

MORAVSKÁ VYSOKÁ ŠKOLA OLMOUC

Ústavy informatiky a aplikované matiky

Kryptoměny a porovnání způsobů těžby

Cryptocurrencies and comparison of mining methods

BAKALÁŘSKÁ PRÁCE

Jméno studenta – Jiří Blabla

Vedoucí práce: PhDr. Jan Lavrinčík, Ph.D.

Olomouc 2021

Prohlášení

Prohlašuji, že jsem bakalářskou práci na téma „Kryptoměny a porovnání způsobů těžby“
vypracoval samostatně s použitím uvedených zdrojů a literatury.

V Olomouci dne:

.....

Jiří Blabla

Poděkování

Chtěl bych poděkovat PhDr. Jan Lavrinčík Ph.D. za vedení, trpělivost a odborné rady, které mi pomohly při kompletaci práce. V neposlední řadě bych rád poděkoval také své rodině, která mě při vytváření této práce podpořila.

Obsah

Úvod	1
Hlavní cíl	2
Dílčí cíle	2
Teoretická část	3
1 Základní pojmy	3
<i>Digitální měna</i>	<i>3</i>
<i>Kryptoměna</i>	<i>3</i>
<i>Virtuální měna</i>	<i>3</i>
1.1 Kryptografie	4
1.2 Blockchain	4
1.3 Altcoin	5
1.4 Benchmark	6
2 Výčet vybraných kryptoměn a jejich charakteristika	7
2.1 Bitcoin.....	7
2.1.1 Uchovávání a správa.....	8
2.1.2 Anonymita a bezpečnost.....	8
2.1.3 Historie	9
2.2 Ethereum a kryptoměna Ether	10
<i>Smart contracts</i>	<i>10</i>
2.2.1 Kryptoměna Ether	11
2.2.2 Historie	11
2.3 Litecoin	12
2.3.1 Historie	12
<i>CryptoNote</i>	<i>14</i>

2.4	Monero	14
2.4.1	Hlavní principy Monero měny	15
2.4.2	Historie	15
2.5	Ripple a XRP	15
	<i>Kryptoměna XRP</i>	16
3	Těžba kryptoměn	16
	<i>Proof of Work</i>	17
	<i>Halving</i>	17
	<i>Mining pool</i>	17
3.1	Způsoby těžby	18
3.1.1	Těžba s využitím programu	18
3.1.2	Těžba pomocí cloud služby	18
3.1.3	Těžební stanice (mining rig).....	19
3.2	Hashrate (hashovací rychlost).....	19
3.3	CPU těžba	20
3.4	GPU těžba	20
3.5	FPGA těžba.....	20
3.6	ASIC těžba	20
3.7	ASIC vs GPU	21
3.8	Nejznámější těžební algoritmy	21
3.9	Cryptojacking.....	23
3.10	Ekologické dopady těžby kryptoměn	23
3.11	HiveOS.....	24
3.12	SMOS.....	25
3.13	NiceHash.....	25
3.14	CGMiner	25
	Praktická část.....	27

1 Stavba těžební stanice	27
2 Testování stability počítačové sestavy	29
2.1 CPU testování, Cinebench R15	29
2.2 GPU testování, 3DMark	30
3 Operační systémy HiveOS a SMOS.....	33
3.1 HiveOS.....	33
<i>Instalace</i>	33
3.2 SMOS (SimpleMining OS).....	36
<i>Instalace</i>	36
3.3 Porovnání operačních systémů Hive a SimpleMining.....	37
<i>Hodnotící kritéria</i>	37
4 Těžební programy NiceHash a CGMiner	39
4.1 NiceHash.....	39
<i>Instalace</i>	39
4.2 CGMiner	41
<i>Instalace</i>	41
4.3 Porovnání těžebních programů NiceHash a CGMiner	42
5 Operační systém vs software určený pro těžbu	43
Závěr	44
Zdroje a literatura	46
Seznam použité literatury.....	46
Internetové zdroje	46
Seznam obrázků a tabulek.....	50
Abstrakt a klíčová slova	52

Úvod

S rostoucím technologickým pokrokem dnešního světa se začaly rozvíjet alternativní formy peněžních prostředků v podobě kryptoměn s cílem vytvoření decentralizovaného platebního systému a celkového rozvoje projektů založených na principu blockchainu. Takto definovaná měna se charakterizuje přímými, transparentními transakcemi, které lze vykonávat celosvětově s minimálními poplatky. V posledních letech dochází ke značnému růstu povědomí široké veřejnosti o kryptoměnách v závislosti na úspěchu nejznámější kryptoměny s názvem Bitcoin. Z velké části je popularita zapříčiněna rozdíly od tradičního fungování platebního systému, anonymitou, či formou potencionálně vysokého zhodnocení v krátkém čase.

Na internetu se vyskytuje spousta druhů, kterými lze platit za produkty a služby. Existují společnosti zprostředkující elektronické peněženky, díky kterým jsme schopni operovat s virtuálními financemi, které máme podloženy reálnou měnou. Kryptoměny nejsou podloženy žádnou formou a omezují tak nevýhody centralizovaných měn a vliv inflace.

S problematikou digitálních prostředků značně souvisí také těžba neobjevených bloků kryptoměn, které nabízí mnoho způsobů, jakými lze generovat nové „mince“ pomocí složitých výpočetních operací.

V teoretické části bakalářské práce jsem se rozhodl zaměřit na základní pojmy působící v oboru a výčet vybraných druhů digitálních měn, jejich principy fungování a historické milníky v průběhu několika let. Následně jsem pokračoval teorií popisující způsoby těžby a fungování jednotlivých druhů dle konkrétního zaměření. V neposlední řadě charakteristikou nejznámějších a nejrozšířenějších těžebních algoritmů současnosti a hrozeb spjatých s těžbou kryptoměn.

V praktické části jsem se věnoval stavbě těžební počítačové sestavy a testování stability systému při zátěžových testech. Poté jsem se zaměřil na instalaci a porovnávání vybraných operačních systémů Hive a SimpleMining podle stanovených kritérií hodnotící náročnost instalace, uživatelskou přívětivost, výkon a v neposlední řadě také dodatečnou konfiguraci zařízení. Následovala další část praktické instalace a porovnání těžebních programů pro operační systém Windows na základě zmíněných kritérií.

Hlavní cíl

Hlavním cílem bakalářské práce je přiblížit způsoby fungování vybraných druhů kryptoměn a jejich nejdůležitější historické milníky. Zaměřím se na analýzu procesu těžby a dostupné formy generování nových jednotek kryptoměn.

Výstupem praktické části bakalářské práce bude stavba a optimalizace funkční počítačové sestavy určené k těžbě kryptoměny Bitcoin. Dále bude následovat analýza a porovnání dvou operačních systémů Hive a SimpleMining pomocí srovnávacích kritérií. Zaměřím se také na proces instalace a porovnání těžebních programů NiceHash a CGMiner pro operační systém Windows. Vzhledem ke komparaci dle hodnotících kritérií budu schopen určit vhodnou volbu operačního systému a programu pro začínající těžaře.

Dílčí cíle

1. Prvním dílčím cílem je charakteristika základních pojmů z oblasti kryptoměn. Analýza historického vývoje a stanovení základních rozdílů mezi digitální měnou, virtuální měnou a kryptoměnou. Vymezení principu fungování a využití systému blockchain v reálném světě.
2. Druhým dílčím cílem je analýza procesu těžby a definování pojmů nutných k porozumění zkoumané problematiky. Zaměřím se hlavně na objasnění pojmů Proof of work, Halving, Mining pool a také na rizika spjatá s těžbou.
3. Dalším dílčím cílem této práce je výběr optimální grafické karty prostřednictvím volně dostupných nástrojů a informací k maximalizaci těžebního výkonu a minimalizaci finančních nákladů. Mým cílem je stavba finančně nenáročné stanice na základě výběru vhodného hardwarového vybavení a testování pomocí benchmark testů k zajištění stabilního fungování počítačové sestavy.
4. Poslední dílčí cíl se zabývá analýzou a porovnáním párů těžebních operačních systémů a programů fungujících na navržené počítačové sestavě. Srovnání bude probíhat na základě hodnotících kritérií, které mi pomohou stanovit nejvhodnější typ těžby.

Teoretická část

1 Základní pojmy

Z počátku teoretické části bakalářské práce je nutné definovat základní pojmy vyskytující se v oblasti problematiky kryptoměn a těžebního procesu, mezi které patří:

Digitální měna

Zcela digitálně definovaná měna neboli elektronická hodnota peněz. Ve skutečném světě nemá žádný ekvivalent, jedná se pouze o záznam v databázi. V reálném světě našla digitální měna využití např. k definování dostupných prostředků na bankovních účtech, kdy jsou reálné peníze během vkladu na pobočce banky „převedeny“ do digitální formy a naopak. Digitální měnu můžeme nazvat jako nadřazený pojem pro kryptoměny a také virtuální měny.¹

Kryptoměna

Termín označující nehmotné aktivum sloužící jako prostředek směny. Jedná se o necentralizovanou měnu, generovanou pomocí speciálních šifrovacích technik. Veškeré záznamy o vlastnictví kryptoměn jsou vedeny v počítačové databázi a slouží k zabezpečení všech provedených transakcí.² Využívání kryptoměn je v dnešní době považováno za důvěryhodnou a bezpečnou formu vykonávání plateb. Vývoj ceny a použitelnosti kryptoměn se odvíjí od světové poptávky na trhu.³

Virtuální měna

Stejně jako kryptoměny, řadíme virtuální měnu do oblasti digitálních měn. Její hodnota je definována, řízená podle tvůrce a následně používána v dané virtuální komunitě. Mimo svou

¹ *Digital currency* [online]. 2020 [cit. 2021-03-18]. Dostupné z: <https://www.investopedia.com/terms/d/digital-currency.asp>

² *Cryptocurrency* [online]. 2021 [cit. 2021-03-18]. Dostupné z: <https://www.investopedia.com/terms/c/cryptocurrency.asp>

³ QUEST, Martin. *Cryptocurrency master bundle: The art of hodling crypto mining mindset the ico approach cryptocurrency 101 blockchain dynamics* [online]. 2018. [cit. 2021-03-18].

oblast působení měna ztrácí její hodnotu a také význam.⁴ Virtuální měna, kterou lze použít jako ekvivalentní hodnotu v reálném světě, se označuje jako „konvertibilní“ virtuální měna.

1.1 Kryptografie

Každé oběživo na tomto světě musí být regulováno a opatřeno bezpečnostními prvky, aby bylo možné zabránit podvodnému jednání s nimi. Centrální banka tuto roli plní u národní centralizované měny, bohužel u digitálních měn není možné zabránit padělání pomocí běžných bezpečnostních prvků, proto dochází k využití kryptografie. Kryptografie zajišťuje implementaci bezpečnostních prvků do samotného systému a poskytuje možnost regulace nově vzniklých jednotek či znemožnění falšování.

Dělení kryptografie

1) *Symetrická*

Výpočetně málo náročný způsob, který využívá k procesu šifrování a dešifrování jeden stejný klíč. Nevýhodou tohoto způsobu použití je nutnost předešlé komunikace mezi uzly pro dohodnutí či vygenerování klíče.

2) *Asymetrická*

Šifrování a dešifrování probíhá pomocí dvou rozdílných klíčů, které se dělí na veřejný šifrovací a soukromý dešifrovací klíč lokalizovaný u každého uživatele.

