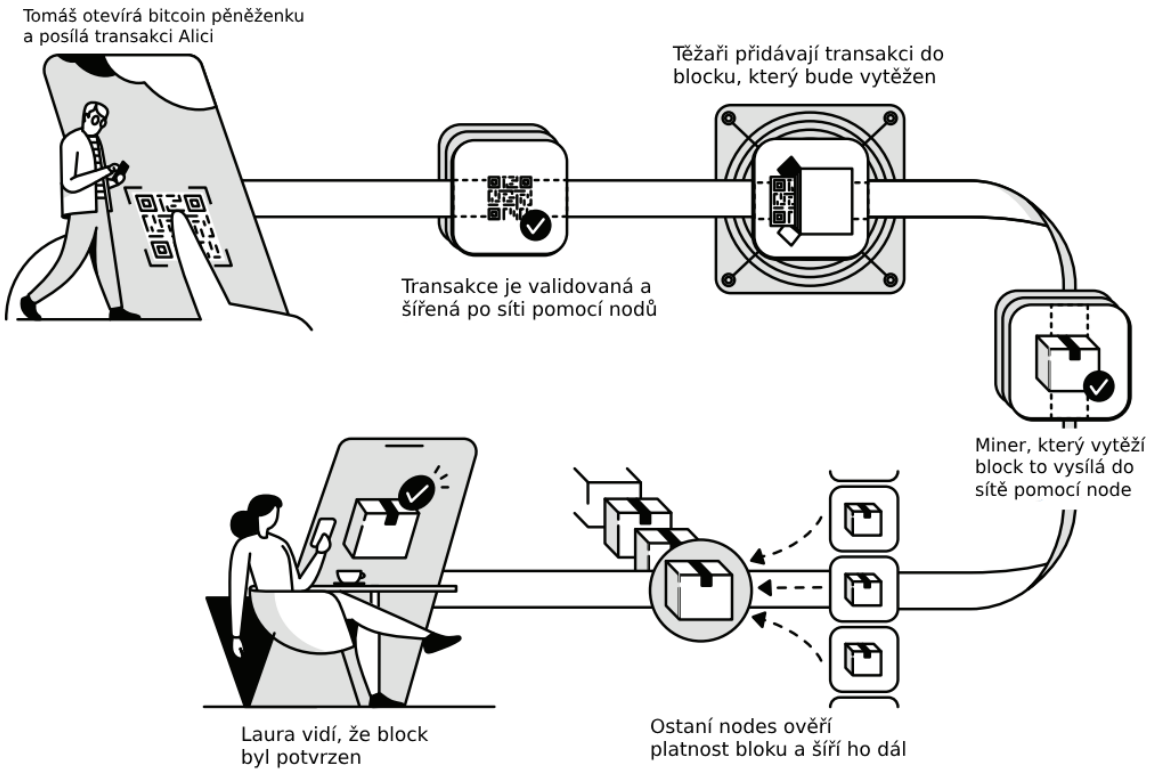
Existují 2 hlavní uzly, Full Node a Miner Node. Full node jsou uzly, které ověřují platnost transakcí a udržují kompletní historii všech transakcí v blockchainu. Zajišťují

dodržování pravidel sítě a odmítají neplatné transakce. Dále udržují kompletní kopii blockchainu, který postupně aktualizují, což jim umožňuje ověřovat nové transakce a bloky. Tím, že dodržují a prosazují pravidla sítě, uzly hrají klíčovou roli při zajištění konsensu v síti. Provoz těchto uzlů nepřináší konkrétní finanční odměnu, ale jeho energetická náročnost je relativně nízká.



Obrázek 1: Nodes šířící informace o provedené transakci (Zdroj: Bitcoin Mining Handbook) [1]

Miner node je naopak těžařský uzel, který slouží k těžbě nových bloků a zabezpečení sítě. Jeho hlavní účel je propojit blockchain s těžícími zařízeními, které spotřebovávají hodně energie. Za svou práci jsou odměňováni nově vytvořenými kryptoměnami a poplatky za transakce uvnitř sítě. [1]



Obrázek 2: Vizuální zobrazení transakce bitcoinu (Zdroj: Bitcoin Mining Handbook) (1)

Zde je vidět průběh proof of work transakce u bitcoinu. Uživatel, který chce poslat bitcoin vytváří transakci ve své peněžence. Tato transakce obsahuje informace o tom, kolik bitcoinů se posílá, na jakou adresu a případně další metadata. Odesílatel použije svůj privátní klíč k podpisu této transakce. Privátní klíč je důležitý, protože pouze ten, kdo má přístup k privátnímu klíči, může poslat bitcoiny z příslušné adresy. Podpis zajišťuje, že transakce je legitimní a pochází od vlastníka příslušného účtu. Po podpisu se transakce šíří po síti bitcoinových nodů. Tyto nody jsou počítače připojené k síti bitcoin a spolupracují při šíření a ověřování transakcí. Těžaři se v síti bitcoinu snaží potvrdit transakci a začlenit ji do bloku. Tento proces se nazývá těžba. Během těžby jsou nové transakce seskupeny do bloku, který je poté přidán do blockchainu. K ověření transakce je zapotřebí souhlas většiny nodů v síti. To znamená, že alespoň 51 % nodů musí potvrdit platnost transakce. Potvrzení zajišťuje, že transakce je legitimní a že nelze zneužít systém pro vytváření falešných transakcí. (1)

5.2.2 Proof of Stake

Proof of Stake (PoS) představuje alternativní mechanismus konsenzu v blockchainových sítích. Na rozdíl od PoW, který klade důraz na výpočetní práci a těžbu, PoS upřednostňuje držení a vlastnictví kryptoměny. Účastníci sítě mají možnost

vytvořit nebo potvrdit bloky na základě množství kryptoměny, kterou vlastní a dočasně "uzamknu" jako záruku. Čím větší je podíl kryptoměny, tím vyšší je pravděpodobnost, že budou vybráni k vytvoření nebo ověření bloku a obdržení odměny. To odstraňuje potřebu výpočetní práce a těžby, což může být energeticky efektivnější než PoW. Odměny jsou udělovány v podobě poplatků za transakce nebo nově vytvořených kryptoměn, a to podle podílu kryptoměny, kterou uživatelé uzamkli. Tím, že snižuje důraz na výpočetní výkon a těžbu, může představovat udržitelnější a ekologičtější alternativu. Některé blockchainové projekty, včetně Ethereum, zkoumají a implementují PoS jako součást svých aktualizací, aby zlepšily efektivitu svých sítí. [9]

5.2.3 51% Útok

51% útok, známý také jako "většinový útok," je situace, kdy útočník získá kontrolu nad většinou výpočetní síly nebo těžebního výkonu v blockchainové síti kryptoměny. Tato většina umožňuje útočníkovi ovlivňovat a manipulovat s běžnými aspekty provozu sítě, včetně potvrzování neplatných transakcí a vytváření nových bloků.

Klíčovým prvkem většinového útoku je schopnost útočníka provádět tzv. "double-spending" (dvojí utrácení). To znamená, že útočník může odeslat určitý počet kryptoměn na určitou adresu a poté zahájit 51% útok, který mu umožní zpětně odvolat tuto transakci a znovu utratit stejné kryptoměny. Tím vzniká riziko zneužití systému a narušení důvěryhodnosti a bezpečnosti kryptoměny.

Je důležité si uvědomit, že 51% útok vyžaduje značné množství těžebního výkonu a zdrojů, což je obvykle nákladné a obtížně dosažitelné. Většina kryptoměn s vysokou kapitalizací a dostatečnou decentralizací má dostatečná opatření k prevenci a odhalení 51 % útoků.[8]

5.3 Typy těžby

Před samotným spuštěním procesu těžby je zásadní určit optimální a nejefektivnější způsob těžby v souladu s potřebami uživatele. V této části se podrobně zaměříme na různé typy těžby a jejich charakteristiky, abychom vám poskytli ucelený pohled na toto rozmanité pole. Od tradičního softwaru až po inovativní cloudové služby, každá metoda má své výhody a omezení, která je důležité zvážit při rozhodování o těžební strategii.

5.3.1 Program

Těžba pomocí softwaru je jedním z nejběžnějších způsobů těžby kryptoměn. Využívá se specializovaného softwaru, který využívá výpočetního výkonu počítače nebo speciálního zařízení. Jedním z hlavních faktorů úspěchu této metody je správný výběr softwaru, který je kompatibilní s vaším hardwarovým vybavením a kryptoměnou, kterou chcete těžit. Existuje široká škála softwaru s různými funkcemi a možnostmi přizpůsobení, takže je důležité provést důkladné průzkumy a testy, abyste našli tu nejlepší volbu pro vaše potřeby. Výhodou těžby pomocí softwaru je možnost zapojit se do těžby s relativně nízkými náklady a bez potřeby specializovaného hardwaru, jako je tomu u těžebních stanic. To umožňuje širšímu spektru uživatelů vstoupit do světa těžby kryptoměn. Nicméně je důležité si uvědomit, že těžba pomocí softwaru může být náročná na výpočetní vybavení počítače a vyžaduje stabilní internetové připojení. Navíc s rostoucí obtížností těžby a konkurencí na trhu se může stát, že bude stále obtížnější dosahovat vysokých zisků prostřednictvím této metody.

5.3.2 Těžební stanice

Těžební stanice představuje jednu z pokročilých forem těžby kryptoměn, která využívá specializovaného hardwaru navrženého speciálně pro účely těžby. Tyto stanice jsou často složeny z výkonných grafických karet nebo speciálních integrovaných obvodů (ASIC), které jsou optimalizovány pro těžbou kryptoměn. Kromě toho obsahují základní desku, standardní komponenty, jako je procesor, paměť RAM a úložiště. Jednou z hlavních výhod těžebních stanic je jejich vysoká účinnost a výkon ve srovnání s běžnými počítači. Díky specializovanému hardwaru jsou schopny dosahovat vyššího výpočetního výkonu při snížené spotřebě energie, což v konečném důsledku přispívá k vyšším ziskům a nižším provozním nákladům. Další výhodou těžebních stanic je možnost jejich škálování. Uživatelé mohou postupně rozšiřovat svou těžební kapacitu přidáváním dalších grafických karet nebo ASIC čipů do svých stanic, což umožňuje flexibilní přizpůsobení těžebního provozu aktuálním potřebám a tržním podmínkám. Nicméně, nákup a provoz těžební stanice může být nákladný a vyžaduje investici do specializovaného hardwaru a infrastruktury. Navíc, s rychlým vývojem technologií v oblasti těžby kryptoměn, může dojít k rychlé zastarání hardware, což vyžaduje pravidelnou aktualizaci a modernizaci těžebních stanic.[23]

5.3.3 Cloud služba

Cloud služba představuje moderní a stále populárnější způsob těžby kryptoměn, který využívá pronájem výpočetního výkonu. Tento model těžby umožňuje uživatelům přistupovat k výpočetním prostředkům a těžebním algoritmům prostřednictvím internetu, bez nutnosti vlastnit fyzický hardware. Jednou z hlavních výhod cloudové služby je eliminace potřeby investovat do drahého hardwaru a infrastruktury, což může výrazně snížit počáteční náklady a rizika spojená s technologickou zastaralostí. Další výhodou je flexibilita a škálovatelnost, kterou cloudová služba poskytuje. Uživatelé mohou snadno přizpůsobit svou těžební kapacitu podle aktuálních potřeb a podmínek na trhu bez nutnosti fyzických úprav infrastruktury. To umožňuje efektivní využití zdrojů a optimalizaci výkonu těžby. Tyto služby mají své farmy umístěny v oblastech s nízkou cenou elektřiny. Nicméně, cloudová těžba není bez omezení a rizik. Jedním z hlavních rizik je závislost na poskytovateli cloudových služeb a spolehlivosti jejich infrastruktury a služeb. Výpadky služeb nebo bezpečnostní incidenty mohou mít významný dopad na těžební operace a zisky uživatele. Kromě toho může být cloudová těžba citlivá na změny cen energie nebo cen kryptoměn, což může ovlivnit celkovou rentabilitu této metody. [23]

5.3.4 Ekologické dopady těžby

Proces těžby vyžaduje obrovské množství elektrické energie. Hlavním zdrojem energie pro těžaře kryptoměn jsou fosilní paliva, přičemž uhelná energie tvoří 45 % energetického mixu. To vede k masivní produkci skleníkových plynů, přispívajících k globálnímu oteplování. V průběhu těžby kryptoměn se vypouští obrovské množství emisí oxidu uhličitého, což má negativní dopad na životní prostředí. Výpočetně náročný proces těžby vyžaduje velké množství elektřiny, což vede ke zvýšené spotřebě energie a tím i k vyšší produkci skleníkových plynů. Například, těžba Bitcoinu v roce 2020 a 2021 vedla k emisím více než 85,89 milionů tun CO2eq, což je ekvivalentem spálení 84 miliard tun uhlí, 190 elektráren spalujících zemní plyn nebo přes 25 milionů tun skládkovaných odpadů. K tomu, aby byly tyto emise vykompenzovány, by bylo třeba zasadit přibližně 3,9 miliardy stromů, což by zabralo plochu téměř rovnající se ploše zemí jako Nizozemsko, Švýcarsko nebo Dánsko, nebo 7 % Amazonie. V kontextu energetické náročnosti lze porovnat těžbu Bitcoinu s elektrickou spotřebou celých zemí. Například roční spotřeba elektřiny pro těžbu Bitcoinu přesahuje spotřebu elektrické energie celého Česka, což je více než 62 terawatthodin ročně. Podobně,

globální spotřeba elektřiny pro těžbu Bitcoinu v roce 2023 byla odhadnuta na více než 120 terawatthodin, což je více než spotřeba mnoha rozvojových zemí po celý rok. Tyto dopady jsou znepokojivé, růst trhu s kryptoměnami zůstává nekontrolovaný a jeho environmentální náklady jsou často opomíjeny. Celkově je tedy potřeba provést komplexní hodnocení environmentálních dopadů trhu s kryptoměnami a vyvinout opatření, která minimalizují tyto dopady a přispívají k udržitelnější budoucnosti digitální ekonomiky. [24]

5.4 Těžební zařízení

V oblasti těžby kryptoměn existuje několik specifických zařízení, každé s vlastními charakteristikami a využitím. Tyto těžební nástroje se vyvíjejí v souladu s technologickým pokrokem a měnícími se potřebami těžařské komunity. Níže jsou popsána klíčová těžební zařízení:

5.4.1 Procesor

V současné době je patrný ústup popularity těžby pomocí procesoru (CPU) u většiny kryptoměn. I když dříve bylo možné tímto způsobem generovat zisk, stává se to stále méně efektivním kvůli nárůstu náročnosti. Existují stále kryptoměny, jako je Monero, které umožňují těžbu pouze pomocí CPU. Nicméně, v porovnání s GPU a ASIC, procesory nabízejí nižší výkon a efektivitu při těžbě kryptoměn. To je částečně způsobeno jejich obecným zaměřením na širokou škálu úloh a nedostatkem specializace na těžební operace. Procesory jsou také náchylnější k vyšším nákladům na energii ve srovnání s GPU a ASIC. Navzdory tomu zůstávají procesory flexibilním řešením. [30]

5.4.2 Grafická karta

Grafická karta (GPU) se stala jedním z nejběžnějších nástrojů pro těžbu kryptoměn, zejména v době, kdy byla těžba pomocí CPU překonána. GPU je schopna provádět paralelní výpočty potřebné pro těžbu efektivněji než CPU, což umožňuje těžařům dosáhnout vyššího výkonu a zisků. Grafické karty mají také výhodu široké dostupnosti a flexibility, což umožňuje uživatelům snadněji rozšiřovat svou těžební kapacitu přidáním dalších karet do svých systémů.[30]

5.4.3 Hradlové pole

Hradlové pole (FPGA) představuje další formu těžebního zařízení, které se stalo populární pro některé specifické aplikace. FPGA je programovatelný integrovaný obvod, který může být upraven k provádění určitých úloh, včetně těžby kryptoměn. FPGA nabízí vyšší výkon a energetickou efektivitu než CPU a GPU, a zároveň umožňuje uživatelům určitou míru flexibility při optimalizaci svých těžebních operací. Přestože FPGA není tak široce dostupné jako GPU a ASIC, nachází své uplatnění především v profesionálních těžebních farmách. Použití hradlových polí pro těžbu vyžaduje pokročilou schopnost programování. (30)

5.4.4 ASIC

Aplikačně specifické integrované obvody (ASIC) jsou považovány za vrchol efektivity a výkonu v oblasti těžby kryptoměn. Tyto speciálně navržené čipy jsou optimalizovány přímo pro provádění konkrétních těžebních algoritmů a poskytují extrémně vysoký výkon při minimální spotřebě energie. ASIC je běžně používán pro těžbu kryptoměn, jako je Bitcoin, která vyžaduje extrémně vysokou výpočetní sílu pro efektivní těžbu. Jednou z hlavních výhod ASIC je jeho specializace na konkrétní algoritmy, což umožňuje dosahovat vysokých hashovacích rychlostí a zisků. Přestože je z ekonomického hlediska přívětivější, je také náchylný k technologické zastaralosti a není flexibilní jako GPU, CPU nebo FPGA, protože se nedá použít na nic jiného než na těžbu kryptoměn, což může být problém v případě, že se algoritmus změní nebo zastará. Pořízení těchto zařízení také zahrnuje vysoké investiční náklady, které mohou dosáhnout až na statisíce korun. (30)

5.4.5 Mining pool

Těžební bazén, někdy nazývaný i mining pool, je skupina těžařů, kteří spojují své síly a zdroje k dosažení společného cíle - těžby kryptoměn. Jednotliví těžaři přidávají svůj výpočetní výkon do společného bazénu a společně potvrzují transakce na blockchainu. Když je blok úspěšně těžen, odměna je rozdělena mezi všechny členy těžebního bazénu podle jejich příspěvku výpočetního výkonu. Tímto způsobem mají těžaři vyšší pravděpodobnost pravidelného získávání odměn, než kdyby těžili samostatně.

Těžební bazén také pomáhá vyrovnat rozdíly ve výkonnosti mezi jednotlivými těžaři a zvýšit decentralizaci těžby, protože i menší těžaři mohou přispět k těžbě a získávat odměny. (1)

5.4.6 Neautorizovaná těžba

Typicky pod anglickým názvem cryptojacking – představuje kybernetický útok, kdy útočníci neoprávněně využívají výpočetního výkonu počítačů či jiných zařízení k těžbě kryptoměn bez vědomí či souhlasu uživatele. Tento fenomén se skládá ze dvou hlavních metod, konkrétně malwarového cryptojackingu a webového cryptojackingu. V případě malwarového cryptojackingu využívají útočníci škodlivý software, který infikuje počítače nebo webové stránky. Tento malware operuje na pozadí systému a tajně provádí těžbu kryptoměn, přičemž získává odměny v podobě nově vytvořených mincí. Ovlivnění uživatelé to zpravidla nezaznamenají, což zvyšuje riziko neoprávněného využívání jejich výpočetního výkonu.

V webovém cryptojackingu pak útočníci vkládají škodlivý kód přímo do webových stránek, které navštěvují uživatelé. Tento kód je schopen využívat výpočetní sílu návštěvníků k těžbě kryptoměn, aniž by byli o této činnosti informováni. Uživatelé jsou tak nechtěně zapojeni do procesu těžby, což představuje závažné bezpečnostní riziko.[7]

5.5 Algoritmy těžby

V této části se zaměříme na podstatné algoritmy v oblasti těžby kryptoměn, které stojí v základu blockchainových sítí. Tyto algoritmy nejen umožňují fungování digitálních měn, ale také definují mechanismy, které zajišťují bezpečnost a decentralizaci sítě.

5.5.1 SHA-256

SHA-256, neboli Secure Hash Algorithm 256-bit, je kryptografická hashovací funkce běžně používaná v blockchainových sítích jako je Bitcoin. V těžbě Bitcoinu slouží SHA-256 jako základ pro generování jedinečného identifikátoru (hash) pro každý potenciální blok transakcí. Těžaři soutěží o nalezení nonce (náhodného čísla), které, když je spojeno s blokovými daty vytvoří hash, který splňuje cílový požadavek obtížnosti sítě.

Zjednodušeně řečeno, představte si těžaře jako jednotlivce v kasinu, kteří házejí kostkou. Každý hod představuje jeden pokus o vytvoření hash hodnoty. Cílem je hodit číslo pod určený práh (například hodit méně než 10 s kostkou s 1000 stranami). Čím více hodů (pokusů o hash) za sekundu, tím vyšší šance na úspěch. Jakmile těžař najde nonce hodnotu pod obtížnostním cílem, vyhrává kolo a navrhuje nový blok sítě. Tento proces vyžaduje značné množství výpočetní síly. [1]

Obtížnost síťového bloku Bitcoinu se upravuje každých 2016 bloků (~2 týdny), aby se udržel průměrný čas vytvoření bloku na 10 minut. Tato úprava zajistí, že nové bloky jsou přidávány do blockchainu konzistentním tempem, bez ohledu na změny v celkové hashovací síle sítě. Jakmile se do sítě přidává více nebo méně těžařů, obtížnost se přizpůsobí, aby udržela tento cílový čas bloku.

Celkově má SHA-256 klíčovou roli v procesu těžby tím, že poskytuje bezpečný a efektivní způsob generování jedinečných identifikátorů bloku, čímž zajišťuje bezpečnost sítě Bitcoinu a usnadňuje vydávání nových bitcoinů [6]

5.5.2 SCRYPT

Algoritmus Scrypt, používaný například v Litecoinu, se odlišuje od SHA-256 tím, že je paměťově náročnější. To znamená, že těžba vyžaduje více paměti než čistou výpočetní sílu. Tato charakteristika je implementována s cílem omezit výhody specializovaných těžebních zařízení, známých jako ASICs. Scrypt tím zvyšuje přístupnost k těžbě pro běžné počítače s dostatečnou pamětí. [38]

5.5.3 Ethash

Jedná se o Proof of Work algoritmus používaná pro těžbu Ethereum a kryptoměny založené na Ethereum síti. Jedná se o modifikovanou verzi algoritmu Dagger-Hashimoto, která je odolná proti ASIC a efektivně ověřitelná. Ethash používá rozsáhlou datovou sadu, která se postupně rozšiřuje, ale vejde se do VRAM starého GPU. Jeho cílem je generovat hash hodnotu menší než stanovený práh, nazývaný obtížnost. Tím řídí rychlost těžby bloků v síti Ethereum. Těžaři obdrží odměny za těžbu bloků a za přidání pomocných bloků do blockchainu. Ethash algoritmus poskytuje těžařům představu o potřebných výpočetních zdrojích a umožňuje generování jednoho bloku každých 12 sekund. [4]

5.5.4 RandomX

RandomX je algoritmus, který zdůrazňuje efektivitu na běžných CPU. Používá se především v kryptoměnách, jako je Monero. Cílem RandomX je snížit vliv specializovaných těžebních zařízení a zároveň umožnit těžbu pomocí běžných procesorů.[5]

5.5.5 Equihash

Equihash je hashovací algoritmus používaný v různých blockchainových sítích s Proof of Work (PoW). Byl vytvořen jako reakce na rostoucí centralizaci těžby způsobenou ASIC těžebními stroji. Jeho klíčovou vlastností je "paměťová náročnost", což znamená, že vyžaduje velké množství paměti pro generování důkazu, což ztěžuje vytváření specializovaných těžebních zařízení, to pomáhá udržovat těžbu decentralizovanou a zabraňuje vytváření monopolů ve těžebním odvětví. Navíc, Equihash je efektivní při odolávání různým útokům, jako je 51% útok, díky čemuž zvyšuje bezpečnost blockchainové sítě. Díky těmto vlastnostem se Equihash stal preferovanou volbou pro projekty, které chtějí udržet decentralizaci a zvýšit odolnost vůči útokům. [3]

5.5.6 KAWPOW

Tento algoritmus je chráněn proti ASIC těžbě a potenciální centralizaci. Pro dosažení tohoto zabezpečení vývojáři střídají algoritmy X15 a SHA51. Jejich volba závisí na hashy předchozího bloku. KAWPOW algoritmus se proto vynikajícím způsobem osvědčuje na grafických kartách. Pokud jde o těžbu pomocí algoritmu KAWPOW, jsou NVIDIA grafické karty lepší. [32]

5.6 Těžební software

Těžební software představuje klíčový nástroj pro těžbu kryptoměn, který umožňuje uživatelům spravovat a optimalizovat svůj těžební hardware pro získávání kryptoměnových odměn. Existuje mnoho různých programů pro těžbu, z nichž každý má své vlastní jedinečné vlastnosti a funkce. Níže jsou uvedeny některé z nejznámějších těžebních softwarů:

5.6.1 Nicehash Miner

Specializovaný software navržený pro těžbu kryptoměn, který patří mezi nejpoužívanější platformy svého druhu. Poskytuje uživatelům jednoduché a efektivní prostředí pro správu jejich těžebního hardwaru. NiceHash Miner je optimalizován pro různé typy těžebního hardware, včetně GPU,CPU a ASIC. Nabízí jednoduché uživatelské prostředí a přednastavené nastavení pro maximální efektivitu těžby. [40]

5.6.2 CGMiner

CGMiner je jedním z nejstarších a nejuznávanějších softwarů pro těžbu kryptoměn, zejména Litecoinu. Vyvinut byl v roce 2011 australským programátorem Conem

Kolivasem pro těžbu Bitcoinu a Litecoinu. Díky otevřenému zdroji, jednoduchému rozhraní a kompatibilitě s různými platformami a hardwarem patří mezi špičku těžebního softwaru.

CGMiner používá příkazový řádek pro ovládání těžebního procesu, což umožňuje dálkové řízení zařízení a nastavení ventilátorů. Nabízí pokročilou detekci nových bloků a snadné škálování výkonu těžby. Ačkoliv je určen zejména pro Linux, funguje také na Windows a Mac OS. Je napsán v jazyce C a je kompatibilní s různým těžebním hardwarem jako FPGAs, GPU a CPU. (11)

5.6.3 GMiner

GMiner je těžební software, který je primárně určen pro těžbu pomocí GPU. Tento software je oblíbený pro svou vysokou účinnost a stabilitu a podporuje širokou škálu těžebních algoritmů, včetně těch nejnovějších a nejvýnosnějších. (40)

5.6.4 T-rex

T-rex je další těžební software zaměřený na těžbu pomocí GPU, konkrétně na karty NVIDIA. Tento software je oblíbený pro svou jednoduchost a vysoký výkon a podporuje širokou škálu těžebních algoritmů, včetně těch používaných pro těžbu kryptoměn, jako je Ethereum. (40)

5.6.5 HiveOS

HiveOS je operační systém založený na Linuxu, který je navržen speciálně pro těžbu kryptoměn. Tento systém umožňuje těžařům snadněji spravovat a monitorovat své těžební operace prostřednictvím uživatelsky přívětivého rozhraní. HiveOS nabízí nástroje pro vzdálenou správu, sledování výkonu a spotřeby energie, a také automatickou optimalizaci těžebních nastavení pro zvýšení ziskovosti.

5.6.6 Minerstat

Minerstat je další platforma zaměřená na těžbu kryptoměn, avšak na rozdíl od Hiveon OS se Minerstat zaměřuje na poskytování rozsáhlých analytických a správcovských nástrojů pro těžaře. Tato platforma umožňuje uživatelům monitorovat a spravovat své těžební operace z jednoho centrálního rozhraní. Minerstat poskytuje rozšířené analytické nástroje a reporty, které pomáhají uživatelům porozumět výkonu jejich těžebních operací a identifikovat oblasti pro zlepšení. Kromě toho nabízí automatickou

optimalizaci těžebních nastavení, která zahrnuje dynamické přizpůsobení nastavení podle aktuálních podmínek na trhu a síti kryptoměn.

Podobně jako konkurenční platformy, i Minerstat umožňuje vzdálenou správu těžebních zařízení a sledování jejich výkonu. Díky tomu uživatelé mohou efektivně řídit své těžební farmy z jednoho centrálního místa. Platforma je navržena tak, aby podporovala širokou škálu kryptoměn, což umožňuje uživatelům těžit různá digitální aktiva podle jejich preference a aktuálních tržních podmínek.

Bezpečnostní funkce jsou také důležitou součástí Minerstatu, který klade důraz na ochranu těžebních operací před hrozbami jako jsou útoky na síťovou bezpečnost nebo zneužití těžebního hardwaru. Celkově lze říci, že Minerstat poskytuje komplexní prostředí pro správu těžebních operací, které umožňuje uživatelům efektivněji a bezpečněji těžit kryptoměny.