1.2 Blockchain

V minulosti byl tento pojem spojován se způsobem uchovávání a sdílení dat. Nyní je však spojen s modelem decentralizované sítě, která je také často označována jako Distributed Ledger Technology (DLT).⁵ Tato síť ukládá transparentní informace o každé vykonané transakci. Jako jednoduchá forma vysvětlení, jakým způsobem Blockchain funguje, se často uvádí aplikace Dokumenty Google. Při sdílení vytvořeného dokumentu dochází k šíření distribuce souboru, nikoliv k jeho kopírování nebo přenesení. Vytváří se tak decentralizovaná distribuce, která je přístupná k modifikaci všem uživatelům v reálném čase.

S využitím sítě blockchain jsme schopni zajistit absolutní transparentnost, stabilitu a také omezit podvodné jednání. Blockchain je z velké části spojován pouze s kryptoměnami, ale

⁴ Virtual Currency [online]. 2020 [cit. 2021-03-18]. Dostupné z: <https://www.investopedia.com/terms/v/virtual-currency.asp>

⁵ Distributed ledger technology (DLT) [online]. 2017 [cit. 2021-03-18]. Dostupné z: <https://searchcio.techtarget.com/definition/distributed-ledger>

často nachází své využití v mnoha oblastech, mezi které patří monitorování dodavatelských řetězců, věrnostních programů, sdílení dat a také ochrany autorských práv. Velkou popularitu nabyl také při implementaci do řešení online voleb.⁶

„Blockchain umožnil lidem, kteří si vzájemně nedůvěřují, prostřednictvím internetu vyměňovat nebo vytvářet záznamy zcela bezpečnou cestou, a to bez nějakého prostředníka (například notáře, banky, správce databáze nějaké MMO hry). Na jeho provozu se totiž podílejí místo centrálního správce přímo jeho uživatelé. Každý se může zapojit jak přímo do ověřování transakcí (těžby kryptoměn), tak do hlídání těch, kdo v daném blockchainu transakce ověřuje. Stačí k tomu provozovat takzvaný nod, což není nic jiného než aktuální kopie blockchainové databáze. Ve zkratce blockchain představuje velmi specifickou formu databáze.“⁷

1.3 Altcoin

Pojem označující všechny kryptoměny, které byly vytvořeny po úspěchu Bitcoinu. Velmi často se tyto měny prezentují jako vylepšené varianty Bitcoinu. V průběhu tvorby Altcoinů, došlo k rozdělení do čtyř hlavních kategorií, které nazýváme: minig-based, stablecoins, security tokens a utility tokens.⁸

Mining-based altcoin

Altcoiny založeny na principu fungování proof-of-work. Za nejznámější mining-based altcoin současnosti, je považována kryptoměna Ether.

Stablecoins

Druh kryptoměn, které se snaží udržet cenovou stabilitu. Stabilita je zajištěna svázáním hodnoty kryptoměny s reálnou měnou (americký dolar nebo euro) a nesmí převyšovat její nominální hodnotu.⁹

⁶ LEWIS, Antony. *The Basics of Bitcoins and Blockchains: An Introduction to Cryptocurrencies and the Technology That Powers Them*. 1. Florida, USA: Mango Publishing Group, 2018. ISBN 978-1-63353-800-9.

⁷ Wikisofia, *Blockchain* [online]. [cit. 2021-03-26]. Dostupné z: <https://wikisofia.cz/wiki/Blockchain>

⁸ *What is Altcoin* [online]. [cit. 2021-03-19]. Dostupné z: <https://www.techslang.com/definition/what-is-an-altcoin/>

⁹ *Stable coins* [online]. [cit. 2021-03-19]. Dostupné z: <https://www.alza.cz/stable-coins>

Security Tokens

Také označovány jako bezpečnostní tokeny fungují podobně jako investiční smlouvy (očekávání budoucího zisku ze zhodnocení trhu). U bezpečnostních tokenů je jasné definováno, kdo tokeny může nakupovat, spravovat a zpracovávat.

Utility Tokens

Užitkové tokeny, měna programů a aplikací. Forma digitálních mincí (kupónů), které lze využívat k nákupu produktů nebo služeb v rámci dané aplikace. Na rozdíl od bezpečnostních tokenů, nelze měnu používat v rámci investice.¹⁰

1.4 Benchmark

Testovací programy orientované k měření výkonu hardwaru, softwaru a celkového fungování počítačové sestavy. Tyto programy slouží k porovnání výpočetního výkonu mezi zařízeními a ověření stability fungování při zátěži komponent. Veškeré srovnávací testy jsou navrženy tak, aby napodobovaly pracovní zatížení hardwaru.¹¹

CPU test

Benchmark test procesoru využívá matematické úlohy k zjištění výpočetního výkonu na základě množství dat, které může CPU v určitém časovém úseku zpracovávat. Měření může také probíhat pomocí vyhledávání prvočísel, kdy s rostoucím počtem procházených čísel roste bodové ohodnocení výkonnosti procesoru.

HDD a SSD test

Měření na základě rychlosti čtení, zápisu a vyhledávání dat v paměťových modulech. Rychlost pevných disků může značně ovlivňovat výkon ostatních komponent počítačové sestavy.

¹⁰ *SECURITY TOKENS VS. UTILITY TOKENS: A CONCISE GUIDE* [online]. [cit. 2021-03-19]. Dostupné z: <https://www.blockchain-council.org/blockchain/security-tokens-vs-utility-tokens-a-concise-guide/>

¹¹ *Benchmark Computer* [online]. [cit. 2021-03-19]. Dostupné z: <https://www.techopedia.com/definition/27137/benchmark-computer>

GPU test

Určování výkonnosti grafických karet pomocí 2D a 3D grafických testování v závislosti na počtu vygenerovaných snímků za sekundu. S rostoucím počtem snímků roste bodové ohodnocení naměřeného výkonu.

2 Výčet vybraných kryptoměn a jejich charakteristika

V této kapitole se zaměřím na charakteristiku vybraných druhů kryptoměn, historii a principy fungování. V první řadě definuji nejznámější kryptoměnu Bitcoin, způsob jeho uchovávání, bezpečnost a také historický vývoj v čase. Dále budu postupovat vyličením základních informací, spjatých s kryptoměnami Ethereum, Litecoin, Monero a Ripple. Také objasním základní terminologii nutnou k bezproblémové orientaci v dané problematice.

2.1 Bitcoin

Nezávislá a neovlivnitelná digitální měna fungující na principu peer-to-peer sítě, pod názvem Blockchain, která pracuje současně na počítačích po celém světě. Pomocí blockchainu jsou zaznamenávány veškeré transakce a vlastnictví Bitcoin měny. Komunikace v tzv. „Bitcoin síti“, probíhá na základě programového vybavení počítače nebo mobilních zařízení (uzlů), které mezi sebou odesílají potřebná data. Stabilita vývoje ceny Bitcoinu je velmi proměnlivá z důvodu závislosti na poptávce a nabídce trhu, proto může docházet k ovlivňování vývoje kurzu prostřednictvím sociálních sítí a jiných médií.¹²

„Tvorba nových jednotek Bitcoinu je předem dána matematickým algoritmem. Algoritmus je nastaven tak, aby zajišťoval, jak konečný počet jednotek Bitcoinu, tak rychlost vytváření (těžby) nových jednotek. Nové jednotky měny tedy nelze na rozdíl od běžných měn podléhajících centrálním bankám nárazově a účelově vytvořit. Stejně tak nelze centrálně manipulovat s hodnotou měny. Jednotlivé „mince“ Bitcoinu mají podobu jedinečného číselného kódu. Každá „mince“ je unikátní a nezaměnitelná. Konečný počet jednotek Bitcoinu je nastaven 20 999 999,9769 BTC. Algoritmus je dále průběžně upravován tak, aby se počet vytěžených jednotek

¹² PRYPTO. *Bitcoin for dummies*. 1. New Jersey: John Wiley, 2016. ISBN 978-1-119-07613-1.

za určitý časový interval postupně snižoval. Podle tohoto nastavení budou veškeré bitcoiny vytěženy v roce 2140 (většina z nich již však v r. 2030)“¹³

2.1.1 Uchovávání a správa

Obdobně jako bankovní účet nebo peněženka slouží k ochraně a uchování peněžních prostředků, tak i Bitcoin je potřeba uchovávat a chránit před případnou krádeží. V tomto případě existuje mnoho způsobů, jakými lze digitální měny uchovávat. V první řadě existují fyzické principy uložení v osobním počítači a mobilních zařízeních nebo využití tzv. hardwarových peněženek (trezorů). Jedná se o fyzické zařízení, které bylo vytvořeno k bezpečnému uchovávání digitálních měn v offline režimu. Způsob uložení pomocí hardwarové peněženky poskytuje absolutní kontrolu, ale může také dojít ke ztrátě nebo poškození zařízení. Mezi další formy uchovávání digitálních měn řadíme služby třetích stran, kdy využíváme již vytvořené online peněženky.¹⁴

2.1.2 Anonymita a bezpečnost

Často se můžeme na internetu setkat se šířením dezinformace, týkající se anonymity Bitcoinu. Ve většině případů se setkáváme s tvrzením o absolutní anonymitě, bohužel opak je pravdou. V případě, kdy kryptoměnu využijeme pro platbu za zboží nebo služby v reálném světě, dochází automaticky k vytvoření identifikovatelného záznamu provedené transakce. Jelikož je blockchain systém transparentní a přístupný všem uživatelům, nabízí možnost zpětného vyhledání úspěšně vykonaných transakcí a potřebných informací.¹⁵

Bitcoin nabízí určitou formu anonymity, ale v jiném slova smyslu. Pro každou transakci jsme schopni vytvářet nové bitcoinové adresy. Adresy jsou tvořeny unikátními řetězci s délkou 26 až 34 znaků a jsou poskládány z písmen anglické abecedy a čísel. Vytvořená adresa není přímo spjatá s informacemi o vlastníkově daného účtu a zprostředkuje nám tedy danou míru anonymity. Mezi další formy uchování bezejmennosti řadíme tzv. Bitcoin mixer (popř. Bitcoin tumbler). Proces fungující na principu míchání transakcí s jinými transakcemi ostatních

¹³ Kurzy, *Co je to Bitcoin* [online]. 2021 [cit. 2021-03-20]. Dostupné z: <https://www.kurzy.cz/Bitcoin/co-je-to-Bitcoin>

¹⁴ FILLNER, Karel. *Jak na Bitcoin: Krok za krokem* [online]. 2017 [cit. 2021-03-18].

¹⁵ *Is Bitcoin anonymous* [online]. 2020 [cit. 2021-03-18]. Dostupné z: <https://Bitcoinmagazine.com/learning-Bitcoin/is-Bitcoin-anonymous>

uživatelů tak, aby zakryly cestu k původní Bitcoin adrese. V největší míře je zmíněná technika používána podvodníky a hackery k „praní špinavých peněz“. ¹⁶

2.1.3 Historie

První zmínky vzniku Bitcoinu se datují již od roku 2007, přičemž za doby existence došlo již k mnoha významným milníkům. Za zakladatele této měny se považuje skupina lidí, která vystupovala pod pseudonymem „Satoshi Nakamoto“.

Rok 2008

V roce 2008 došlo k výraznému postupu ve vývoji Bitcoinu, jelikož 31. října 2008 proběhla anonymní registrace domény „Bitcoin.org“ a první veřejná zmínka o existenci zmíněné kryptoměny.

Rok 2009

V roce 2009 proběhla zásadní událost. Vytěžení prvního reálného bloku Bitcoinu a následného zapsání do záznamů blockchainu, konkrétně se jednalo o 50 BTC. Částka je do této doby uložena na adrese „1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa“, která patří vlastníkovvi jménem Satoshi. Rok 2009 přinesl také verzi Bitcoin softwaru pod označením „0.1“. Jednalo se o open-source zdrojový kód umožňující těžbu kryptoměny. Ve stejném roce byla zaznamenána první uskutečněná transakce od Sathoshiho na účet kryptografa Hala Finneyho.

Rok 2010

Vznik prvního online tržiště využívajícího Bitcoin platbu pod názvem „The Bitcoin Market“ vytvořeného uživatelem „dwdollar“. V roce 2010 postihl kryptoměnu první velký problém v podobě prolomení protokolu hackerem. Kvůli chybě v 74,638 bloku byl hacker schopen odcizit měnu v hodnotě 184 miliard Bitcoinů. Netrvalo dlouho a tato chyba byla z protokolu odstraněna.

¹⁶What is Bitcoin and how does it work [online]. 2021 [cit. 2021-03-18]. Dostupné z: <https://www.bbc.co.uk/newsround/25622442>

Rok 2011

Rozšíření platební metody v rámci fungování reálného světa, první výskyty v obchodech, darovacích organizacích, ale také nelegálních online tržištích z důvodu nízkého rizika dopadení. Jednalo se o obchody přístupné pouze pomocí speciálního webového prohlížeče s názvem „Tor“. Tržiště sloužily k nákupu nelegálního zboží (drogy, zbraně apod.).

Rok 2012, 2013

Stoupající poptávka po kryptoměně odstartovala vytvoření Bitcoin bankomatů. První bankomat byl k nalezení v San Diegu (Kalifornii), kde bylo možné nakupovat a prodávat Bitcoinů za reálné peníze. Od roku 2013 se k Bitcoinu začalo přistupovat podobnou formou jako u běžných aktiv a kryptoměna se nevyhnula daním.¹⁷

2.2 Ethereum a kryptoměna Ether

Ethereum je decentralizovaná open-source platforma založena na bázi blockchainu, která zastrešuje vlastní kryptoměnu s názvem Ether. Na rozdíl od Bitcoinu se systém Ethereum stará o celou síť projektů s hlavní myšlenkou úplného omezení centralizace a zabránění zranitelnosti spotřebitelských dat. Data jsou velmi často náchylná na hackerské útoky z důvodu uložení na lokálních serverech společnosti.¹⁸

Smart contracts

Smart contracts neboli inteligentní smlouvy označují počítačový kód fungující na systému blockchain, který slouží ke správě peněz, majetku a všech cenných vlastnictví. Inteligentní smlouvy fungují na jednoduchém principu plnění podmínek. V případě, že je podmínka splněna, dojde k provedení akce a naopak. Systém jednoduchých podmínek je napsán v programovacím jazyce s názvem Solidity, který byl a je vyvíjen tvůrci Etherea.¹⁹

¹⁷A short history of Bitcoin [online]. 2020 [cit. 2021-03-18]. Dostupné z: <https://www.bernardmarr.com/default.asp?contentID=1237>

¹⁸G. SOLOMON, Michael. *Ethereum: for dummies*. 1. Kanada: John Wiley, 2019. ISBN 978-1-119-47412-8.

¹⁹An Introduction to Smart Contracts and Their Potential and Inherent Limitations [online]. 2018 [cit. 2021-03-18]. Dostupné z: <https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/>

2.2.1 Kryptoměna Ether

Ve velké míře dochází k záměně terminologie Ethereum a Ether, kdy je kryptoměna často označována jako Ethereum, ale toto tvrzení je mylné. Jedná se o transakční token využívaný v síti Ethereum. V reálném světě si měnu můžeme představit jako jakési palivo (ether) pohánějící chod generátoru (ethereum). Ether se řadí v žebříčku kryptoměn po Bitcoinu na druhé místo největších a nejsilnějších měn současnosti. Na rozdíl od Bitcoinu není ether omezen limitem vyčerpatelnosti a dochází tak k růstu tržní hodnoty v závislosti na poptávce. Doba na vytvoření nového bloku kryptoměny je výrazně nižší než u Bitcoinu a lze ho vytvořit během několika sekund. Smysl etheru není nahradit dosavadní platební formy nebo konkurovat jiným kryptoměnám, ale usnadnit průběh všech uskutečňovaných obchodů.²⁰

2.2.2 Historie

Rok 2013

První návrh a princip fungování Ethereum systému sepsaný do bílé knihy ruským programátorem Vitalikem Buterinem a britským programátorem Gavinem Woodem.

Rok 2014, 2015

Vytvoření a odstartování crowdsoucing kampaně k získání kapitálu nutného pro budoucí vývoj a fungování systému formou prodeje Ethereum tokenů. Během kampaně bylo vybráno téměř 18 milionů dolarů. V roce 2015 došlo ke spuštění první verze s názvem „Frontier“.

Rok 2016

Na začátku roku 2016 došlo k masivnímu hackerskému útoku, během něhož byla odcizena kryptoměna v hodnotě 50 milionů, útok započal první vlnu pochybností o bezpečnosti. Pochybnosti zapříčinily rozdělení komunity na dvě části, mezi které patří Ethereum (ETH) a Ethereum Classic (ETC).²¹

²⁰ *Ether (ETH)* [online]. 2021 [cit. 2021-03-18]. Dostupné z: <https://www.investopedia.com/terms/e/ether-cryptocurrency.asp>

²¹ *A brief history of Ethereum* [online]. 2018 [cit. 2021-03-18]. Dostupné z: <https://coinrivet.com/guides/cryptocurrencies/a-brief-history-of-ethereum/>

Rok 2017

V průběhu let cena Etherea značně kolísala. Hlavní cenový milník této kryptoměny vznikl v roce 2017, kdy došlo k rapidnímu nárůstu ceny o více než 13 000 % původní hodnoty, což zapříčinilo také zvýšení zájmu a poptávky u investorů.

2.3 Litecoin

Digitální peer-to-peer měna založená na principu fungování Bitcoinu. Stejně jako u jiných kryptoměn, tak i Litecoin je založen na open-source kryptografickém protokolu s hlavním cílem rozšíření decentralizačního fenoménu. Ačkoliv hlavní idea Litecoinu vychází z fungování již známého Bitcoinu, nabízí měna mnoho vylepšení. Mezi hlavní výhodu, kterou Litecoin nabízí, patří levnější transakční poplatky.²² Kvůli nižším finančním nákladům na transakce a převody v rámci Litecoinu, dosahuje měna velkého úspěchu a budoucího potenciálu. Nízké poplatky a rychlost provedení transakcí způsobil nárůst popularity kryptoměny a celosvětového využití platební služby. Hlavním cílem bylo vytvořit jednoduchý způsob umožňující rychlé a levné platby napříč kontinenty.²³

Litecoin má přesně definovanou hranici dostupných prostředků k vytěžení, která je stanovena na 84 miliónů. Konečná hodnota 84 miliónů byla stanovena z 21 miliónového limitu Bitcoinů v závislosti na čtyřikrát rychlejšímu způsobu zpracování Litecoinu. Pevně stanovené množství měny zajišťuje stabilitu v rámci působení investičních trhů, a proto nedochází k celkovému ovlivňování měny a činí tak Litecoin z dlouhodobého hlediska velice stabilní.

2.3.1 Historie

Rok 2011

První zmínka a publikace open-source projektu jednoho z prvních altcoinů. Tvůrcem této kryptoměny je Charlie Lee, který také vystupuje pod pseudonymem „Satoshilite“.

²² *Litecoin (LTC)* [online]. 2021 [cit. 2021-03-18]. Dostupné z: <https://www.investopedia.com/terms/l/Litecoin.asp>

²³ *Bitcoin vs. Litecoin: What's the Difference?* [online]. 2021 [cit. 2021-03-18]. Dostupné z: <https://www.investopedia.com/articles/investing/042015/Bitcoin-vs-Litecoin-whats-difference.asp>

Rok 2013

Konec roku 2013 přinesl Litecoinu masivní vzestup, kdy hodnota dosahovala téměř 50 dolarů. Tento vzestup zvýšil zájem investorů a těžařů.

Rok 2014

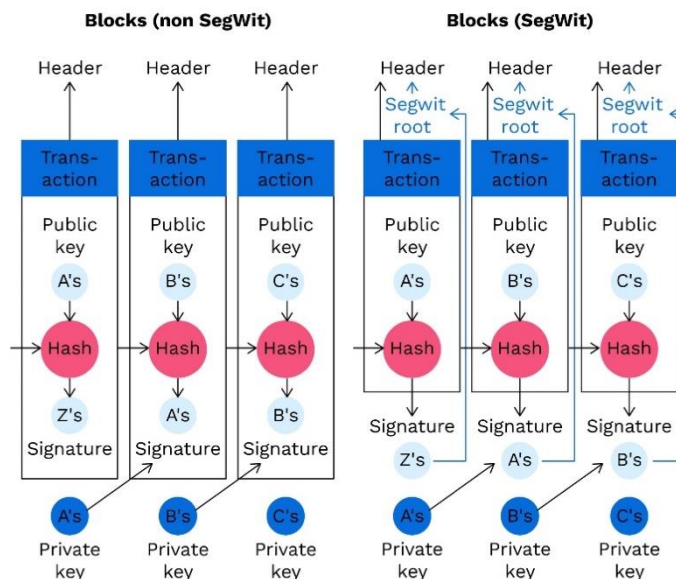
Začátek roku 2014 sebou přinesl problém, týkající se ztráty menších těžařů z důvodu znevýhodnění těžby grafickými kartami, jelikož firma KnCMiner představila ASIC zařízení pro těžbu Litecoinu s obrovským nárůstem výkonu. Z důvodu absence řešení této problematiky se měna za týden propadla téměř o 70% původní ceny na historické minimum.

Rok 2017

Vzkříšení cenové hodnoty Litecoinu a představení nových vizí v podobě SegWitu a Lightning Networks. SegWit implementoval tzv. soft-fork pravidla, která fungovala na principu oddělení dat mimo základní blok blockchainu za účelem řešení problému škálovatelnosti kryptoměn. Z důvodu podobnosti měny s Bitcoinem, posloužil Litecoin jako testovací subjekt před ostrou implementací SegWit pro Bitcoin. Testování proběhlo úspěšně a došlo k přijetí SegWit pravidel. V téže roce byla také vyvinuta tzv. druhá vrstva neboli Lightning Networks, která implementovala využití platebních kanálů za účelem efektivnějšího vykonávání transakcí v blockchainu.²⁴

²⁴ *History of Litecoin* [online]. 2021 [cit. 2021-03-18]. Dostupné z: <https://www.coinhouse.com/Litecoin-price/>

SegWit and block size



Obrázek 1 <https://bitpanda-academy.imgix.net/null19b43d8e-81e7-487a-a776-3c887d4c6450/bitpanda-academy-intermediate-16-segwit-infographic.png?auto=compress%2Cformat&fit=min&fm=jpg&q=80&w=2100>

CryptoNote

Aplikační protokol využíván k uchování soukromí a bezpečnosti decentralizovaných kryptoměn. Protokol řeší problematiku sledování transakčních informací v systému blockchain a je nejčastěji využíván v závislosti s kryptoměnami.