5.7 Historie grafických karet v těžbě kryptoměn

Historie grafických karet v těžbě kryptoměn sahá až k prvním krokům digitálních měn, zejména s nástupem Bitcoinu v roce 2009. V té době byly k těžbě využívány běžné procesory (CPU), avšak brzy se ukázalo, že grafické karty (GPU) nabízejí mnohem vyšší výpočetní výkon a energetickou efektivitu.

Od roku 2010 se grafické karty staly středem pozornosti v oblasti těžby kryptoměn. Jejich schopnost paralelního zpracování umožnila těžařům generovat nové mince a zabezpečit transakce na blockchainu s větší účinností než kdy předtím. S nástupem dalších kryptoměn, jako je Ethereum, Litecoin a další, grafické karty se staly nezbytnou součástí těžební infrastruktury.

Historie grafických karet v těžbě kryptoměn je rovněž plná významných milníků a technologických inovací. Tyto karty neustále procházejí vývojem, přičemž se jejich výkon a efektivita stále zvyšuje. S rozvojem trhu s kryptoměnami a technologií GPU těžby se očekává, že grafické karty budou hrát stále významnější roli v ekosystému digitálních měn.[31]

5.8 Architektura a specifikace grafických karet pro těžbu

Architektura a specifikace grafických karet určených pro těžbu kryptoměn jsou klíčovými faktory, které ovlivňují jejich těžební výkon a efektivitu. Tyto karty se liší od běžných herních nebo kancelářských GPU svými specifickými vlastnostmi, které jsou optimalizovány pro vysoký výkon a nízkou spotřebu energie při těžbě.

Jedním z klíčových prvků těchto karet je množství stream procesorů, jako jsou CUDA jádra u NVIDIA nebo Stream procesory u AMD. Tyto procesory umožňují provádět mnoho výpočetních operací paralelně, což je zásadní pro efektivní těžbu kryptoměn.
Další důležitou specifikací je paměťová kapacita karty, která ovlivňuje schopnost těžit kryptoměny s vysokou paměťovou náročností, jako je Ethereum. Čím větší paměť má karta, tím lépe si dokáže poradit s náročnými těžebními algoritmy.
Spotřeba energie, výpočetní výkon a chlazení jsou další klíčové faktory, které ovlivňují výkon grafických karet při těžbě kryptoměn. Optimalizace těchto prvků je klíčová pro dosažení co nejvyššího těžebního výkonu a efektivity. (48)

5.9 Technologické inovace a výkon těžebních grafických karet

Technologické inovace v oblasti těžebních grafických karet přinesly revoluční změny v oblasti těžby kryptoměn. Jednou z nejvýznamnějších inovací bylo zavedení speciálních těžebních karet, které nabízejí optimalizované vlastnosti pro těžbu digitálních měn.
Například NVIDIA a AMD vyvinuly speciální řady grafických karet určených výhradně pro těžbu kryptoměn. Tyto karty často nabízejí vylepšené stream procesory, vyšší paměťovou kapacitu a efektivnější chlazení než běžné herní karty.
Další technologické inovace zahrnují zlepšené výrobní procesy, které umožňují výrobu grafických karet s vyšším výkonem a nižší spotřebou energie. Kromě toho se také objevují nové těžební algoritmy optimalizované pro konkrétní typy grafických karet, což dále zvyšuje jejich efektivitu při těžbě různých kryptoměn. (46) (41)

5.10 Porovnání výkonu a optimalizace grafických karet pro těžbu

Porovnání výkonu grafických karet pro těžbu kryptoměn je nezbytné pro správný výběr vhodného zařízení.
Jak už bylo řečeno, těžební výkon grafických karet je obvykle měřen v hashovacích operacích za sekundu (hashrate). Tato hodnota udává, kolik hashů může karta vygenerovat za jednu sekundu při těžbě určité kryptoměny. Výkon karty je ovlivněn její architekturou, technickými specifikacemi a optimalizacemi ovladačů a softwaru.
Optimalizace grafických karet pro těžbu zahrnuje aktualizace ovladačů a softwaru, nastavení těžebních parametrů a správné chlazení zařízení. Správná optimalizace může významně zvýšit těžební výkon a efektivitu karty. (48)

5.11 Výběr vhodné grafické karty pro těžební potřeby

Při výběru vhodné grafické karty pro těžbu kryptoměn je důležité zvážit několik faktorů, včetně ceny, výkonu, energetické efektivity a dostupnosti na trhu.

Některé karty nabízejí vyšší výkon za vyšší cenu, zatímco jiné jsou cenově dostupnější, ale mohou mít nižší výkon. Dále je nutné zohlednit i spotřebu energie a náklady na chlazení, které mohou ovlivnit celkové náklady na těžbu a ziskovost investice. Některé algoritmy těžby jsou lépe optimalizovány pro určité typy grafických karet. Vybrání vhodné grafické karty pro daný algoritmus může zlepšit efektivitu a ziskovost těžby.

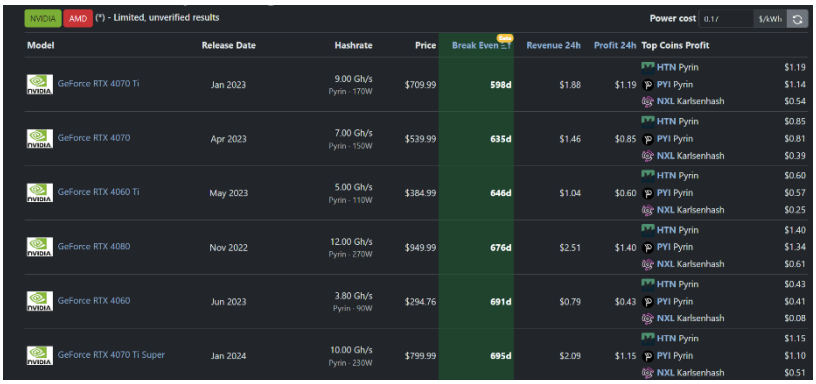
Výběr vhodné grafické karty by měl být proveden s ohledem na konkrétní požadavky a očekávání těžebního procesu, aby byla dosažena maximální efektivita a výdělečnost.[48]

6 Stavba těžební stanice

Stavba těžební stanice představuje klíčový krok pro každého, kdo se zabývá těžbou kryptoměn. Tato praktická část práce se zabývá praktickými aspekty stavby těžební stanice s důrazem na výběr a testování softwarů. Finance jsou zásadním aspektem každého projektu, a to i při stavbě těžební stanice. Zahrnují náklady na hardware, software, elektřinu, chlazení a další provozní náklady. Správné plánování financí je klíčové pro dosažení dlouhodobé udržitelnosti a rentability těžebního zařízení. je důležité zvážit finanční prostředky a předpokládanou dobu návratnosti investice. Výběr grafické karty je rozhodujícím faktorem pro úspěšnou těžbu kryptoměn. Musí být proveden s ohledem na výkon, spotřebu energie, dostupnost na trhu a návratnost investice. Existuje mnoho webových stánek, které aktivně sledují grafické karty a srovnávají je v kontextu těžby. Výběr těžené kryptoměny je rovněž klíčovým rozhodnutím. Je důležité zohlednit aktuální trendy na trhu, potenciální zisky a rizika spojená s danou měnou. Výběr softwaru pro těžbu je důležitý pro optimalizaci výkonu těžební stanice. Existuje mnoho různých programů, které mohou být použity pro těžbu různých kryptoměn, a je nezbytné vybrat ten nejvhodnější pro konkrétní potřeby a hardware.

6.1 Porovnání grafických karet

Pro usnadnění rozhodovaní je doporučené využít webové stránky s tabulkami nejpopulárnějších a nejvýkonnějších GPU pro těžbu. Jedná se o webové platformy jako whattomine.com nebo samotný nicehash.com. Tyto nástroje aktivně sledují a porovnávají vlastnosti a výkonnost různých grafických karet včetně jejich hashovací rychlosti, doporučeného algoritmu, ceny a návratnost investice, což pomáhá ve výběru a nakupování grafických karet pro těžbu kryptoměn.



Obrázek 3: Webová stránka whattomine.com s roztříděnými GPU podle návratnosti investice (Zdroj: whattomine.com)

6.2 Testování sestavy

Pro testování stability sestavy jsem zvolil program 3DMark, který je široce používaný pro testování výkonu počítačů a grafických karet. Tento program poskytuje komplexní sadu testů, které zkoumají různé aspekty výkonu, včetně grafického zpracování, fyzikální simulace a celkového výkonu a stability systému. Po dokončení testů jsem analyzoval výsledky a potvrdil, že sestava funguje bez problémů, co se týče stability a teplot.

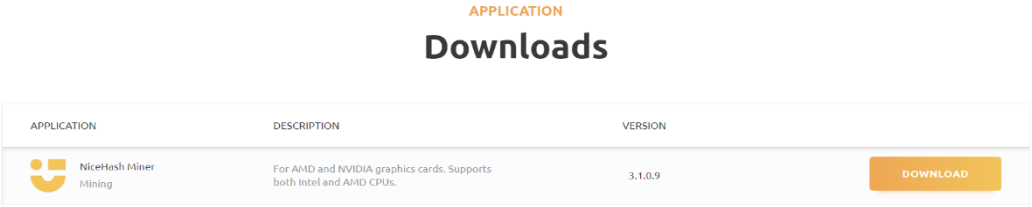
Obrázek 4: Výsledky 3DMark benchmarků (Zdroj: Autor)

6.3 Porovnání těžebního softwaru: NiceHash, CGMiner a T-rex

V rámci této části praktického testování softwaru na těžbu kryptoměn jsem se zabýval instalací, konfigurací a testováním tří široce užívaných programů pro těžbu kryptoměn na operačním systému Windows: NiceHash, CGMiner a T-rex Miner. Volba těchto softwarů byla provedena na základě hodnocení a recenzí získaných během pečlivého sledování trhu a diskusních fór, a také na základě zkušeností aktivních uživatelů v této oblasti. Cílem tohoto testování je získat srovnatelné výsledky ohledně účinnosti a spolehlivosti všech tří programů v reálných podmínkách těžby kryptoměn na platformě Windows. Následně budu tyto výsledky analyzovat a vyhodnocovat, aby bylo možné určit nejlepší možnost pro efektivní těžbu kryptoměn na dané platformě.

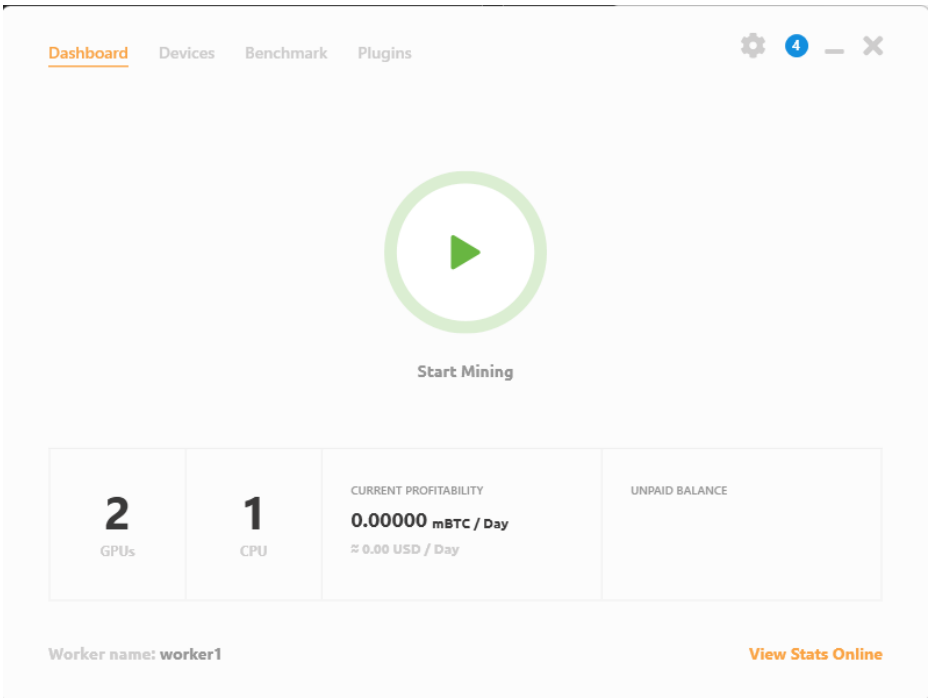
6.3.1 NiceHash

Instalace programu Nicehash je jednoduchá a uživatelsky přívětivá. Jako první krok je třeba stáhnout instalační soubor „nhm_windows_3.1.0.9.exe“ ze stránky vývojářů (www.nicehash.com).



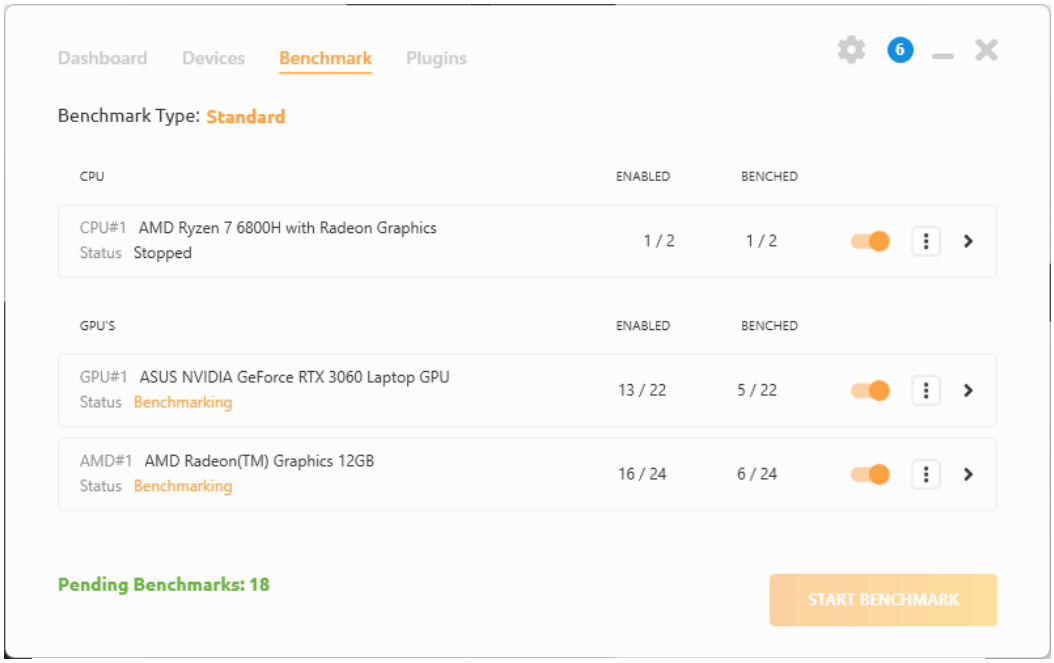
Obrázek 5: Stahování instalačního souboru NiceHash (Zdroj: Autor)

Po dokončeném stahování je třeba zapnout instalační soubor, po instalaci se zobrazí program s uživatelsky přívětivým rozhraním. Program začne automaticky detekovat nainstalovaný hardware. Následně je nutné vytvořit účet. Po úspěšné registraci a příhlášení do programu se NiceHash automaticky propojí s webovým rozhraním, čímž se počítač připraví k těžbě. Stačí pouze kliknout na tlačítko „Start mining“ a program automaticky začne benchmarkovat jednotlivé komponenty. Po dokončeném benchmarku se zapne konzole a těžba začne.