2.4 Monero

Decentralizovaná kryptoměna založená na open-source protokolu CryptoNote s primárním zaměřením na bezpečnost a soukromí transakcí uživatele. Přestože Monero funguje na podobném principu jako ostatní kryptoměny, využívá speciální kryptografické techniky k eliminaci informací všech vykonaných transakcí a skrytí citlivých dat k uchování anonymity. Zabezpečení umožňuje síti validovat příchozí a odchozí transakce bez sdílení informací o předešlých platbách nebo peněžním zůstatku na účtu.²⁵

²⁵ SerHack. *Mastering Monero: The future of private transactions* [online]. 1. 2020 [cit. 2021-03-18].

2.4.1 Hlavní principy Monero měny

Decentralizace

Globální distribuce zamezující hackerské útokům na servery, databáze. Zabraňuje také možnost cenzury a ovládání informací.

Bezpečnost a soukromí

Síť Monero je zabezpečena pomocí vlastních kryptografických technik, a proto není nutné svěřovat finance třetí straně. Na rozdíl od jiných blockchain kryptoměn, Monero v transakcích nenese informace o majiteli účtu, odesílateli ani příjemci.

Fungibilita

Definuje nerozeznatelnost měnových jednotek. Například když kamarádovi půjčíme na určitou dobu jedno Monero a kamarád nám jej potom vrátí, nejsme schopni rozeznat, zda se jedná o stejnou jednotku.²⁶

2.4.2 Historie

Rok 2013, 2014

Odstartování nového projektu s názvem Bytecoin, které proběhlo v roce 2012. Jednalo se o první digitální měnu napsanou pomocí protokolu CryptoNote, která splňovala podmínky na vývoj měny zaměřené na bezpečnost a soukromí, bohužel disponovala pouze s 20 % nevytěžené měny. Tým sedmi vývojářů převzal open-source projekt bytecoin a využil potenciál kryptoměny. Novým názvem se stal BitMonero, který se však zanedlouho upravil pouze na Monero.²⁷

2.5 Ripple a XRP

Ve většině případů je Ripple chybně označován jako kryptoměna, ale správně se jedná o decentralizovanou platební síť, přesněji o digitální platební open-source a peer-to-peer platformu umožňující převod odlišných měn.

²⁶ *Fungibility Monero* [online]. 2021 [cit. 2021-03-18]. Dostupné z: <https://www.getmonero.org/resources/moneropedia/fungibility.html>

²⁷ SerHack. *Mastering Monero: The future of private transactions* [online]. 1. 2020 [cit. 2021-03-18]

Kryptoměna XRP

„Tokeny XRP slouží jako mezičlánek mezi různými páry fiat měn a zajišťují jejich likviditu. XRP funguje v praxi na jednoduchém principu. Chce-li klient americké banky poslat svému známému (např. do Velké Británie) 50 dolarů, nakoupí banka za tuto částku XRP tokeny a přes RippleNet je pošle na vybraný účet v britské bance. Ta přijaté tokeny prodá a ekvivalent 50 amerických dolarů vyplátí v librách na účet příjemce. Informace o převodu se zaznamenají do XRP Ledgeru, obdoby Bitcoinového blockchainu. Zde jsou data o transakci volně přístupná a dohledatelná – využíváním XRP tak bankovní instituce mj. posilují svou důvěryhodnost.“²⁸

3 Těžba kryptoměn

Hlavním a podstatným cílem těžby je zisk v závislosti na maximalizaci výpočetního výkonu těžebního stroje. Termín označující proces ověřování a přidávání uživatelských transakcí do blockchainu. Každý uživatel zainteresovaný v procesu těžby (taktéž označován jako uzel), přebírá a ověřuje uskutečněné transakce, které modeluje do tzv. bloků. Jakékoliv uzavřené obchody jsou automaticky přeneseny těžařům k ověření validity a blokovému formování. Každý těžební proces bloku začíná hashováním transakce z memory poolu a přidáním informace s cílem připsání odměny za odvedenou práci. Vzniklá transakce je následně zapsána jako coinbase transakce a tvoří první záznam nového bloku. Následně jsou transakce hashovány a formovány do tvaru stromu. Hashovací strom obsahuje dvojice transakcí, které opakovaně vykonávají proces do doby, než dosáhne prvotního uzlu stromu, taktéž často nazývaný jako „root hash“. Pod „root hash“ si můžeme představit uzel, ve kterém jsou obsaženy všechny předem vykonané hashovací operace. S nárůstem počtu nových těžařů a zvýšení konkurence těžby, dochází ke zvyšování obtížnosti hashování. Při procesu těžby je nutné opakovaně využívat jeden blok do doby, než dojde k jeho úplnému vytěžení. V případě, že dojde k úspěšnému ukončení procesu těžby jednoho bloku, je následně ověřen ostatními uzly a zapsán do blockchainu. Tímto krokem dojde k uzavření procesu a přesunu na další blok.²⁹

²⁸ Kryptoměna Ripple (XRP) [online]. 2021 [cit. 2021-03-19]. Dostupné z: <https://finex.cz/kryptomena/xrp-ripple/>

²⁹ BENSON, Jared. *Cryptocurrency mining: The beginner's guide to mining cryptocurrency coins, how to start, mining rigs, ASIC, the best coins to mine*. 1. Kalifornie: CreateSpace Independent Publishing Platform, 2018. ISBN 13:978-1985063228.

Proof of Work

Důkaz na základě vykonané práce. Protokol vyvinutý s hlavním cílem omezení kybernetických DDoS útoků, fungující na principu odesílání fiktivních žádostí na server. S příchodem Bitcoinu došlo k zavedení funkcionality protokolu v podobě dokazování hodnoty finančních prostředků pomocí vykonané práce. V současné době je názvosloví z velké části spojováno s kryptoměnami.³⁰

Halving

„Halving Bitcoinu (případně jiné kryptoměny) je snížení odměny těžařů na polovinu. Halving má podstatný vliv na nabídku Bitcoinu - po halvingu se "do oběhu" dostává při stejné intenzitě těžby pouze polovina mincí. Při halvingu 11.5.2020 se například odměna těžaře za jeden vytěžený blok snížila z 25 BTC na 12.5BTC.“³¹

Mining pool

Řešení problematiky s prvotním zahájením těžby nových bloků. V principu jsou vypláceny odměny těžařům, kteří jako první objeví nový těžební blok. Objevení nového bloku vyžaduje obrovský výpočetní výkon, a proto z velké části znevýhodňuje menší těžaře. Mining pool je provozován třetí stranou a zajišťuje rozdělení a sdílení vytěžené měny mezi všechny těžaře v závislosti na jejich poskytovaném těžebním výkonu.³²

„Vůbec první těžební pool se nazývá Slush Pool a byl založen v roce 2010 v Praze. Dnes je provozován firmou Braiins a je největším poolem na světě mimo Čínu. Braiins je také lídrem ve vývoji open-source softwaru pro těžící zařízení. Z tohoto důvodu doporučujeme Slush Pool všem potenciálním zájemcům o těžbu Bitcoinu, protože nejde pouze o místní firmu, ale také o zavedenou a důvěryhodnou firmu v celém odvětví.“³³

³⁰ Proof of Work [online]. 2020 [cit. 2021-03-18]. Dostupné z: <https://www.investopedia.com/terms/p/proof-work.asp>

³¹ Kurzy, Halving - halving Bitcoinu a ostatních kryptoměn [online]. 2021 [cit. 2021-03-19]. Dostupné z: <https://www.kurzy.cz/kryptomeny/halving/>

³² Mining pool [online]. 2020 [cit. 2021-03-18]. Dostupné z: https://en.Bitcoin.it/wiki/Pooled_mining

³³ Alza, Jak funguje těžba Bitcoinu a jak těžit profitabilně? [online]. 2019 [cit. 2021-03-20]. Dostupné z: <https://www.alza.cz/jak-funguje-tezba-Bitcoinu#pool>

3.1 Způsoby těžby

Před samotným zahájením těžebního procesu je nutné stanovení ideálního a nejeftivnějšího typu těžby v závislosti na požadavcích uživatele. Existuje mnoho způsobu, jakými lze kryptoměny těžit. V této kapitole se zaměřím na charakteristiku základních těžebních způsobů ve formě využití programového vybavení, cloudových služeb a také fyzických těžebních stanic. V neposlední řadě se zaměřím na nejpoužívanější těžební algoritmy a vysvětlení jednotlivých konceptů těžby s využitím procesoru, grafické karty, hradlových polí a ASIC zařízení.

3.1.1 Těžba s využitím programu

Uživatelsky nejprívětivější způsob těžby. Na trhu existuje mnoho programů nabízející kompletní řešení v oblasti těžby kryptoměn, avšak valná většina programů funguje téměř na stejném principu. Startovacím bodem je samozřejmě stažení aplikace, následné zadání adresy peněženky k vyplácení odměn a spuštění těžebního procesu. S rostoucím výkonem zařízení se samozřejmě zvyšuje hodnota vypláceného profitu. Využívání programů je limitováno omezenou dodatečnou konfigurací zařízení.

3.1.2 Těžba pomocí cloud služby

Způsob těžby kryptoměn s využitím vypůjčeného výpočetního výkonu. Cloudová těžba nabízí uživatelům možnost těžby bez nutnosti technických znalostí v oboru. Díky uživatelsky přívětivé formě cloudové služby si je uživatel schopen vytvořit online účet k nákupu a správě výpočetního výkonu a započít těžbu během několika minut odkudkoliv na světě. Trend cloudové těžby raketově roste na popularitě v závislosti na velké poptávce kryptoměn. Model těžby v cloudu nabízí za daný měsíční paušál k pronájmu výkon těžebních farem, které jsou nejčastěji umístěny v částech světa s nízkou cenovou hladinou za elektřinu a chladným klimatem z důvodu chlazení těžebních jednotek. Uživatelé mají absolutní kontrolu nad těžbou kryptoměn bez nutnosti správy hardwaru nebo softwaru. Přestože zmíněná forma těžby nabízí mnoho výhod a pro některé jedince je značně přínosná, nese s sebou jistá rizika a nevýhody. Rizika a nevýhody jsou spjaté s výskytem podvodných služeb, ale také nestabilitou cenového vývoje kryptoměn a následného snižování očekávaného zisku.³⁴

³⁴ Cloud mining [online]. 2020 [cit. 2021-03-18]. Dostupné z: <https://www.investopedia.com/terms/c/cloud-mining.asp>

„Existuje mnoho míst, s poměrně dlouhou historií a relativně dobře rozmanitými datovými centry pro cloud těžbu po celém světě. A čím více měn pro těžbu nabízí, tím delší je smlouva a tím vyšší je vstupní poplatek. Vstupní poplatek pro cloud mining se může výrazně lišit. Například Hashtoro cena za 10 TH/s je 400 eur, zatímco Genesis těžební cena za 10 TH/s je 2.800 eur. To znamená že za \$ 6000 můžete zakoupit roční smlouvu na 100 TH. Vzhledem k současné složitosti sítě můžete své investice vrátit do jednoho roku. Budete vydělávat 1.71 Bitcoin. A pokud se jeho cena zvýší, uživatel získá z tohoto růstu další příjmy, jako tomu bylo v roce 2017.“³⁵

3.1.3 Těžební stanice (mining rig)

Zařízení, počítač přizpůsobený primárně k těžbě kryptoměn s nejvyšší možnou efektivitou. Těžební stanice jsou přizpůsobeny v závislosti na způsobu a lokalitě těžby. Hlavní částí rigu je základová deska vybavená jedním nebo více PCI-Express sloty, které jsou osazeny grafickými kartami s vysokým výkonem. Stejně jako u běžného počítače je stanice osazena příslušným procesorem, RAM pamětí a úložným diskem. Celá sestava je napájena dostatečně výkonným zdrojem k zajištění funkčnosti a stability při těžební zátěži.³⁶

3.2 Hashrate (hashovací rychlost)

„Veličina udávající míru výpočetního výkonu uzlu nebo celé Bitcoinové sítě. Její jednotkou je h/s – počet spočtených hashů za sekundu. Odvozené jednotky jsou kH/s (kilohash; 1kh/s = 1000 h/s), Mh/s (megahash; 1 Mh/s = 1000 kh/s), GH/s (gigahash; 1 Gh/s = 1000 Mh/s), Th/s (terahash; 1 Th/s = 1000 Gh/s), PH/s (petahash; 1 Ph/s = 1000 Th/s), EH/s (exahash; 1 Eh/s = 1000 Ph/s). Výkon celé sítě se mezi léty 2009-2013 zvýšil z 1 Mh/s na 10 Ph/s (tj. rozdíl o 10 dekadických řádů).“³⁷

³⁵ Fxstreet, Cloud mining jednoduché a levné s platformou Hashtoro [online]. 2018 [cit. 2021-03-20]. Dostupné z: <https://www.fxstreet.cz/zpravodajstvi-98053.html>

³⁶ Mining rig [online]. 2015 [cit. 2021-03-18]. Dostupné z: https://en.Bitcoin.it/wiki/Mining_rig

³⁷ STROUKAL, Dominik a Jan SKALICKÝ. Bitcoin a jiné kryptopeníze budoucnosti: historie, ekonomie a technologie kryptoměn, stručná příručka pro úplné začátečníky. 2., rozšířené vydání. Praha: Grada Publishing, 2018. Finance pro každého. ISBN 978-80-271-0742-1.

3.3 CPU těžba

Většina kryptoměn je optimalizována k využití těžebního výkonu CPU i GPU. Proces těžby pomocí procesoru se ale stává každým dnem méně použitelný v závislosti na stoupající náročnosti. Mezi nejznámější měnu, u které lze generovat profit pomocí výpočetního výkonu procesoru, můžeme zařadit Monero. Nevýhodou používání tohoto způsobu těžby je značné opotřebení a malá uživatelská podpora.

3.4 GPU těžba

Těžba kryptoměn na principu proof-of-work s využitím výpočetního výkonu grafického čipu. Architektura grafických karet je primárně přizpůsobena k složitému grafickému renderování a nabízí ideální výkon k těžbě Altcoinů. Těžba pomocí GPU je závislá na mnoha faktorech, mezi které patří hashrate, cena a také spotřeba elektřiny. S rostoucí cenou Bitcoinu a náročností generování nových bloků došlo v roce 2017 k celosvětovému kolapsu prodeje grafických karet a křemíkových čipů.

3.5 FPGA těžba

Pojem FPGA označuje programovatelná hradlová pole. Možnost programovatelnosti FPGA udává velkou flexibilitu, jelikož umožňuje lepší optimalizaci a provádění složitých operací s nízkou spotřebou elektrické energie. Nevýhodou používání integrovaných obvodů k procesu těžby je nutná znalost programovacího jazyka pro hradlová pole.

3.6 ASIC těžba

Způsob těžby vykonávané pomocí zařízení navrženého speciálně na těžbu kryptoměn s názvem ASIC. Application Specific Integrated Circuit označuje počítačový čip (integrovaný obvod) přizpůsobený k opakovanému a rychlému vykonávání procesu. Z důvodu specifického zaměření pouze na těžbu může zařízení dosahovat vyššího výpočetního výkonu a efektivnosti. ASIC zařízení generují vyšší hashrate s nižší spotřebou elektrické energie než těžební rig a proto jsou z ekonomického hlediska pro většinu uživatelů mnohem přívětivější. Mezi nevýhody využívání ASIC se řadí jednostranná použitelnost a pořizovací cena.

3.7 ASIC vs GPU

„Hlavním rozdílem ASIC mineru oproti systémům, jako je těžba grafickými kartami (GPU) či procesory (CPU), je všestrannost využití. ASIC miner je možné využít velmi omezeně, a to k těžbě pouze jednoho algoritmu. GPU a CPU těžba je však mnohem univerzálnější a je zde široká škála algoritmů, které lze využívat. Další specifikum ASIC mineru je takové, že se nedá využít pro nic jiného než pro těžbu kryptoměn. Oproti tomu GPU karty či procesory není problém dále použít například do desktopových PC, či výkon GPU a CPU přesměrovat do jiné oblasti výpočtů, než jsou právě ty pro kryptoměny.“³⁸

3.8 Nejznámější těžební algoritmy³⁹

SHA-256

Algoritmus generující unikátní 256bitové řetězce, který se řadí mezi jeden z nejsilnějších hashovacích algoritmů současnosti a momentálně ho využívá 191⁴⁰ druhů kryptoměn. Hashovací frekvence SHA-256 je uváděná v giga hash za sekundu (GH/s). Mezi nejznámější kryptoměny využívající zmíněný algoritmus patří: Bitcoin, Peercoin, Bitcoin Cash, Terracoin a další.

„Funkce SHA-256 obecně dokáže zašifrovat libovolně dlouhý vstupní text na 256bitový hash, který lze znázornit jako text o 64 hexadecimálních písmenech. Funkce je ale natolik složitá, že nepatrná změna ve vstupních datech způsobí vygenerování úplně jiného výstupu. Současně se vyznačuje jednosměrností – je tedy jednoduché spočítat hash, ale není možno z hashe odvodit původní vstup.“⁴¹

Scrypt

Nabízí mnohem vyšší rychlost než SHA-256 z důvodu efektivnějšího využití paměti. Scrypt může být vykonáván procesorem i grafickou kartou a nachází momentální využití

³⁸ Kryptomagazin, *Co je to ASIC miner a jak funguje?* [online]. [cit. 2021-03-20]. Dostupné z: <https://kryptomagazin.cz/co-je-to-asic-miner-a-jak-funguje-kvalitni-informace-pro-vsechny-zajemce-o-tezbu-kryptomen/>

³⁹ Hashgains, *cryptocurrency mining algorithms* [online]. [cit. 2021-03-19]. Dostupné z: <https://www.hashgains.com/wiki/c/what-is-cryptocurrency-mining-algorithms>

⁴⁰ Cryptorival, *SHA-256* [online]. [cit. 2021-03-19]. Dostupné z: <https://cryptorival.com/algorithms/sha256/>

⁴¹ Bitcoin.cz, *Princip těžení Bitcoinu* [online]. 2017 [cit. 2021-03-19]. Dostupné z: <https://Bitcoin.cz/index.php/2017/02/24/princip-tezeni-Bitcoinu-teorie-ii/>

u 593⁴² kryptoměn. Hashovací rychlost algoritmu se měří v kilo hash za sekundu (KH/s). Nejznámější kryptoměny využívající Scrypt algoritmus jsou: Litecoin, Latium, Dodgecoin a další.

X11

Jedná se o energeticky nejúspornější algoritmus umožňující využívat maximální výkon grafického čipu až s 30% snížením odběru elektrické energie. Funguje na principu zřetězeného hashování jedenácti hashovacích algoritmů. Rychlost je určena v mega hash za sekundu (MH/s). Vznik algoritmu byl zapříčiněn pochybností nad bezpečností SHA-256 a omezení způsobů těžby ASIC zařízení. Nejznámější kryptoměny založené na X11 algoritmu jsou: Dash, XCurrency, CannabisCoin a také StarCoin.

CryptoNight

Algoritmus vyvinutý původním vývojářským týmem Bytecoin a CryptoNote. Hlavním cílem algoritmu je umožnění paralelního využití výkonu procesoru a grafické karty k těžbě kryptoměn. Nevýhodnou využití CryptoNight protokolu je nutný přístup a zápis do paměti. Díky tomu není možné využití protokolu v ASIC zařízeních. Populární kryptoměny založené na CryptoNight protokolu jsou: Monero, Bytecoin, FantomCoin a Dashcoin.

⁴² Cryptorival, *Skrypt* [online]. [cit. 2021-03-19]. Dostupné z: <https://cryptorival.com/algorithms/scrypt/>

Ethash

Proof of Work algoritmus vytvořený společností Ethereum využívající hashovací algoritmy Keccak-256 a Keccak-512.⁴³ Hlavním důvodem vzniku Ethash bylo omezení ASIC těžařů (zavedení pouhé GPU těžby) a vytvoření vysoce efektivního algoritmu, který se dříve nazýval Dagger-Hashimoto. Název vznikl spojením dvou jmen Dagger a Hashimoto. V první řadě Dagger vyvinutý Vitalikem Buterinem používající směrové acyklické grafy (DAG), díky kterým se zvyšuje úroveň práce těžby. Algoritmus Hashimoto vyvinutý Thaddeusem Dryjou s cílem vytvoření odolnosti vůči ASIC stanicím. Kombinací zmíněných dvou algoritmů vznikl dostatečně složitý systém těžby k omezení implementace do ASIC zařízení. S přibývajícími problémy došlo k ukončení projektu a odstartování vývoje Ethash.⁴⁴

3.9 Cryptojacking

Typ kybernetického útoku, při kterém hacker infikuje počítačové stanice příslušným malwarem, díky kterému je schopen těžit kryptoměnu bez vědomí uživatele. Obvykle ke Cryptojackingu dochází při nevědomé instalaci běžného softwaru, který je spjatý se škodlivým kódem. Následně po instalaci programu dojde ke spuštění skriptu a zavedení těžebního procesu do počítače. Proces těžby značně zpomaluje chod počítače a zkracuje životnost komponent.

3.10 Ekologické dopady těžby kryptoměn

Těžba kryptoměn a zpracovávání blockchain transakcí je vysoce energeticky náročný proces. Dle výzkumu z roku 2014 bylo potvrzeno, že pouhá těžba Bitcoinu spotřebuje stejné množství elektrické energie jako celé Irsko.⁴⁵ Nadměrná energetická spotřeba je částečně způsobena ověřováním jediné transakční adresy několika uzly.