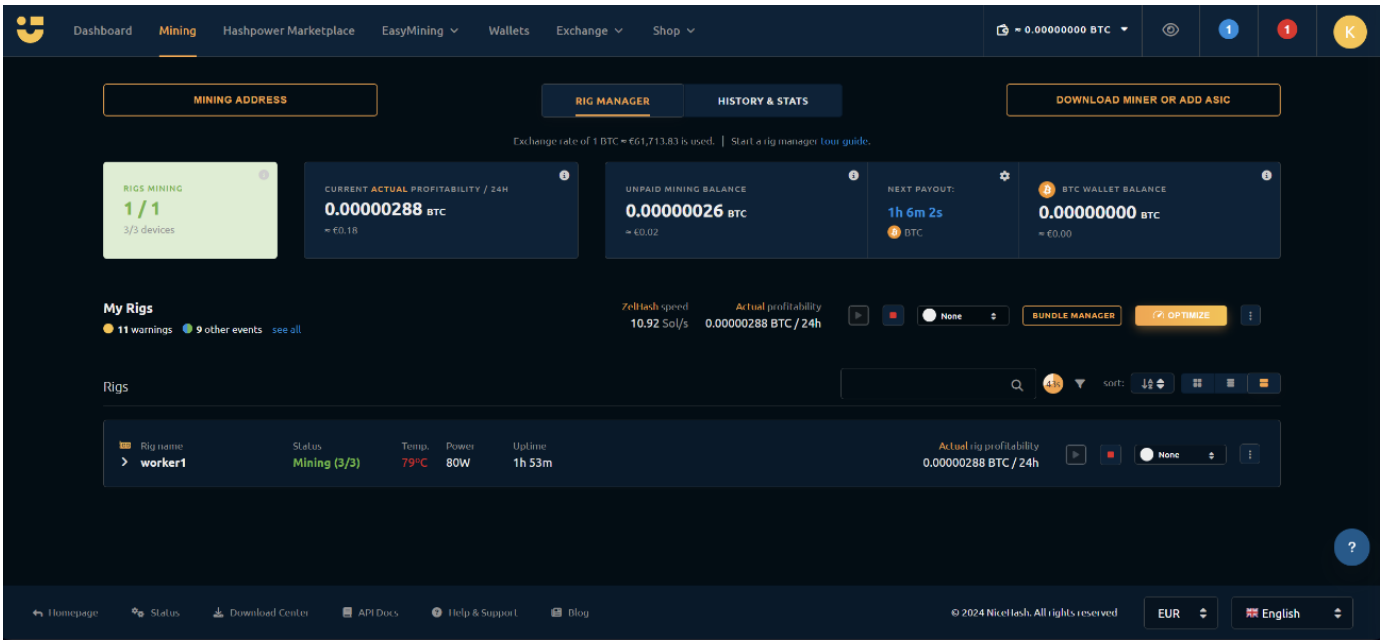
Obrázek 6: Uživatelské rozhraní programu NiceHash (Zdroj: Autor)

Při probíhajícím benchmarku jednotlivých komponentů program hledá aktuálně nejefektivnější algoritmus pro největší výdělek. Je také možné vypnout a zapnout jednotlivé komponenty nebo algoritmus pro každé zařízení



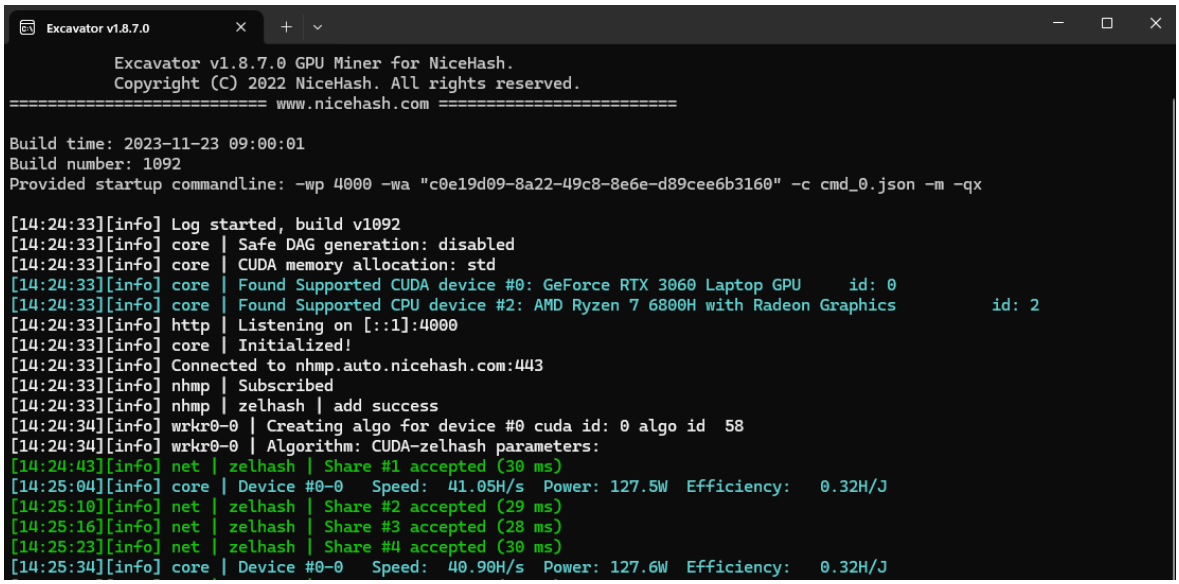
Obrázek 7: Probíhající benchmark testy v programu NiceHash (Zdroj: Autor)

NiceHash má také webové rozhraní přes které je těžbu také možné ovládat. To je velice praktické pokud bych chtěl zařízení ovládat na dálku.



Obrázek 8: Webové rozhraní Nicehash.com (Zdroj: Autor)

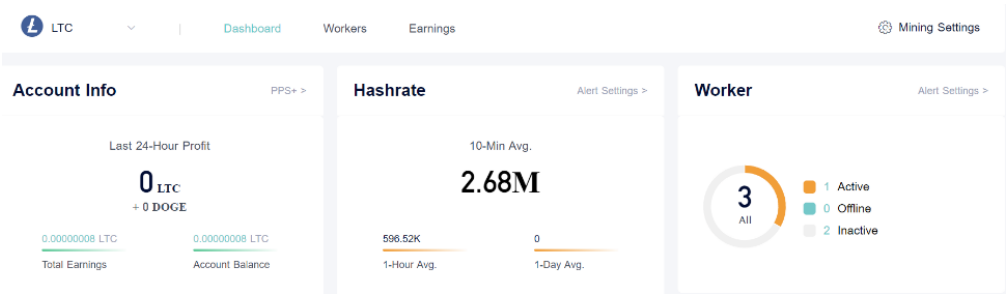
Po hotovém benchmarku se zapne konzole, kde jsou informace o aktuální těžbě



Obrázek 9: Konzole s informacemi o těžbě (Zdroj: Autor)

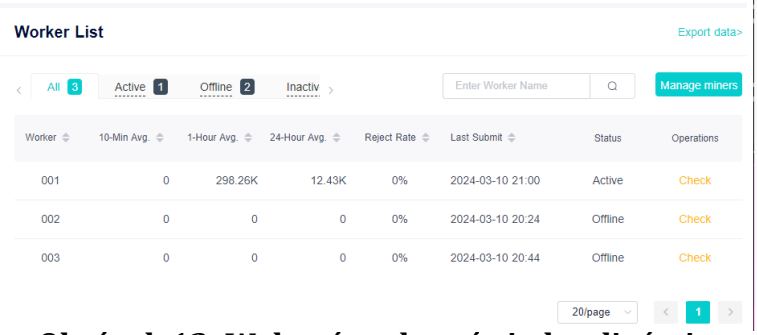
6.3.2 CGMiner

Pro úspěšné spuštění CGMineru je nezbytné správně nakonfigurovat konfigurační soubor. Je nutné předem vědet v jakém mining poolu budeme těžit a na jakou peněženku budou vypláceny odměny. Je nutné vytvořit účet u mining poolu, ve kterém budeme těžit. V tomto případě jsem vybral pool viaBTC, který jsem vybral pomocí webové stránky "https://miningpoolstats.stream". Registrace probíhala jednoduše prostřednictvím registračního formuláře na stránkách www.viabtc.com. Po úspěšném zaregistrování a přihlášení do administrace mi byli poskytnuty údaje na připojení do poolu přímo z těžebního softwaru.



Obrázek 10: Uživatelské rozhraní viaBTC poolu po připojení ze CGMineru (Zdroj: Autor)

Pro správné připojení k poolu je potřeba správné nastavení konfiguračního souboru s názvem cgminer.conf, kde je třeba zadat adresy poolu stratum+tcp:/ltc.viabtc.io:3333, jméno workera(user) a heslo(pass). Worker představuje jedno konkrétní těžební zařízení, které bude monitorováno a spravováno Je zde velká variabilita konfiguračních možností. Po spuštění souboru cgminer.exe se načte konfigurační soubor, spustí se konzole a započne připojení k poolu a těžba kryptoměn.



Obrázek 12: Webové rozhraní s jednotlivými workery a jejich aktivitou (Zdroj: Autor)

```
"pools" : [
        {
                "url" : "stratum+tcp://ltc.viabtc.io:3333",
                "user" : "xdxxxd.001",
                "pass" : "123"
        },
        {
                "url" : "stratum+tcp://ltc.viabtc.io:25",
                "user" : "xdxxxd.001",
                "pass" : "123"
        },
        {
                "url" : "stratum+tcp://ltc.viabtc.io:443",
                "user" : "xdxxxd.001",
                "pass" : "123"
        }
]
,
"intensity" : "13",
"vectors" : "1",
"worksize" : "256",
"kernel" : "scrypt",
"lookup-gap" : "0",
"thread-concurrency" : "8000",
"shaders" : "0",
"gpu-engine" : "0-955",
"gpu-fan" : "0-85",
"gpu-memclock" : "1270",
"gpu-memdiff" : "0",
"gpu-powertune" : "0",
"gpu-vddc" : "0.000",
"temp-cutoff" : "80",
"temp-overheat" : "70",
"temp-target" : "60",
"api-port" : "4028",
"auto-fan" : true,
"auto-gpu" : true,
"expiry" : "120",
"gpu-dyninterval" : "7",
"gpu-platform" : "0",
"gpu-threads" : "2",
"log" : "5",
"queue" : "1",
"scan-time" : "60",
"scrypt" : true,
"temp-hysteresis" : "3",
"shares" : "0",
"kernel-path" : "/usr/local/bin"
}
```

Obrázek 11: Konfigurační soubor cgminer.conf (Zdroj: Autor)

Popis jednotlivých konfigurací v konfiguračním souboru:

pools: Toto nastavení obsahuje seznam těžebních bazénů, ke kterým se cgminer připojuje. Každý bazén má svou vlastní adresu URL, uživatelské jméno a heslo, které slouží k ověření a účasti na těžbě v daném bazénu.

intensity: Toto nastavení určuje úroveň intenzity těžby, což ovlivňuje, jak moc jsou využity zdroje GPU. Vyšší intenzita může zvýšit rychlost těžby, ale také zvýší zátěž na hardware.

vectors: Určuje, zda jsou vektorové instrukce použity při těžbě. Vektorové instrukce mohou zvýšit výkon těžby na některých typech GPU.

worksize: Stanovuje velikost pracovního bloku, který je zpracováván GPU. Optimální velikost pracovního bloku může záviset na konkrétním hardwaru a těžebním algoritmu.

kernel: Toto nastavení specifikuje použitý hashovací algoritmus pro těžbu. V tomto případě je použit algoritmus scrypt, který je často používán pro těžbu kryptoměn jako Litecoin.

lookup-gap: Určuje, jak často jsou prováděny vyhledávání nonce v hashovacím procesu. Nastavení tohoto parametru může ovlivnit efektivitu těžby a stabilitu systému.

thread-concurrency: Stanovuje počet vláken použitých pro těžbu. Vyšší počet vláken může zvýšit rychlost těžby, ale také zvýší zátěž.

shaders: Určuje počet shaderů GPU použitých pro těžbu. Shader je součástí GPU, která provádí výpočty během těžebního procesu.

gpu-engine: Nastavuje frekvenci jádra GPU. Optimalizace frekvence jádra může mít významný vliv na výkon těžby.

gpu-fan: Určuje rychlost ventilátoru GPU. Správné chlazení je klíčové pro udržení stability a dlouhodobého provozu hardwaru.

gpu-memclock: Nastavuje frekvenci paměti GPU. Optimalizace paměťové frekvence může také ovlivnit výkon těžby.

gpu-memdiff: Specifikuje rozdíl v paměťovém taktech mezi jednotlivými GPU. Toto nastavení může být užitečné pro vyvážení zátěže mezi různými GPU v těžebním zařízení.

gpu-powertune: Toto nastavení umožňuje upravit spotřebu energie GPU. Snížení hodnoty může snížit spotřebu energie, ale také může ovlivnit výkon těžby. Naopak zvýšení hodnoty může zlepšit výkon, ale také zvýší spotřebu energie.

gpu-vddc: Určuje napětí dodávané GPU. Optimalizace napětí může pomoci dosáhnout lepší účinnosti těžby a snížit tepelnou zátěž.

temp-cutoff: Stanovuje maximální teplotu GPU, při které se těžba zastaví. Toto nastavení chrání hardware před přehřátím a poškozením.

temp-overheat: Určuje teplotu, při které se aktivuje režim přehřátí. Při dosažení této teploty se může snížit výkon GPU nebo se těžba úplně zastaví.

temp-target: Stanovuje cílovou teplotu GPU. Těžební software se snaží udržovat tuto teplotu optimalizací rychlosti ventilátoru a výkonu GPU.

api-port: Specifikuje port pro přístup k API cgmineru. To umožňuje monitorování a řízení těžebního procesu pomocí externích aplikací.

auto-fan: Určuje, zda je automatická regulace ventilátoru GPU zapnuta. Pokud je zapnuto, software automaticky upravuje rychlost ventilátoru podle teploty GPU.

auto-gpu: Specifikuje, zda jsou automatické úpravy parametrů GPU povoleny. Pokud je zapnuto, software automaticky optimalizuje nastavení GPU pro dosažení maximálního výkonu.

expiry: Určuje dobu platnosti pracovního bloku, po které je potřeba obnovit komunikaci s těžebním poolem.

gpu-dyninterval: Nastavuje interval pro dynamické změny parametrů GPU. Toto nastavení umožňuje softwaru reagovat na změny v těžebním prostředí.

gpu-platform: Specifikuje platformu GPU, pokud je k dispozici více GPU. To umožňuje vybrat, které GPU se mají používat pro těžbu.

gpu-threads: Určuje počet vláken použitých pro těžbu na jednom GPU.

log: Nastavuje úroveň detailů v logovacích zprávách. Vyšší hodnota znamená více detailů.

queue: Specifikuje velikost fronty pro odesílání a přijímání dat mezi těžebním softwarem a těžebním bazénem.