„Jedna Bitcoinová transakce celkově spotřebuje 30 kWh elektřiny skrze celý blockchain (distribuovanou databázi). Celkový objem proudu, který je k jedné transakci potřeba, představuje přibližně stovku 100wattových žárovek svítit v kuse 300 hodin.“⁴⁶

⁴³ BitcoinWiki, *Ethash* [online]. 2020 [cit. 2021-03-19]. Dostupné z: <https://en.Bitcoinwiki.org/wiki/Ethash>

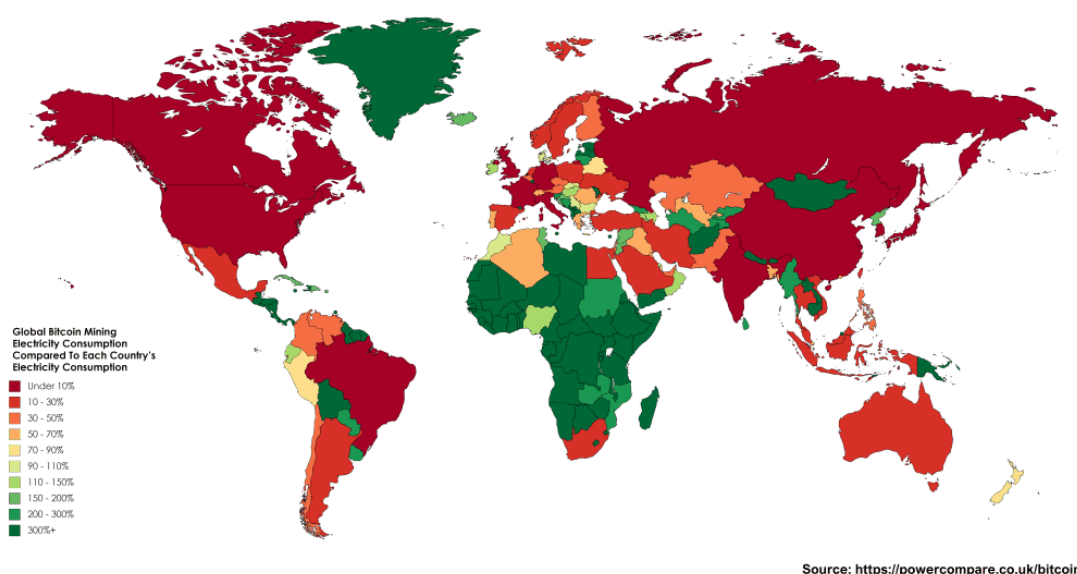
⁴⁴ Bit2me, *What is the Ethash mining algorithm* [online]. [cit. 2021-03-19]. Dostupné z: <https://academy.bit2me.com/en/what-is-the-algorithm-of-ethash-mining/>

⁴⁵ Malone, David & O'Dwyer, K.J.. (2014). *Bitcoin Mining and its Energy Footprint*. 280-285. 10.1049/cp.2014.0699.

⁴⁶ Finance, *Ekologie a kryptoměny – čeká nás zajímavá budoucnost?* [online]. [cit. 2021-03-27]. Dostupné z: <https://www.finance.cz/499524-ekologicke-kryptomeny/>

Hlavní důvod výskytu oxidu uhličitého a dusíku v atmosféře je způsobeno spalováním uhlénného materiálu k výrobě elektrické energie, během níž dochází k znečišťování ovzduší. Problémy spjaté s enormní spotřebou elektrické energie při generování nové kryptoměny, mohou v dlouhodobé perspektivě značně ovlivnit nárůst globálního oteplování, znečištění ovzduší a následné zvýšení úmrtnosti obyvatelstva.

Těžba kryptoměn často využívá elektřinu z obnovitelných zdrojů ve formě větrných elektráren, bioplynu, solární energie a vodních elektráren, aby bylo možné předejít negativnímu působení na životní prostředí.



Obrázek 2 Spotřeba elektrické energie těžbou Bitcoinu v porovnání s běžnou spotřebou konkrétních zemí, Zdroj: <https://powercompare.co.uk/wp-content/uploads/Bitcoin-mining-as-share-world.png>

3.11 HiveOS

Operační systém vyvinutý na linuxové distribuci verze Ubuntu 16.0.4 TLS. Systém byl vyvinut s hlavním cílem poskytnout celkové řešení těžby kryptoměn a správu zařízení uživatelsky přívětivou formou. HiveOS je webový nástroj pro jednoduché monitorování a správu těžebních stanic odkudkoliv na světě. Podporuje GPU, ASIC, CPU zařízení, a proto je často také označován jako multi-těžební systém.

„Jedná se o populární platformu po celém světě, která nabízí velkou škálu možností v těžbě kryptoměn, jako například dobře přehledný monitoring vašich rigů (GPU) či minerů (ASIC). Dále nabízí mnoho typů miner sw, které umožňují těžit velkou škálu algoritmů.“⁴⁷

3.12 SMOS

Celým názvem SimpleMining OS je uživatelsky přívětivý operační systém vytvořený na linuxovém jádře verze Ubuntu 16.0.4 LTS. Systém je primárně zaměřen na těžbu kryptoměn pomocí grafických karet výrobců Nvidia a AMD. SMOS neposkytuje žádnou podporu pro fungování ASIC zařízení.

„Hlavní výhodou oproti těžení přes MS Windows je hlavně to, že SMOS má už v sobě integrovanou většinu minerů (těžící program), a tak nemusíte na každou měnu stahovat jiný miner a ten nastavovat.“⁴⁸

3.13 NiceHash

Společnost s největším světovým trhem nabízející výpočetní těžební sílu. Služba NiceHash funguje na principu propojení koncových uzlů a poskytování hashovacího výkonu. Existují dva druhy využití, z pohledu kupujícího a prodávajícího. Kupující má možnost vybírat z portfolia nabízených kryptoměn a následně zakoupit požadovaný výkon nutný k vytěžení předem stanoveného objemu jednotek. Zvolená hodnota kryptoměn je vytěžena pomocí všech propojených počítačů s nainstalovaným program NiceHash. Proávající (těžař) nabízí výpočetní výkon své pracovní stanice kupujícím za adekvátní finanční ohodnocení v podobě Bitcoinu a vyplňuje tak poptávku na trhu.

3.14 CGMiner

Software vytvořený programátorem Conem Kolivasem v roce 2011. CGMiner je uživateli považován za jeden z nejlepších těžebních softwarů současnosti, který podporuje těžbu na ASIC, GPU, FPGA a CPU zařízeních. Jedná se o open-source program založený na linuxové bázi s podporou operačních systémů MacOS, Windows a Linux. Hlavní výhodou softwaru je

⁴⁷ Kryptoguru, *Plafroma HiveOS* [online]. 2020 [cit. 2021-03-20]. Dostupné z: <https://kryptoguru.cz/platforma-hive-os-videonavod-registrace-instalace-a-nastaveni/>

⁴⁸ Gleton, *Software v oblasti kryptoměn* [online]. [cit. 2021-03-20]. Dostupné z: <https://gleton.cz/blog/software-v-oblasti-kryptomen>

multiplatformní využití, stabilita a podpora komunity vývojářů. Používání softwaru je doporučeno pro zkušenější uživatele z důvodu absence GUI (grafického rozhraní).

Praktická část

1 Stavba těžební stanice

Startovacím bodem těžebního procesu je zvolení správné konfigurace a postavení finančně nenáročných počítačových sestav. Existuje mnoho způsobů, jakými lze počítač sestavit. Vše se odvíjí pouze na volných finančních prostředcích, které chceme do projektu investovat v závislosti na době návratnosti investice.

V mém případě byl startovací kapitál stanoven na rozmezí 15 000 – 18 000 Kč, který musel zajistit investici všech hardwarových komponent počítače. V první řadě bylo potřeba ověřit dostupnost grafických karet, které byly v době stavby celosvětově nedostatkové zboží z důvodu nárustu ceny Bitcoinu. Hledal jsem proto grafickou kartu s nejvyšší hashovací rychlostí v poměru s cenou. K tomuto hledání posloužila srovnávací tabulka nejznámějších a nejvýhodnějších GPU k těžbě v roce 2021.

Tabulka 1 Srovnání grafických karet vhodných na těžbu (ceny říjen 2020), Zdroj: https://www.computerlounge.co.nz/data/media/images/blog/gpu_hash_rates.png

GPU	Odhad hashrate	Průměrná cena	Potřebný výkon
GTX 1650	13.7 MH/s	4 300 Kč	75 W
GTX 1650 Super	20.1 MH/s	5 200 Kč	100 W
GTX 1660 Super	26.4 MH/s	6 750 Kč	125 W
GTX 1660 Ti	25.5 MH/s	7 670 Kč	120 W
RTX 2060	27.6 MH/s	9 055 Kč	160 W
RTX 2060 Super	37.4 MH/s	10 440 Kč	175 W
RTX 2070	36.7 MH/s	11 050 Kč	175 W
RTX 3060 Ti	60.2 MH/s	14 580 Kč	200 W
RTX 3070	61.8 MH/s	18 260 Kč	220 W
RTX 3080	97.9 MH/s	28 080 Kč	320 W
RTX 3090	121.2 MH/s	51 400 Kč	350 W
RX 570	31.3 MH/s	4 600 Kč	150 W
RX 590	32.7 MH/s	5 060 Kč	185 W
RX 5500 XT	26.4 MH/s	5 060 Kč	130 W
RX 5600 XT	37.8 MH/s	8 750 Kč	150 W
RX 5700 XT	54.2 MH/s	12 360 Kč	225 W
RX 6900	59.1 MH/s	23 600 Kč	250 W
RX 6800 XT	66.0 MH/s	27 900 Kč	300 W
RX 6900 XT	67.0 MH/s	30 700 Kč	300 W

Proces porovnávání jsem si ulehčil využitím online kalkulačky profitability od NiceHash, která umožňuje výpočet denního profitu v závislosti na okamžitém vývoji tržní ceny Bitcoinu. Kalkulačka obsahuje tři interaktivní pole pro zadávání hodnot. Pole s názvem „Currency“ poskytuje výběr 158 druhů měn, formulář dále obsahuje pole „El. Costs“ pro zadání aktuální ceny elektrické energie v kWh. Taktéž je nutné vybrat v poli „Device“ typ grafické karty (v mém případě AMD RX5700XT 8 GB) a počet zařízení obsažených v počítači „Number of devices“. Následně stačí vyvolat akci kliknutím na tlačítko „Calculate“, která zobrazí aktuální výši čistého denního, týdenního a měsíčního profitu v závislosti na vývoji tržní hodnoty Bitcoinu.

The screenshot shows the NiceHash calculator interface. It has four main input fields: 'Currency' set to 'CZK - Kč', 'EL costs' set to '4 CZK/kWh', 'Device' set to 'AMD RX 5700 XT 8GB', and 'Number of devices' set to '1'. Below these is a '+ Add Another Device' link. A large orange 'CALCULATE' button is centered at the bottom, with a 'Clear All' link below it.

Obrázek 3 Kalkulátor NiceHash, Zdroj: Autor

AMD RX 5700 XT 8GB

Your approx. income with NiceHash

103.12 CZK / Day

START MINING WITH NICEHASH

*Please note that values are only estimations based on past performance - real values can be lower or higher. Exchange rate of 1 BTC = 1290691.10 CZK was used.