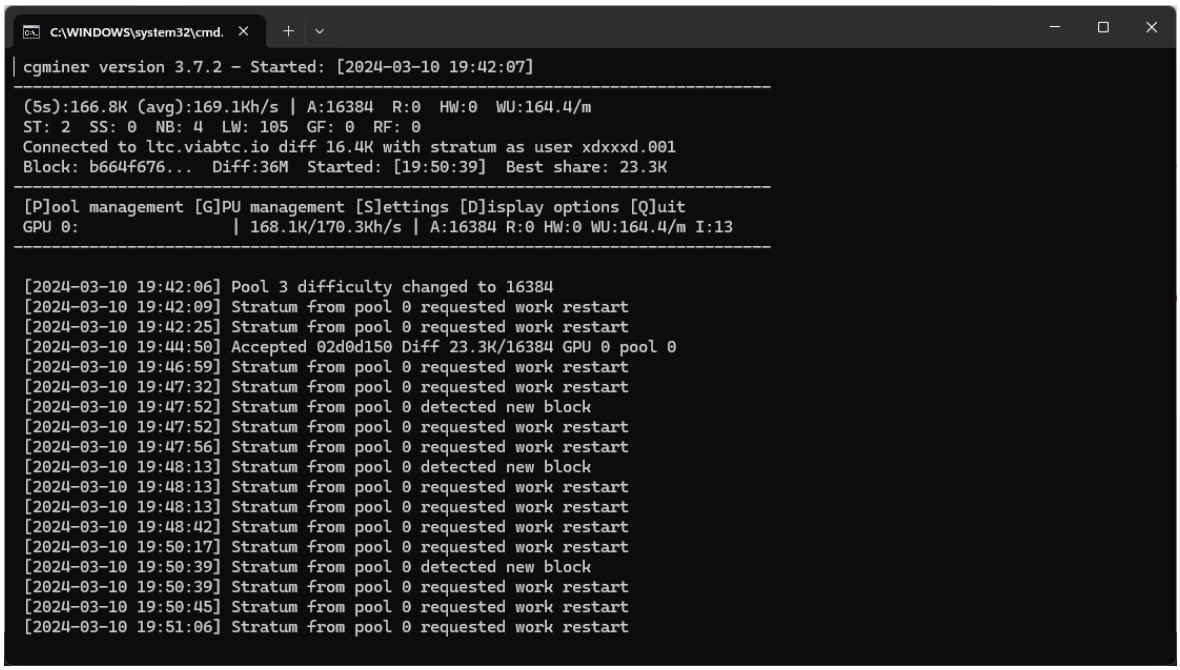
scan-time: Určuje interval pro skenování nových bloků.

scrypt: Toto nastavení specifikuje, zda je použit scrypt algoritmus pro těžbu kryptoměn.

temp-hysteresis: Stanovuje rozdíl mezi zapnutím a vypnutím chlazení, což může pomoci zabránit častým cyklům zapínání a vypínání ventilátorů.

shares: Určuje počet akceptovaných akcií, které mají být zaznamenány v logovacích zprávách.

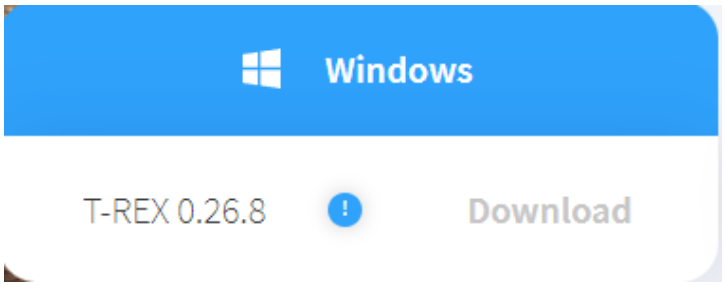
kernel-path: Specifikuje cestu k použitému jádru (kernel) pro těžbu kryptoměn.



Obrázek 13: Konzole s informacemi o těžbě CGMiner a připojení k viaBTC poolu (Zdroj: Autor)

6.3.3 T-rex

Instalace softwaru T-rex je také relativně jednoduchá, jako první krok jsem z oficiální stránky „https://trex-miner.com“ stáhl soubor „t-rex-0.26.8-win.zip“

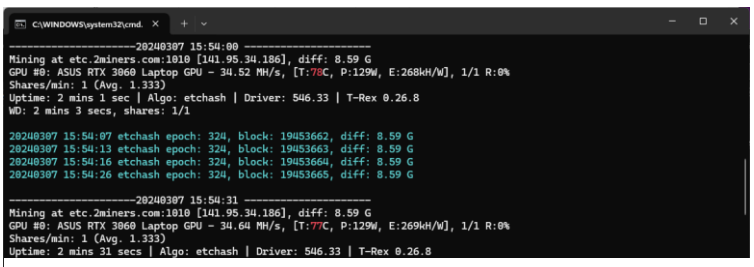


Obrázek 14: Stahování t-rex mineru ze stránky trex-miner.com (Zdroj: Autor)

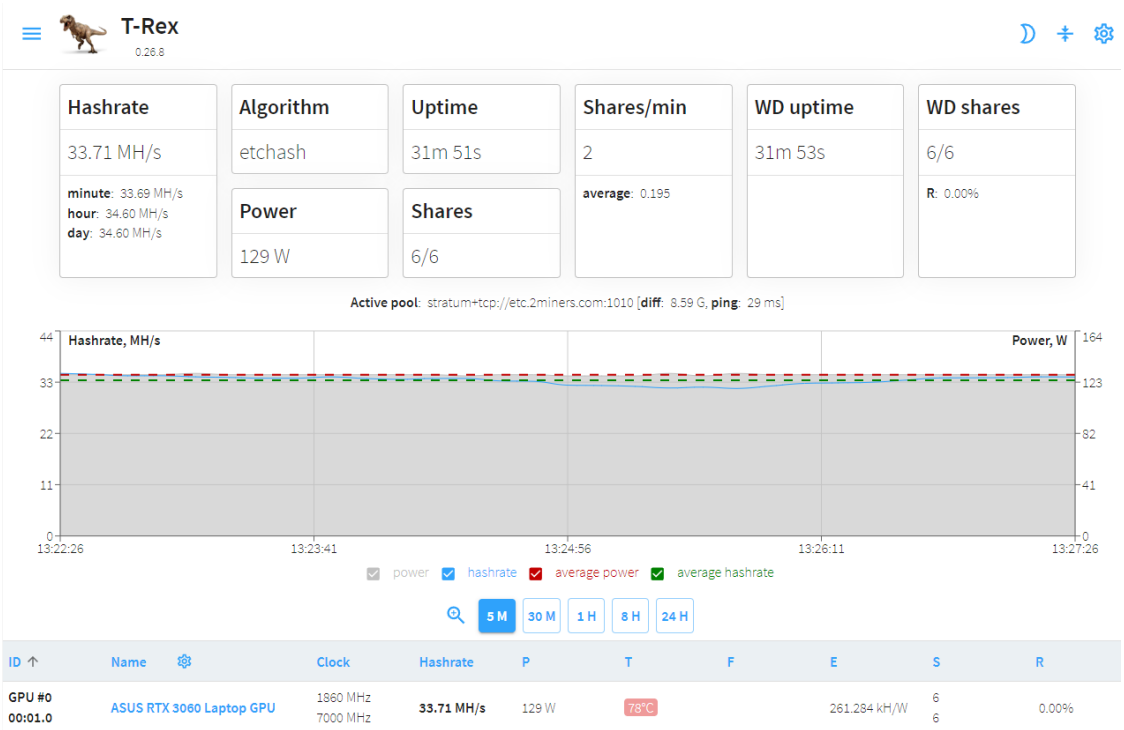
Po extrahování se ve staženém souboru nachází mnoho předvytvořených konfigurací pro těžbu. Konfigurační soubory jsou ve formě „.bat“. V konfiguračním souboru se nachází informace o těžené kryptoměně, o připojeném poolu a intenzity těžby. Je možné si vytvářet vlastní konfigurace, kde můžu například dělat dual mining(těžba dvou a více kryptoměn zároveň). Jediná potřebná změna v přednastavených konfiguracích je adresa peněženky, na kterou chci dostávat odměny za těžbu

Obrázek 15: Konfigurační .bat soubor trex miner (Zdroj:Autor)

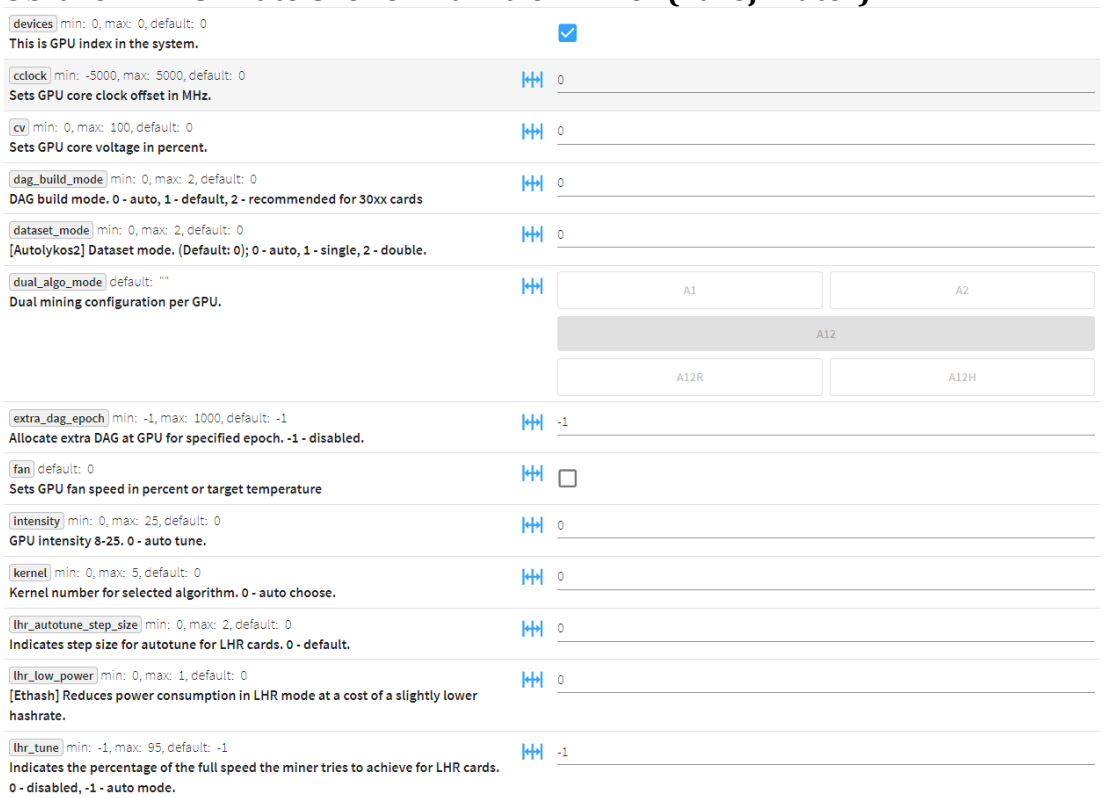
Po spuštění dávkového souboru se zapne konzole s informacemi o těžbě. V konzoli se také ukáže lokální adresa „127.0.0.1:4067/trex“, na které najdeme uživatelské rozhraní pro ovládání těžby. Pro nastavení GPU se zde nachází mnoho možností jako například index grafické karty v systému, úprava offsetu jádra GPU v MHz, úprava napětí jádra GPU v procentech a nebo Intenzita těžby GPU a tak dále. Další dostupná nastavení zahrnují možnost nastavení IP portu pro API mineru přes HTTP, zapnutí HTTPS protokolu pro volání API a tak dále. API nastavení slouží k ovládání trex mineru na dálku.



Obrázek 16: Konzole trex miner (Zdroj: Autor)



Obrázek 17: Uživatelské rozhraní trex miner (Zdroj: Autor)



Obrázek 18: Konfigurace v uživatelském rozhraní t-rex miner (Zdroj: Autor)

Popis jednotlivých konfigurací v uživatelském rozhraní t-rex miner:

devices: Číslo indexu GPU v počítači, které určuje, která konkrétní grafická karta se má použít pro těžbu.

cclock: Posune frekvenci jádra GPU v MHz. Tímto se ovlivňuje rychlost jádra grafické karty.

cv: Napětí jádra GPU vyjádřené v procentech. Pomocí tohoto nastavení lze upravit napětí jádra grafické karty.

dag_build_mode: Režim sestavování DAG, což je datová struktura používaná v těžebním procesu. Zde se nastavuje, jaký režim sestavení DAGu má být použit.

dataset_mode: Režim datasetu pro určitý těžební algoritmus, konkrétně pro algoritmus Autolykos2.

dual_algo_mode: Konfigurace pro dual mining, kdy jedna GPU může těžit dvě různé kryptoměny současně.

extra_dag_epoch: Určuje, zda má být pro konkrétní GPU přidělen dodatečný DAG v určité epochě, což může být užitečné pro určité specifické účely.

fan: Nastavení rychlosti ventilátoru grafické karty v procentech nebo nastavení cílové teploty.

intensity: Intenzita GPU, která ovlivňuje výkon těžby. Hodnota mezi 8 a 25.

kernel: Číslo jádra, které se použije pro konkrétní těžební algoritmus. Obvykle se používá automatický výběr.

lhr_autotune_step_size: Velikost kroku pro automatické ladění u karet s omezeným hashratem (LHR karty).

lhr_low_power: Snížení spotřeby energie pro karty s omezeným hashratem (LHR karty) za cenu mírně nižšího výkonu.

lhr_tune: Určuje procentuální hodnotu maximální rychlosti pro karty s omezeným hashratem (LHR karty).

lock_cclock: Uzamčení frekvence jádra GPU na určitou hodnotu v MHz.

lock_cv: Uzamčení napětí jádra GPU na určitou hodnotu v mV.