Past earnings of **your setup** on NiceHash

	1 DAY	1 WEEK	1 MONTH
Income	0.00009031 BTC 116.56 CZK	0.00069195 BTC 893.09 CZK	0.00291029 BTC 3756.29 CZK
EL costs	0.00001041 BTC 13.44 CZK	0.00007289 BTC 94.08 CZK	0.00029156 BTC 376.32 CZK
Profit	0.00007990 BTC 103.12 CZK	0.00061906 BTC 799.01 CZK	0.00261873 BTC 3379.97 CZK

Obrázek 4 Výstup kalkulátoru NiceHash, Zdroj: Autor

Poměrově nejpříjemnější grafickou kartu v závislosti na ceně, výkonu a dostupnosti na trhu jsem nakonec zvolil GPU od značky AMD s označením RX 5700 XT. Konkrétně se jedná o AMD Sapphire Nitro+ RX 5700 XT s pořizovací cenou 13 999 Kč. Grafická karta disponuje 8 GB GDDR6 (14 000 Gbps) a rychlostí 2010 MHz grafického čipu. Takto výkonná karta nám umožňuje těžit až s rychlostí 54.2 MH/s. Díky tabulce výčtu grafických karet, internetovým diskuzím a kalkulačce od NiceHash jsem byl schopen vybrat GPU v ideálním poměru výkonu a ceny. Dalším krokem procesu stavby je selekce vhodné základové desky, procesoru, paměti RAM apod. Z důvodu omezeného rozpočtu, který byl z velké části ovlivněn cenou grafické karty nebylo možné zakoupit nové komponenty počítače, a proto přišel na řadu bazarový sortiment. Po dlouhém hledání ideálních komponent jsem se rozhodl pro zakoupení již zkompletované sestavy od značky Packardbell, konkrétně se jednalo o typ PB imedia S2110 s pořizovací cenou 1 200 Kč. Zmíněná sestava byla vybavena dvoujádrovým procesorem AMD E1-1200, 1 TB HDD diskem, 250 W zdrojem, 4 GB operační paměti DDR3 a grafickou kartou AMD Radeon HD 7350 (1 GB) ze které jsem využil pouze základovou desku s procesorem a pamětí RAM. Původní 1 TB HDD disk byl následně nahrazen rychlejším 120 GB SSD diskem. Z důvodu malé velikosti původní počítačové skříně vůči grafické kartě jsem byl nucen přeskládat použité komponenty do větší skříně. V neposlední řadě bylo nezbytné zakoupit výkonnější zdroj pro napájení GPU k zajištění stability fungování počítače. Doporučený výkon zdroje pro grafickou kartu RX 5700 XT je výrobcem stanoven na 500 W, ale abych omezil problémy spojené s napájením sestavy, rozhodl jsem se proto zvolit 650 W zdroj s označením Gigabyte p650b 80 bronze. Dosazení zdroje do sestavy byl poslední krok stavby těžební stanice.

2 Testování stability počítačové sestavy

Kompletně sestavený počítač je potřeba otestovat, aby bylo možné závčas identifikovat správnost fungování jednotlivých částí sestavy. V mém případě jsem zvolil dva druhy softwarů přizpůsobených k zátěžovým testům komponent.

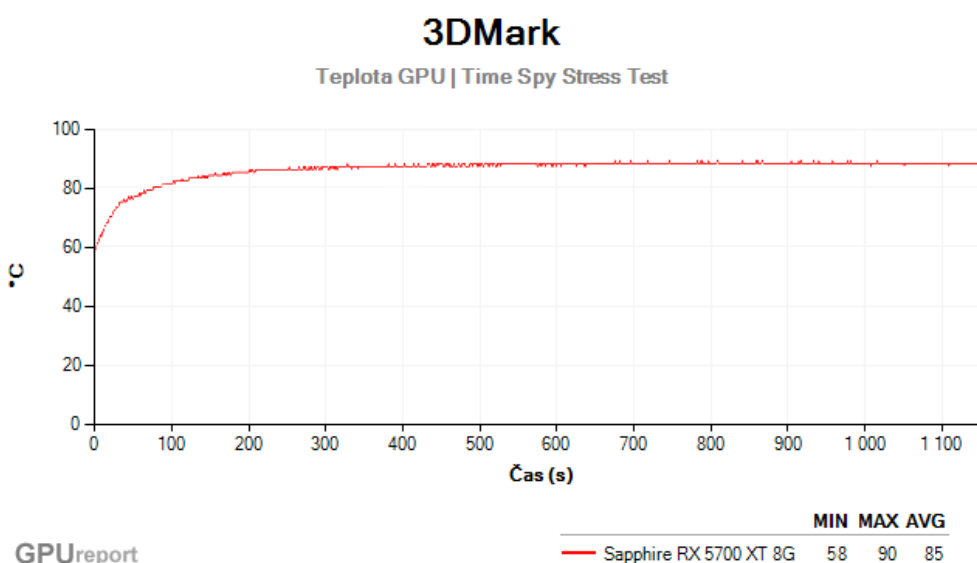
2.1 Testování procesoru, Cinebench R15

První druh softwaru s názvem „Cinebench R15“ slouží k testování výkonu procesoru. Program dokáže testovat výkon jednotlivých jader a také výpočetní výkon celého procesoru. Přesto, že CPU není při těžebním procesu ve velké zátěži, chtěl jsem díky tomuto testování zjistit stav použitého procesoru, popřípadě předejít možným kolizím. Z testu vyplynulo, že

procesor při maximální zátěži nepřesahuje teplotu 68 °C a nedochází k ovlivnění funkčnosti systému.

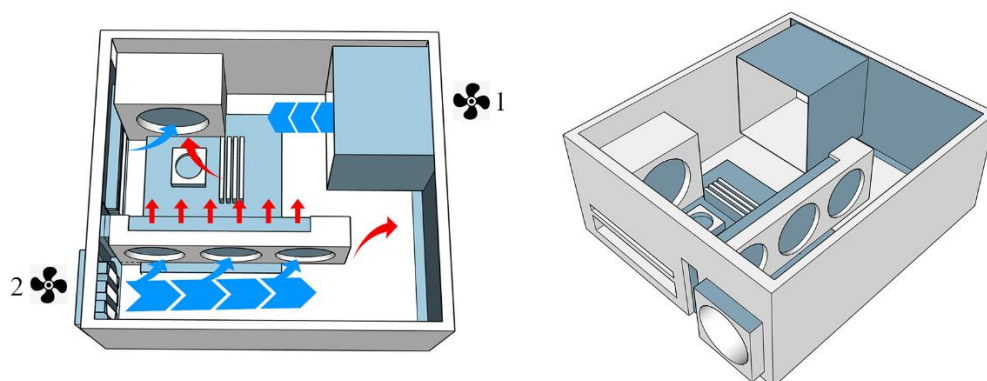
2.2 GPU testování, 3DMark

Test grafické karty probíhal pomocí specializovaného programu s názvem „3DMark“, díky kterému jsem byl schopen otestovat plné zatížení GPU a ověřit tak odolnost zařízení na budoucí proces těžby. Grafickou kartu jsem podrobil testování celkem ve třech případech a výsledky v průměru odpovídaly papírově stanovenému výkonu bez jakýchkoliv poklesů na efektivitě karty. Jedinou problematikou byla teplota grafického čipu, která při maximálním zatížení dosahovala teplot od 85 °C do 90 °C, přičemž běžná provozní teplota grafické karty je stanovena na rozmezí 65 °C až 85 °C. V krátkodobém časovém úseku používání s vyšší teplotou nehrozí poškození, ale v případě dlouhodobého vystavování vysokým teplotám může dojít k negativnímu ovlivnění, či poškození grafické karty.



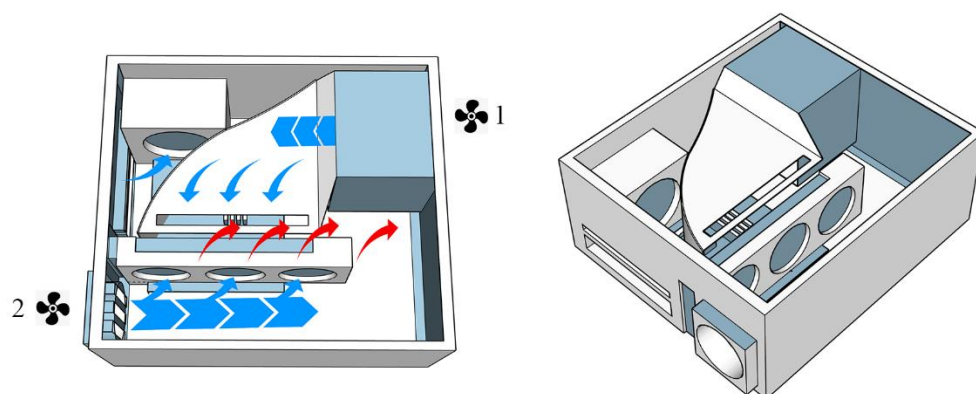
Obrázek 5 Původní teplotní výstup benchmark testu 3DMark, Zdroj: Autor

Z důvodu špatného proudění vzduchu v počítačové skříni docházelo ke kumulaci teploty nad grafickou kartou zapříčiněnou nedostatečným přísunem chlazení ventilátoru s označením jedna (Obrázek 6). Nashromážděný vzduch opětovně ohříval GPU a zároveň také počítačový zdroj, proto nebylo možné, aby grafická karta dosahovala při zátěži nižších teplot.



Obrázek 6 Problematické proudění vzduchu v těžební sestavě, Zdroj: Autor

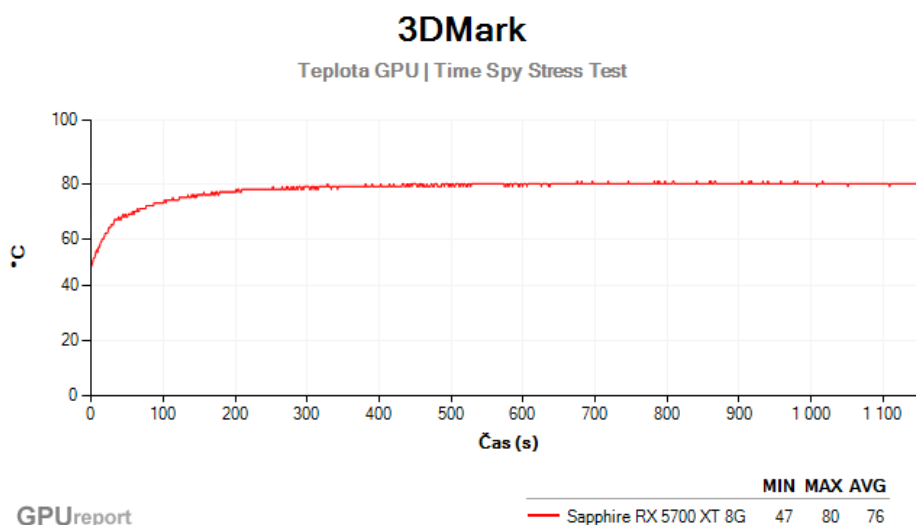
Bylo proto nezbytné zajisit přímé proudění studeného vzduchu na horní hliníkovou část grafické karty k omezení problematického teplotního jevu. V mém případě jsem zvolil nejjednodušší možné řešení v podání vzduchového tunelu vedoucího od ventilátoru s označením jedna (Obrázek 7). Tunel bylo nutné zhotovit z nevodivého a nehořlavého materiálu, z tohoto důvodu jsem zvolil tvrzenou PVC fólii.



Obrázek 7 Vzduchový tunel k chlazení horní části grafické karty, Zdroj: Autor

Po úspěšném zhotovení vzduchového tunelu bylo nutné otestovat vliv přímého chlazení v praxi. Opět přišel na řadu program 3DMark s třemi výkonostními testy, které jasně potvrdily

kladné účiny nového způsobu chlazení. Díky jednoduchému řešení jsem byl schopen dosáhnout výrazně nižších teplot (s maximální teplotou 80 °C) při výkonostní zátěži počítačové sestavy.