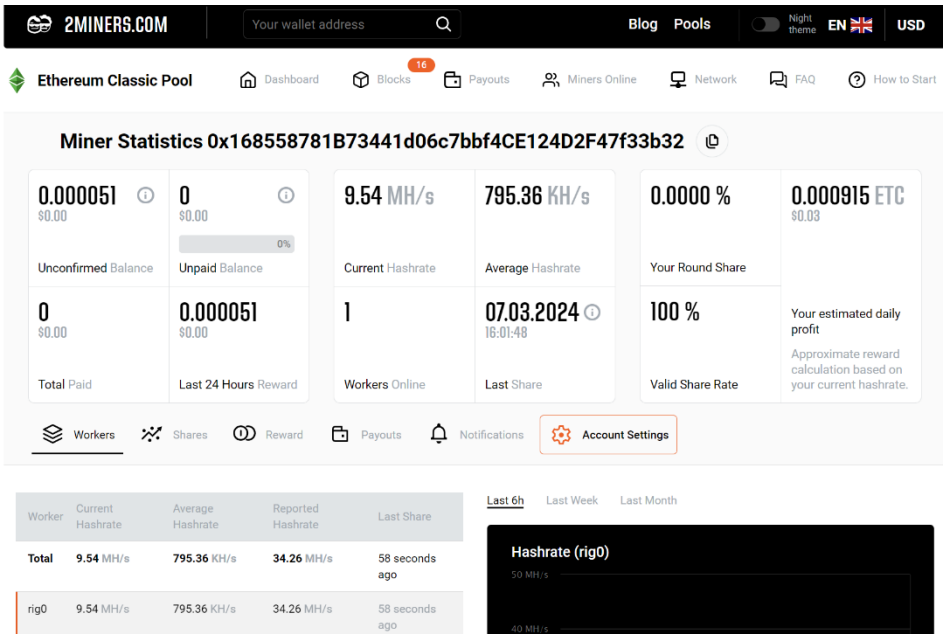
low_load: Režim nízkého zatížení. Sníží zátěž na GPU, pokud je to možné.

mclock: Posunutí paměťového taktu GPU v MHz.

mt: Úpravy paměti pro specifické typy pamětí u starších grafických karet jako(Pascal s pamětí GDDR5 a GDDR5X)

pl: Nastavuje limit výkonu (v procentech pro Windows, ve Watech pro Linux)

Po započaté těžbě si lze ověřit připojení na pool na samotných stránkách jednotlivých poolů (v tomto případě 2miners.com), kde po zadání váší adresy krypto peněženky, kterou jste vložili do configuračního souboru, najdete své statistiky a současnou aktivitu.



Obrázek 19: Oficiální stránka 2miners.com (Zdroj: Autor)

6.3.4 Porovnání dle kritérií

V této části provedu porovnání softwarů Trex Miner, CGMiner a NiceHash na základě čtyř hlavních kritérií. Kritéria budou známkována od 1 do 4. Hodnota 1 značí nejlepší výkon v daném kritériu

Kritéria

1)Jednoduchost Instalace

Toto kritérium hodnotí snadnost instalace softwaru a uživatelsky přívětivé rozhraní, což ovlivňuje, jak rychle a snadno lze nainstalovat daný těžební software a začít s jeho používáním.

2)Konfigurace

Zahrnuje možnosti úpravy nastavení podle individuálních preferencí uživatele, což může ovlivnit flexibilitu a uživatelskou přívětivost softwaru při úpravách nastavení podle konkrétních potřeb uživatele.

3)Výkonnost

Toto kritérium hodnotí efektivitu a stabilitu softwaru při provádění těžebních operací, což zahrnuje rychlost, spolehlivost a schopnost softwaru pracovat s různými typy hardwaru.

4)Další faktory

Tento faktor zahrnuje ostatní aspekty, jako je dostupnost aktualizací, podpora uživatelů, a další užitečné funkce, které mohou přispět k celkové uživatelské zkušenosti s těžebním softwarem

	Instalace	Nastavení/konfigurace	Výkonost	Další faktory
NiceHash	1	4	2	2
CGMiner	3	1	1	3
Trex Miner	2	2	1	3

Tabulka 1: Přehled hodnocení jednotlivých softwarů (Vlastní zpracování)

Jednoduchost Instalace:

NiceHash Miner: Jednoduchá a intuitivní instalace s uživatelsky přívětivým rozhraním, které usnadňuje uživatelům rychlý start.

CGMiner: Instalace může být složitější pro méně zkušené uživatele kvůli absenci grafického rozhraní a nastavení konfiguračního souboru společně s propojením k mining poolu.

Trex Miner: Podobně jako CGMiner, instalace může být obtížnější pro uživatele bez technických znalostí, ale naproti CGMiner je instalace značně jednodušší a je potřeba mnohem menší zásah do konfiguračního souboru při prvotní přípravě.

Konfigurace:

NiceHash Miner: Tento software poskytuje omezené možnosti konfigurace ve srovnání s jinými těžebními softwary. Uživatelé mají přístup pouze k základním nastavením, jako je výběr algoritmu a zapnutí/vypnutí těžby.

CGMiner: Na druhou stranu CGMiner je známý pro svou pokročilou konfigurační možností. Tento software nabízí široké spektrum možností úprav a konfigurace, což je ideální pro pokročilé uživatele, kteří mají technické znalosti a chtějí maximalizovat výkon svého těžebního zařízení. Uživatelé mohou detailně nastavit parametry jako frekvenci jádra GPU, rychlost ventilátoru, limity spotřeby energie a další.

Trex Miner: Nabízí některé možnosti konfigurace, ale v porovnání s NiceHashem je mnohem flexibilnější. Uživatelé mají možnost nastavit různé parametry podle svých

potřeb, včetně úprav frekvence jádra GPU, paměti GPU, rychlosti ventilátoru a dalších. Nicméně ve srovnání s CGMinerem může být Trex Miner stále omezenější v možnostech úprav a konfigurace.

Výkonnost:

NiceHash Miner: Poskytuje stabilní výkon s podporou různých typů hardwaru, ale může mít nižší výkon v porovnání s jinými těžebními softwaremi.

CGMiner: Dobře známý pro svou vysokou výkonnost a spolehlivost při těžbě různých kryptoměn.

Trex Miner: Má výbornou stabilitu a výkonnost, ale může být ovlivněn nedostatkem pokročilých funkcí optimalizace.

Další faktory:

NiceHash Miner:

Vyznačuje se pravidelnými aktualizacemi a dobrou podporou uživatelů. Tento prvek přispívá k tomu, že uživatelé mají neustále k dispozici aktuální verzi softwaru s opravenými chybami a vylepšeními. Díky podpoře uživatelů mohou uživatelé rychle řešit případné problémy nebo získat potřebné informace.

CGMiner:

Disponuje silnou komunitou uživatelů a často aktualizovaným kódem, což znamená, že softwarový nástroj je neustále vylepšován a přizpůsobován novým potřebám a požadavkům. Co se týče uživatelského rozhraní, může být považován za méně přívětivý, což může být pro méně zkušené uživatele nevýhodou. Bohužel, poslední verze CGMineru s podporou pro těžbu na GPU je 3.7.2, která je velmi stará a již dlouho neaktualizovaná. Tento fakt může být problém pro uživatele hledající aktuální funkce a bezpečnostní opravy.

Trex Miner:

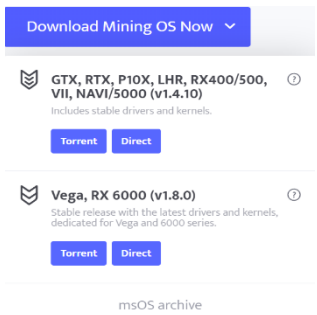
Je známý pro svůj stabilní provoz, což je klíčový faktor pro těžební operace. Nicméně, může chybět dostatečná podpora uživatelů a časté aktualizace. To může znamenat, že uživatelé nemají přístup k nejnovějším funkcím a opravám chyb, což může ovlivnit jejich zkušenost s používáním softwaru. Je také důležité poznamenat, že Trex Miner podporuje pouze NVIDIA grafické karty, což může být omezující pro uživatele s jinými typy grafických karet.

6.4 Porovnání těžebních operačních systémů: HIVEOS, Minerstat

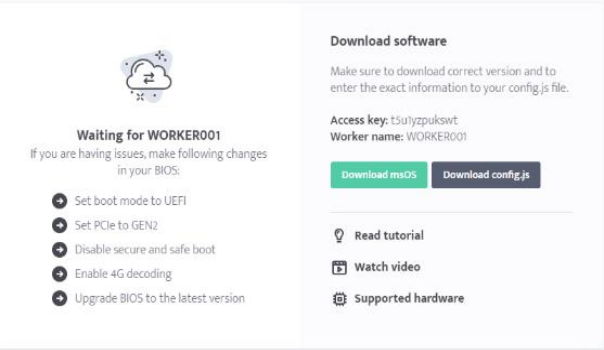
V této části praktického testování jsem se soustředil na instalaci a ověření funkcionality dvou mnou vybraných operačních systémů určených pro těžbu: HiveOS a MinerStatOS. Výběr operačních systémů byl proveden na základě doporučení a recenzí získaných během podrobného průzkumu trhu na diskuzních fórech, kde působí zkušení uživatelé. Cílem tohoto testování je získat srovnatelné výsledky ohledně složitosti instalace, uživatelského rozhraní, stability a dalších klíčových faktorů obou těžebních operačních systémů v reálných podmínkách těžby kryptoměn. Následně budu tyto výsledky analyzovat a vyhodnocovat, aby bylo možné určit nejlepší možnost pro efektivní těžbu kryptoměn pomocí daných operačních systémů.

6.4.1 MinerStat OS

Instalace MinerStat OS začíná registrací účtu na webové stránce "minerstat.com". Po úspěšné registraci je třeba stáhnout instalační soubor, označený jako "msos-v1-4-10-K50-N520-A2030.zip". Po stažení souboru je nutné vytvořit "workera" na platformě MinerStat a stáhnout konfigurační soubor "config.js". Tento konfigurační soubor je důležitý pro správnou konfiguraci těžebního stanice.

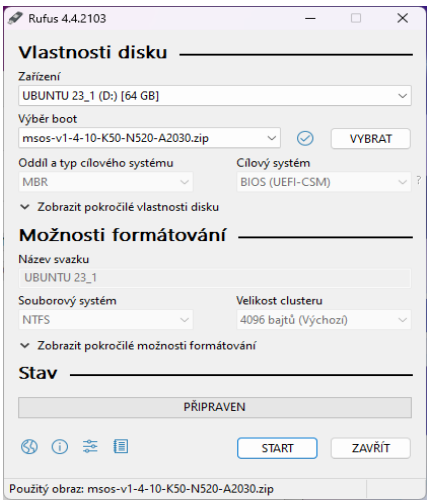


Obrázek 20: Stahování souboru MinerStatOS (Zdroj: Autor)



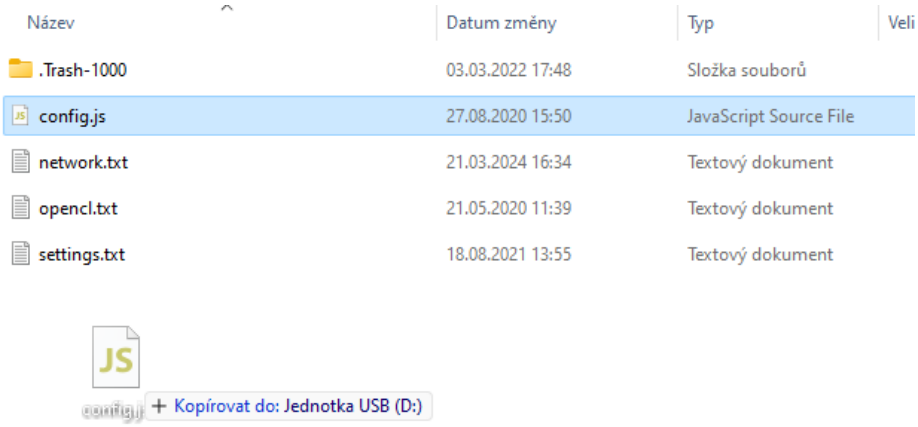
Obrázek 21: Stahnování souboru config.js (Zdroj: Autor)

Po stažení instalačního .zip souboru je také nutné použít software jako Rufus k vytvoření bootovatelného USB disku s operačním systémem MinerStat OS. Rufus je nástroj pro vytváření bootovatelných disků z obrazů ISO, což je klíčový krok před spuštěním instalace HiveOS na těžebním zařízení. Poté je tento bootovatelný USB disk připojen k těžebnímu rigu, aby bylo možné spustit instalaci a nastavení MinerStat OS.



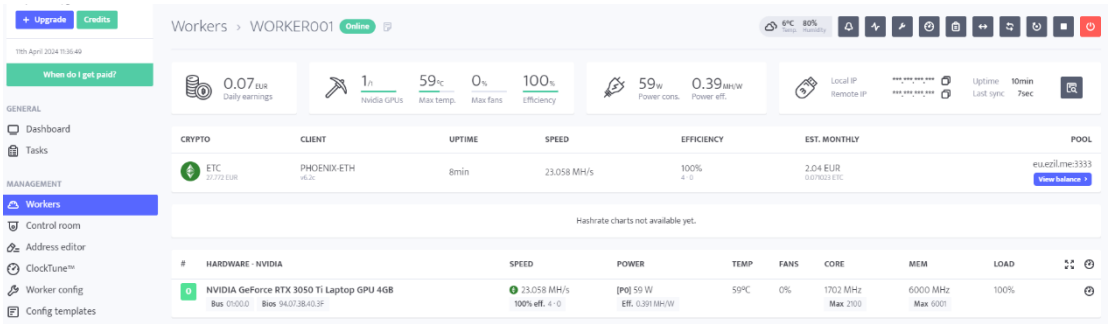
Obrázek 22: Tvorba bootovacího USB s programem Rufus (Zdroj: Autor)

Konfigurační soubor config.js je třeba umístit na bootovatelný disk. Poté se připraví flash disk, na který je konfigurační soubor nahrán, a tento flash disk je následně připojen k těžebnímu rigu. Ideálně by těžební stanice měla být připojena k ethernetové síti, přestože ne všechny síťové karty jsou kompatibilní. Po fyzickém připojení se spustí a inicializace systému lze spravovat MinerStat OS přes online web rozhraní, kde je možné provést další konfigurace a monitorovat těžební operace.



Obrázek 23: Vkládání config.js na bootovatelný USB disk (Zdroj: Autor)

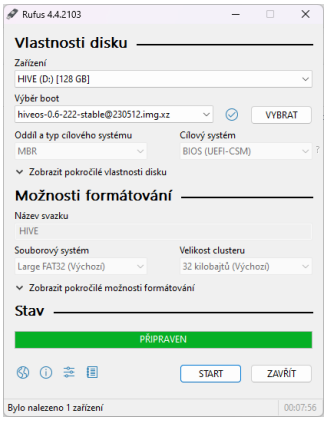
Po zapojení flash disku do těžebního zařízení, které je výhodné připojit na ethernet, protože ne všechny síťové karty jsou podporovány je spuštěn a inicializován systém. Na webovém rozhraní lze sledovat aktuální statistiky a ovládat miner.



Obrázek 24: Uživatelské rozhraní MinerStat OS (Zdroj: Autor)

6.4.2 HiveOS

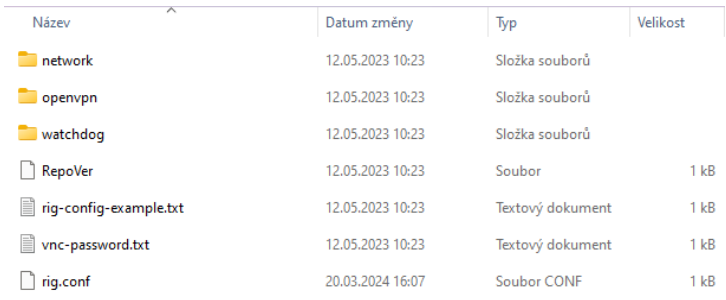
Instalace HiveOS začíná založením účtu na webové stránce "hiveos.farm". Po úspěšné registraci jsem stáhl .zip soubor s operačním systémem. Pro vytvoření bootovatelného disku jsem znovu využil software Rufus, do kterého se nahrává stažený instalační soubor HiveOS.



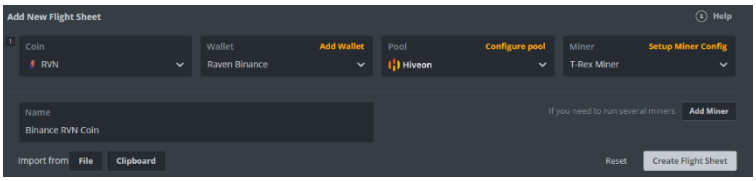
Obrázek 25: Tvorba bootovacího USB s programem Rufus (Zdroj: Autor)

Poté, co je .zip soubor stažen a nahrán na flash disk, je třeba vytvořit "workera" na platformě HiveOS, vytvoření nám dovolí stáhnout konfigurační soubor „rig.conf“, který má automaticky předpřipravenou konfiguraci, kterou je třeba nahrát do bootovatelného flash disku. Po vytvoření workera je také potřeba vytvořit tzv. "flight sheet", což je konfigurační soubor obsahující detailní nastavení pro těžební operace. Flight sheet definuje používaný pool, používáný algoritmus, těženou kryptoměnu a software, pomocí kterého bude worker těžit. Flight sheet se nahrává přes webové rozhraní po spuštění HiveOS.

Obrázek 27: Tvorba Workera a stažení rig.conf (Zdroj: Autor)



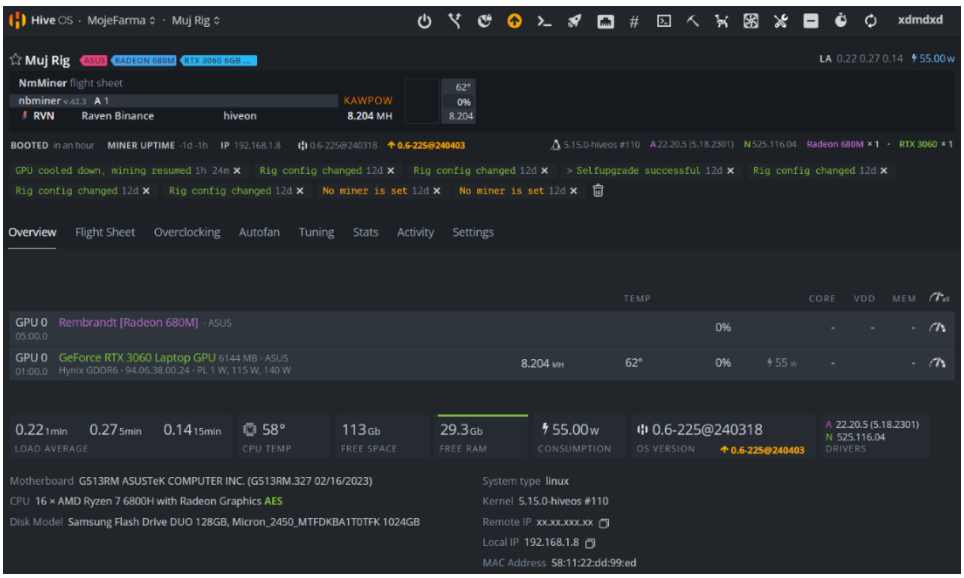
Obrázek 28: Soubory na bootovatelném USB (Zdroj: autor)



Obrázek 26: Tvorba flight sheetu (Zdroj: Autor)

Následně je připravený bootovatelný USB disk připojen k těžebnímu zařízení, přičemž je doporučeno připojení k ethernetové síti pro stabilní připojení. Po fyzickém připojení se těžební rig spustí a inicializuje se operační systém HiveOS.

Na webovém rozhraní HiveOS je možné sledovat aktuální statistiky těžby a provádět další konfigurace pro optimalizaci těžebních operací. Díky uživatelsky přívětivému rozhraní je správa těžebního rigu jednoduchá a efektivní



Obrázek 29: Uživatelské rozhraní HiveOS (Zdroj: Autor)

6.4.3 Porovnání HiveOS a MinerStatOS

V této časti provedu analýzu a porovnání HiveOS a MinerstatOS, dle zmíněných kritérií. Jednoduchost instalace, konfigurace, výkonnost a dalších klíčových faktorů. Využiju obdobnou tabulku jako u porovnání softwarů.

	Instalace	Nastavení/konfigurace	Výkonnost	Další faktory
HiveOS	2	1	1	2
MinerStat OS	2	1	2	1

Tabulka 2: Přehled hodnocení operačních systémů (Vlastní zpracování)

Jednoduchost Instalace:

Instalace obou systémů probíhala obdobně. Pro úplného začátečníka může být proces složitější. Pokud se vyskytne nějaká chyba je třeba hodně trpělivosti a hledání na fórech. Může být potřeba zásah do biosu a v některých případech je třeba manuální instalace driverů.

Konfigurace:

Oba operační systémy, HiveOS a Minerstat, poskytují uživatelům bohaté možnosti konfigurace. To zahrnuje výběr těžebního softwaru a algoritmů, správu připojených zařízení, nastavení přetaktování a napětí, monitoring v reálném čase a reportování výkonu, a také automatické řízení a upozornění. Obě platformy umožňují přizpůsobit svou těžební infrastrukturu podle svých individuálních potřeb a preferencí. Rozhodnutí mezi HiveOS a Minerstatem v tomto ohledu závisí na konkrétních požadavcích.

Výkonnost:

HiveOS: Velmi stabilní, při restartu sám naběhl a nebyl třeba vnější zásah

MinerStatOS: Sám od sebe se čas od času restartuje, po restartu byl třeba manuální zásah.

Další faktory:

HiveOS: Když jde o uživatelské rozhraní je HiveOS velmi zmatečný a neintuitivní. V případě problémů se člověk musí obrátit na komunitu a fóra, protože podpora od developerů je minimální. HiveOS poskytuje detailnější informace o spotřebě energie.

MinerStatOS: Uživatelské rozhraní je přehledné a intuitivní. Nabízí live support v případě problémů. Je zde možnost výplaty ve fiat měně. Ukazatel spotřeba elektřiny není přesný při dual miningu.

7 Shrnutí a diskuse výsledků

Kryptoměny představují revoluční technologii, která mění způsob, jakým lidé vnímají a používají peníze. Tato bakalářská práce se zaměřila na analýzu a prozkoumání světa kryptoměn a jejich těžby, přičemž cílem bylo poskytnout užitečné informace a získat lepší porozumění v této dynamické oblasti. Byly představeny různé kryptoměny, těžební algoritmy a způsoby těžby. Každá z těchto oblastí byla analyzována s cílem poskytnout užitečné informace a širší pochopení fungování kryptoměnového ekosystému. Nejdříve byly představeny různé kryptoměny, jako je Bitcoin, Ethereum, Litecoin a RavenCoin. Každá z těchto měn má své vlastní charakteristiky a využití, ať už jde o historii, technické parametry nebo specifické vlastnosti, které ji odlišují od ostatních. Dále byly rozebrány těžební algoritmy, jako je SHA-256, SCRYPT, Ethash, RandomX a Equihash. Každý algoritmus má své specifické vlastnosti a požadavky na těžební hardware, což ovlivňuje efektivitu a náročnost těžby. Na konec byly popsány různé způsoby těžby, včetně těžby pomocí CPU, GPU, FPGA a ASIC zařízení. Každá metoda má své výhody a nevýhody v závislosti na specifických potřebách těžaře a dostupném technologickém vybavení. V rámci práce byly pečlivě porovnány různé softwary a operační systémy používané při těžbě kryptoměn pomocí grafických karet. Tímto srovnáním byly identifikovány klíčové charakteristiky jednotlivých nástrojů a systémů, aby uživatelé mohli lépe pochopit jejich výhody a nevýhody a lépe se rozhodnout pro nejlepší řešení pro své konkrétní potřeby. Pokud máte levnou elektřinu, tak je těžba kryptoměn velmi lukrativní. Pokud v kryptoměny dlouhodobě věříte, jejich potencionální výnosnost je mnohonásobně vyšší, než se zdá. Mezi analyzované softwary patřily populární nástroje jako NiceHash Miner, CGMiner a Trex Miner, zatímco mezi zkoumané operační systémy patřily HiveOS a MinerStat OS. Každý z těchto nástrojů a systémů má své vlastní charakteristiky, které mohou být klíčové pro úspěch těžebních operací. Závěrem této práce je důležité zdůraznit, že volba správného softwaru a operačního systému může výrazně ovlivnit úspěch těžebních operací a efektivitu zisku kryptoměn. Každá těžební stanice je unikátní a vyžaduje individuální přístup při nastavení a testování různých konfigurací. Je důležité, aby uživatelé pečlivě zvažovali všechny dostupné možnosti a vybrali ty, které nejlépe odpovídají jejich individuálním potřebám a požadavkům.

8 Závěry a doporučení

V praktických závěrech této bakalářské práce jsem se zabýval komplexní problematikou těžby kryptoměn a souvisejících technologií a softwarů. Na základě provedené analýzy a experimentů jsem dospěl k několika klíčovým závěrům a zde je mé doporučení pro investory a těžaře.

Výběr těžebního zařízení

Doporučuji investovat do grafických karet s vysokým výkonem pro těžbu a rychlou návratností investice. Záleží však na konkrétních potřebách a finančních možnostech každého těžaře. Pokud chcete s grafickými kartami zmaximalizovat váš zisk, je možné hledat nové kryptoměny a vsázet na jejich úspěch. Pokud jde o těžbu Bitcoinu, tak je těžké s grafickými kartami zrealizovat nějaký zisk, proto bych v tomto případě doporučil ASIC miner. Ještě je důležité zmínit, že dne 21.4. 2024 proběhlo další bitcoinové půlení a výdělečnost těžby bitcoinu pro malé těžaře je nejasná.

Optimalizace těžebního softwaru

Optimalizace těžebního softwaru hraje klíčovou roli v efektivním provozu těžebních zařízení. Pravidelné aktualizace softwaru zajistí nejen zlepšení výkonnosti, ale také řešení bezpečnostních a kompatibilních problémů. Doporučuji průběžně sledovat vývoj softwaru od různých poskytovatelů a implementovat aktualizace co nejdříve, aby byla zajištěna stabilita a bezpečnost těžebního procesu.

Důležité je také provádět testy s různými typy softwaru, abychom zjistili, který nejlépe vyhovuje našim konkrétním potřebám a podmínkám. Sledujte výkon, stabilitu a uživatelskou přívětivost jednotlivých softwarových platforem a vyberte tu, která poskytuje optimální kombinaci funkcí pro vaši těžební strategii. Buďte otevření novým technologiím a experimentujte s různými nastaveními softwaru, abyste maximalizovali svůj těžební výkon a zisk.

Vzdělávání a sledování trhu:

Sledování kryptoměnového trhu jsou klíčové pro úspěch v oblasti těžby kryptoměn. Doporučuji investovat čas a zdroje do vzdělávání o kryptoměnách a blockchainu, abyste porozuměli novinkám, trendům a potenciálním rizikům na stále volatilním trhu. Sledujte aktuální události a analýzy od odborníků a buďte připraveni reagovat na

změny v tržních podmínkách. Používejte informace získané z vzdělávacích zdrojů k optimalizaci své těžební strategie a maximalizaci svých zisků.

V závěru je důležité zdůraznit, že těžba kryptoměn je komplexní proces, který vyžaduje pečlivé plánování, sledování a adaptaci na aktuální podmínky. S vhodným vybavením, softwarovou optimalizací a bezpečnostními opatřeními mohou investoři a těžaři dosáhnout úspěchu v této dynamické a konkurenční oblasti.

9 Seznam použité literatury

1. FRUMKIN, Daniel; WHITE, Dave; COHOON, Tyler; GRONOWSKA, Magdalena; VOELL, Zack et al. *Braiins Insights: bitcoin mining handbook*. [Prague]: Braiins Insights, [2022]. ISBN 978-80-907975-9-8.

2. STROUKAL, Dominik a SKALICKÝ, Jan. *Bitcoin a jiné kryptopeníze budoucnosti: historie, ekonomie a technologie kryptoměn, stručná příručka pro úplné začátečníky*. Třetí rozšířené vydání. Finance pro každého. Praha: Grada Publishing, 2021. ISBN 9788027110438.

Internetové zdroje

3. AYALA, Gabriel. KOMODO. *Equihash: An Overview & Guide of the Equihash Algorithm* [online]. 2019 [cit. 2024-03-11]. Dostupné z: https://komodoplatform.com/en/academy/equihash-algorithm/

4. AYALA, Gabriel. What is the Ethash mining algorithm? [online]. 2020 [cit. 2024-03-11]. Dostupné z: https://academy.bit2me.com/en/que-es-algoritmo-de-mineria-ethash/

5. AYALA, Gabriel. *What Is Ethash And How Does It Work?* [online]. 2020 [cit. 2024-03-11]. Dostupné z: https://academy.bit2me.com/en/que-es-algoritmo-de-mineria-ethash/

6. BAIVAB KUMAR, Jena. *A Definitive Guide to Learn The SHA-256 (Secure Hash Algorithms)* [online]. 2023 [cit. 2024-04-04]. Dostupné z: https://www.simplilearn.com/tutorials/cyber-security-tutorial/sha-256-algorithm

7. BARNEY, Nick. *What is cryptojacking?* [online]. [cit. 2024-04-19]. Dostupné z: https://www.techtarget.com/whatis/definition/cryptojacking¨

8. BINANCE. *Co je 51% útok?* [online]. 2018, 2023 [cit. 2024-02-01]. Dostupné z: https://academy.binance.com/cs/articles/what-is-a-51-percent-attack

9. BINANCE. *Co je Proof of Stake (PoS)?* [online]. 2018, 2024 [cit. 2024-02-01]. Dostupné z: https://academy.binance.com/cs/articles/proof-of-stake-explained

10. BINANCE. *Co je Proof of Work (PoW)?* [online]. 2018, 2024 [cit. 2024-02-01]. Dostupné z: https://academy.binance.com/cs/articles/proof-of-work-explained

11. BITCOINWIKI. *CGMiner* [online]. 2023 [cit. 2024-03-20]. Dostupné z: https://bitcoinwiki.org/wiki/cgminer

12. CLEARTAX. *What Is Ethash And How Does It Work?* [online]. 2022 [cit. 2024-03-11]. Dostupné z: https://academy.bit2me.com/en/que-es-algoritmo-de-mineria-ethash/

13. CLINEBELL, Katie. *How Green is Ethereum 2.0* [online]. 2024 [cit. 2024-04-14]. Dostupné z: https://www.investopedia.com/how-green-is-ethereum-2-0-6666266

14. COINBASE. *What is Bitcoin?* [online]. 2022 [cit. 2024-03-20]. Dostupné z: https://www.coinbase.com/learn/crypto-basics/what-is-bitcoin

15. COINMATE. *Hash* [online]. 2023 [cit. 2024-03-20]. Dostupné z: https://coinmate.io/cz/hash/#:~:text=Hash%20je%20výsledkem%20kryptografické%20matematické,poznat%2C%20co%20je%20skutečným%20obsahem

16. COINPEDIA MARKETS. *15 years of Bitcoin: 15 milestones from 2008 to 2023* [online]. 2023 [cit. 2024-04-18]. Dostupné z: https://medium.com/coinmonks/15-years-of-bitcoin-15-milestones-from-2008-to-2023-75ccd51b1e0e

17. CUDOMINER. *THE ULTIMATE GUIDE TO GPU/CRYPTO MINING* [online]. 2022 [cit. 2024-04-1ě]. Dostupné z: https://www.cudominer.com/wp-content/uploads/sites/2/2019/09/cudo_mining_ebook_ultimate_guide_v1.7.pdf

18. DAVID, Chris. NERDWALLET. *What Are Altcoins? Bitcoin Alternatives, Explained* [online]. 2022 [cit. 2024-03-20]. Dostupné z: https://www.nerdwallet.com/article/investing/what-are-altcoins

19. GEEKSFORGEEKS. *Cryptography Introduction* [online]. 2023 [cit. 2024-02-18]. Dostupné z: https://www.geeksforgeeks.org/cryptography-introduction/?ref=lbp

20. GEEKSFORGEEKS. *Difference between Private key and Public key* [online]. 2023 [cit. cit. 2024-02-18]. Dostupné z: https://www.geeksforgeeks.org/difference-between-private-key-and-public-key/?ref=lbp

21. GEEKSFORGEEKS. *What is Asymmetric Encryption?* [online]. [cit. 2024-02-18]. Dostupné z: https://www.geeksforgeeks.org/what-is-asymmetric-encryption/?ref=lbp

22. HAYES, Adam. INVESTOPEDIA. *Blockchain Facts: What Is It, How It Works, and How It Can Be Used* [online]. 2023 [cit. 2024-04-18]. Dostupné z: https://www.investopedia.com/terms/b/blockchain.asp

23. HODLNAUT. *Hardware Mining Vs Cloud Mining: Which is Better for You?* [online]. 2022 [cit. 2024-03-10]. Dostupné z: https://www.hodlnaut.com/academy/hardware-mining-vs-cloud-mining

24. CHAMANARA, Sanaz, S. Arman GHAFFARIZADEH a Kaveh MADANI. INVESTOPEDIA. *The Environmental Footprint of Bitcoin Mining Across the Globe: Call for Urgent Action* [online]. 2023 [cit. 2024-03-15]. Dostupné z: https://agupubs.onlinelibrary.wiley.com/doi/10.1029/2023EF003871

25. *Introduction to smart contracts [online]. 2024 [cit.* 2024-04-14*]. Dostupné z: https://ethereum.org/en/smart-contracts/*

26. INVESTOPEDIA. *Altcoins Explained: Pros and Cons, Types, and Future* [online]. 2014, 2023 [cit. 2024-03-20]. Dostupné z: https://www.investopedia.com/terms/a/altcoin.asp

27. INVESTOPEDIA. *What is Bitcoin? How to Mine, Buy, and Use it* [online]. 2023 [cit. 2024-03-25]. Dostupné z: https://www.investopedia.com/terms/b/bitcoin.asp

28. INVESTOPEDIA. *What Is Ethereum and How Does It Work?* [online]. 2024 [cit. 2024-03-25v]. Dostupné z: https://www.investopedia.com/terms/e/ethereum.asp

29. INVESTOPEDIA. *What Is Litecoin (LTC)? How It Works, History, Trends and Future* [online]. 2014, 2023 [cit. 2024-03-25]. Dostupné z: https://www.investopedia.com/terms/l/litecoin.asp

30. KAUR, GUNEET. *What are the different ways to mine cryptocurrency?* [online]. 2023 [cit. 2024-04-14]. Dostupné z: https://cointelegraph.com/learn/what-are-the-different-ways-to-mine-cryptocurrency

31. KIM, Christine. COINDESK. *The Rise of ASICs: A Step-by-Step History of Bitcoin Mining* [online]. [cit. 2024-04-19]. Dostupné z: https://www.coindesk.com/tech/2020/04/26/the-rise-of-asics-a-step-by-step-history-of-bitcoin-mining/

32. KRIPTOMAT. *What is cryptocurrency Ravencoin (RVN) and how does it work?* [online]. 2023 [cit. 2024-04-20]. Dostupné z: https://kriptomat.io/cryptocurrencies/ravencoin/what-is-ravencoin/#What_is_Ravencoin

33. MCFARLANE, Greg. INVESTOPEDIA. *Litecoin (LTC): What It Is, How It Works, vs. Bitcoin* [online]. 2015, 2023 [cit. 2024-03-25]. Dostupné z: https://www.investopedia.com/terms/l/litecoin.asp

34. MCKINSEY. *What is blockchain?* [online]. 2022 [cit. 2024-02-25]. Dostupné z: https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-blockchain

35. NAKAMOTO, Satoshi. *Bitcoin: Peer-to-Peer systém elektronických peněz* [online]. 2008 [cit. 2024-02-25]. Dostupné z: https://bitcoin.org/files/bitcoin-paper/bitcoin_cz.pdf

36. OGUNJOBI, Olumide. *Bitcoin Mixers: Enhancing Privacy in Crypto Landscape* [online]. 2024 [cit. 2024-04-14]. Dostupné z: https://www.cryptoblogs.io/bitcoin-mixers/#:~:text=A%20Bitcoin%20mixer%2C%20also%20known,the%20original%20sender%20or%20recipient.

37. PAGE, James. CRYPTOHEAD. *GPU Usage in Cryptocurrency Mining* [online]. 2021 [cit. 2024-04-14]. Dostupné z: https://cryptohead.io/why-are-gpus-used-for-mining/

38. RHODES, Delton. KOMODO. *Scrypt: What is Scrypt Mining Algorithm* [online]. 2020 [cit. 2024-04-14]. Dostupné z: https://komodoplatform.com/en/academy/scrypt-algorithm/

39. SETH, Shobhit. INVESTOPEDIA. *GPU Usage in Cryptocurrency Mining* [online]. 2023 [cit. 2024-04-14]. Dostupné z: https://www.investopedia.com/tech/gpu-cryptocurrency-mining/

40. SOURCEFORGE. *GMiner vs. NiceHash vs. T-Rex Miner vs. CGMiner Comparison Chart* [online]. 2022 [cit. 2024-04-20]. Dostupné z: https://sourceforge.net/software/compare/GMiner-vs-NiceHash-vs-T-Rex-vs-cgminer/

41. ŠURKALA, Milan. *Ryzen 9 7950X je dobrým CPU pro těžbu kryptoměn, může za to podpora AVX-512* [online]. 2024 [cit. 2024-04-19]. Dostupné z: https://www.svethardware.cz/ryzen-9-7950x-je-dobrym-cpu-pro-tezbu-kryptomen-muze-za-to-podpora-avx-512/60493

42. The Investopedia Team a Amilcar CHAVARRIA. INVESTOPEDIA. *Digital Currency Types, Characteristics, Pros & Cons, Future Uses* [online]. 2024 [cit. 2024-04-14]. Dostupné z: https://www.investopedia.com/terms/d/digital-currency.asp

43. The Investopedia Team a MURRY, Cierra. INVESTOPEDIA. *Cryptocurrency Explained With Pros and Cons for Investment* [online]. 2023 [cit. 2024-04-14]. Dostupné z: https://www.investopedia.com/terms/c/cryptocurrency.asp

44. The Investopedia Team a R. BROWN, Jefreda. INVESTOPEDIA. *Virtual Currency: Definition, Types, Advantages & Disadvantages* [online]. 2023 [cit. 2024-04-14]. Dostupné z: https://www.investopedia.com/terms/v/virtual-currency.asp

45. TREVISAN, Thiago. *How to benchmark your graphics card* [online]. 2023 [cit. 2024-04-14]. Dostupné z: https://www.pcworld.com/article/394845/how-to-benchmark-your-graphics-card.html

46. VÍTEK, Jan. *Těžební hi-end v podobě NVIDIA CMP 170HX se dostává do prodeje za 4400 USD* [online]. 2021 [cit. 2024-04-19]. Dostupné z: https://www.svethardware.cz/tezebni-hi-end-v-podobe-nvidia-cmp-170hx-se-dostava-do-prodeje-za-4400-usd/56239

47. WADE, Jacob. INVESTOPEDIA. *Hash Rate: How It Works and How to Measure* [online]. 2022, 2023 [cit. 2024-04-14]. Dostupné z: https://www.investopedia.com/hash-rate-6746261#:~:text=on%20the%20network.-,How%20to%20Measure%20Hash%20Rate,per%20second%20are%20being%20generated

48. WE BUY USED TAPE. *Which NVIDIA graphics card to use in your crypto mining server?* [online]. 2023 [cit. 2024-04-14]. Dostupné z: https://webuyusedtape.net/2023/03/22/which-nvidia-graphics-card-to-use-in-your-crypto-mining-server/

49. *What is Ether* [online]. 2024 [cit. 2024-04-20]. Dostupné z: https://ethereum.org/en/eth/

10 Přílohy

Seznam obrázků:

Seznam Tabulek:

Webové stránky použitých softwarů v praktické části:

1. NICEHASH. [online]. [cit. 2024-04-22]. Dostupné z: https://www.nicehash.com
2. T-REX MINER. [online]. [cit. 2024-04-23]. Dostupné z: https://trex-miner.com
3. MINERSTAT. [online]. [cit. 2024-04-23]. Dostupné z: https://minerstat.com
4. HIVEOS. [online]. [cit. 2024-04-23]. Dostupné z: https://hiveon.com
5. CGMINER. [online]. [cit. 2024-04-23]. Dostupné z: https://cgminer.info/download/index.html
6. RUFUS. [online]. [cit. 2024-04-23]. Dostupné z: https://rufus.ie/cs/
7. 3DMARK. [online]. [cit. 2024-04-23]. Dostupné z: https://www.3dmark.com
8. VIABTC. [online]. [cit. 2024-04-23]. Dostupné z: https://www.viabtc.com
9. WHATTOMINE. [online]. [cit. 2024-04-23]. Dostupné z: https://whattomine.com

11 Zadání práce z IS (eVŠKP)

Univerzita Hradec Králové
Fakulta informatiky a managementu

Zadání bakalářské práce

Autor:	**Martin Portych**
Studium:	I2100265
Studijní program:	B1802 Aplikovaná informatika
Studijní obor:	Aplikovaná informatika
Název bakalářské práce:	**Grafické karty a kryptoměny**
Název bakalářské práce AJ:	Graphics cards and cybercurrencies

Cíl, metody, literatura, předpoklady:

Cílem bakalářské práce je přehledně zpracovat problematiku těžení kryptoměn použitím grafických karet. Podat přehled základních principů a typů těžení kryptomen, přehled vhodných typů grafických karet, a rovněž upozornit na výhody a rizika jednozlivých typů těžby. Posléze podat přehled v současnosti existujících kryptoměn, případně uvést i některé související okolnosti, např. porovnání kryptoměn dle různých definovaných kritérií, a pod.

Bude poskytnuta zadavatelem

Zadávající pracoviště:	Katedra informačních technologií, Fakulta informatiky a managementu
Vedoucí práce:	prof. RNDr. Peter Mikulecký, Ph.D.
Datum zadání závěrečné práce:	26.1.2021