Obrázek 8 Teplotní výstup benchmark testu 3DMark s nainstalovaným vzduchovým tunelem, Zdroj: Autor

Tabulka 2 Srovnání původního způsobu chlazení a chlazení s nainstalovaným vzduchovým tunelem, Zdroj: Autor

	PŮVODNÍ ZPŮSOB CHLAZENÍ	VZDUCHOVÝ TUNEL
MINIMÁLNÍ TEPLOTA [°C]	58	47
PRŮMĚRNÁ TEPLOTA [°C]	85	76
MAXIMÁLNÍ TEPLOTA [°C]	90	80

Jak již vyplývá z tabulky, docílil jsem snížení maximální dosahované teploty z 90 °C na 80 °C, přičemž průměrná provozní teplota v zátěži nepřesahovala hodnotu 76 °C.

Proces vykonávaných zátěžových testů umožnil včasné odhalit možné nedostatky, které by mohly negativně ovlivňovat chod celé těžební sestavy. V závislosti na identifikaci problému s provozní teplotou jsem byl pomocí relativně snadné úpravy schopen omezit nežádoucí vliv na komponenty a prodloužit tak jejich životnost.

3 Operační systémy HiveOS a SMOS

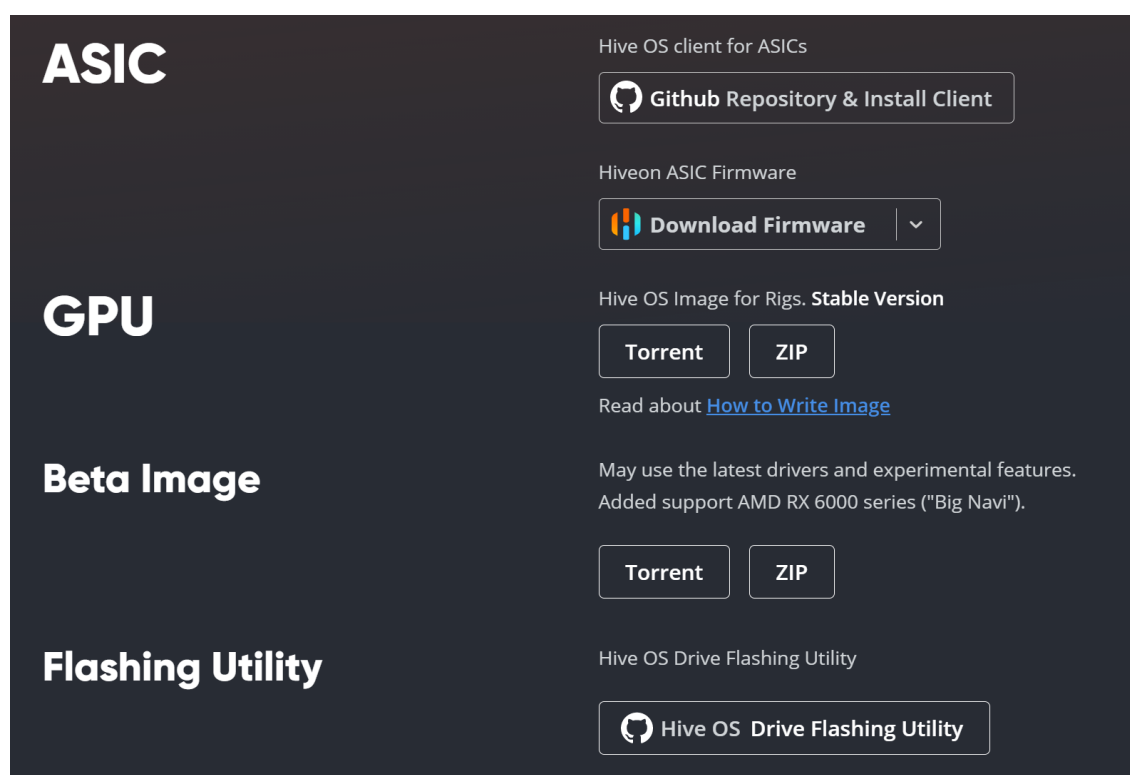
Kapitola popisující instalaci a následné porovnání vybraných operačních systémů HiveOS a SMOS. Hlavní kritéria porovnávají náročnost instalace, uživatelskou přívětivost, stabilitu, výkon a v neposlední řadě také možnost úprav a konfiguraci zařízení.

3.1 HiveOS

Instalace

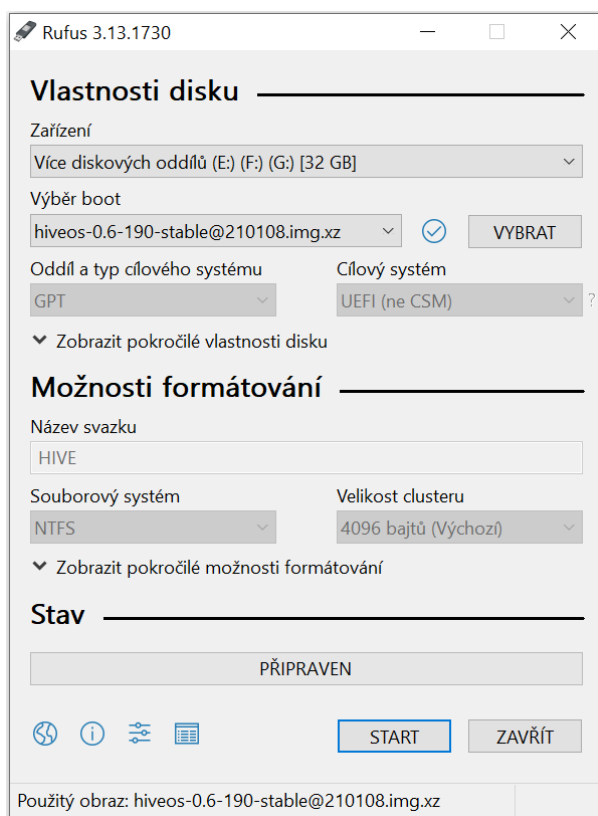
Instalaci těžebního operačního systému HiveOS považuji za uživatelsky velice přívětivou, během níž nejsou vyžadovány příliš velké požadavky na znalosti uživatele.

V první řadě bylo nutné zvolit typ zařízení k těžbě. Webová stránka vývojáře nabízí dva typy instalací rozdělených podle zaměření na ASIC a GPU. V mém případě použití se jednalo o variantu GPU, která nabízí stažení instalačního souboru formou torrentu nebo zip archívu. Kliknutím na interaktivní tlačítko „ZIP“ proběhla akce, která automaticky spustila stahování. Stažený soubor s názvem „hiveos-0.6-190-stable@210108.img.xz“ bylo potřeba extrahovat, aby bylo možné se souborem dále pracovat.



Obrázek 9 Typy instalace operačního systému HiveOS, Zdroj: Autor

Dalším nezbytným krokem instalace bylo stažení a spuštění programu Rufus k vytváření instalačního zařízení. V procesu instalace jsem pokračoval připojením úložného zařízení k počítači, které bylo ihned zobrazeno v rozbalovacím seznamu pod sekci „zařízení“. Dále jsem postupoval zvolením předem extrahovaného souboru s názvem „hiveos-0.6-190-stable@210108.img“ v sekci „výběr boot“ (Obrázek 10). Poté už stačilo pouze spustit proces zápisu kliknutím na tlačítko „start“.

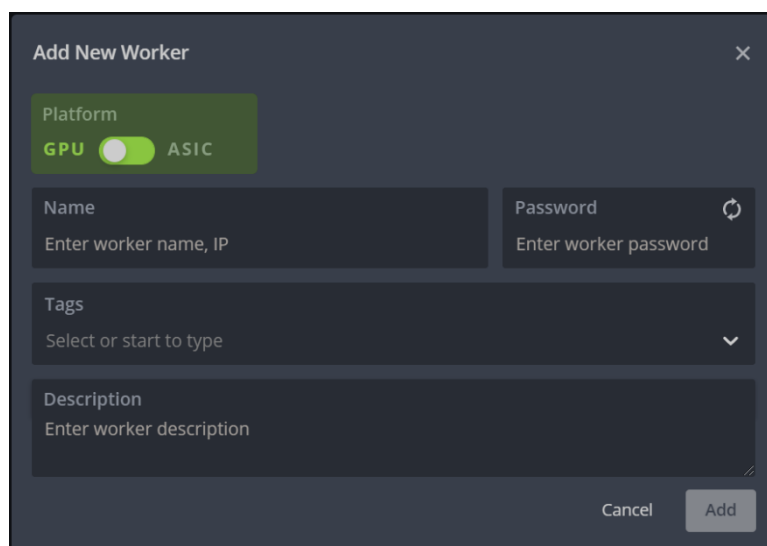


Obrázek 10 Program pro tvorbu instalačního zařízení, Zdroj: Autor

network	08.01.2021 15:30	Složka souborů	
openvpn	08.01.2021 15:30	Složka souborů	
watchdog	08.01.2021 15:30	Složka souborů	
autofan.conf	09.03.2021 18:29	Soubor CONF	1 kB
RepoVer	08.01.2021 15:31	Soubor	1 kB
rig-config-example.txt	08.01.2021 15:30	Textový dokument	1 kB
vnc-password.txt	08.01.2021 15:30	Textový dokument	1 kB
wallet.conf	10.03.2021 13:45	Soubor CONF	1 kB

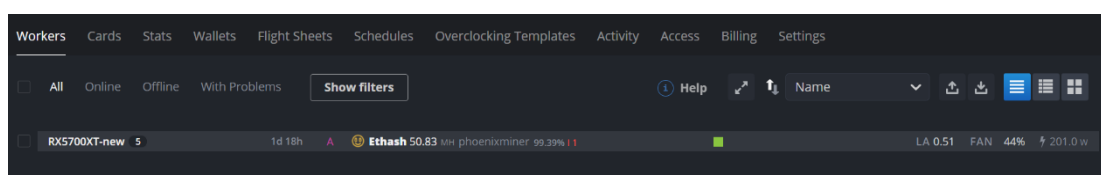
Obrázek 11 Seznam souborů vytvořeného instalačního USB softwarem Rufus, Zdroj: Autor

Posledním krokem vytváření instalačního disku bylo založení uživatelského účtu HiveOS, který slouží ke správě a monitorování chodu těžební stanice. Registrace probíhala vyplněním příslušných údajů registračního formuláře, potvrzením emailové adresy a nastavení dvojité autentizace. Jakmile jsem úspěšně dokončil registraci nového účtu, bylo potřeba propojit vytvořený účet s těžební stanicí. V horní pravé části obrazovky jsem kliknul na ikonu „+“ a následně na tlačítko „Add worker“, které vyvolalo okno se vstupními parametry pro zadání libovolného názvu a hesla farmy (Obrázek 12). Vepsáním validních parametrů a kliknutím na tlačítko „Add“ došlo k automatickému vygenerování a stažení souboru „rig.conf“, který jsem zkopíroval mezi předem vygenerované soubory instalačního zařízení.



Obrázek 12 Formulář přidávání pomoci „Add worker“, Zdroj: Autor

Kompletně dokončené instalační médium jsem připojil pomocí SATA kabelu k počítači, nastavil jej v biosu jako primární zařízení a spustil stanici. Proběhlo automatické spuštění operačního systému HiveOS a následné propojení zařízení s řídicím panelem administrátorského účtu.

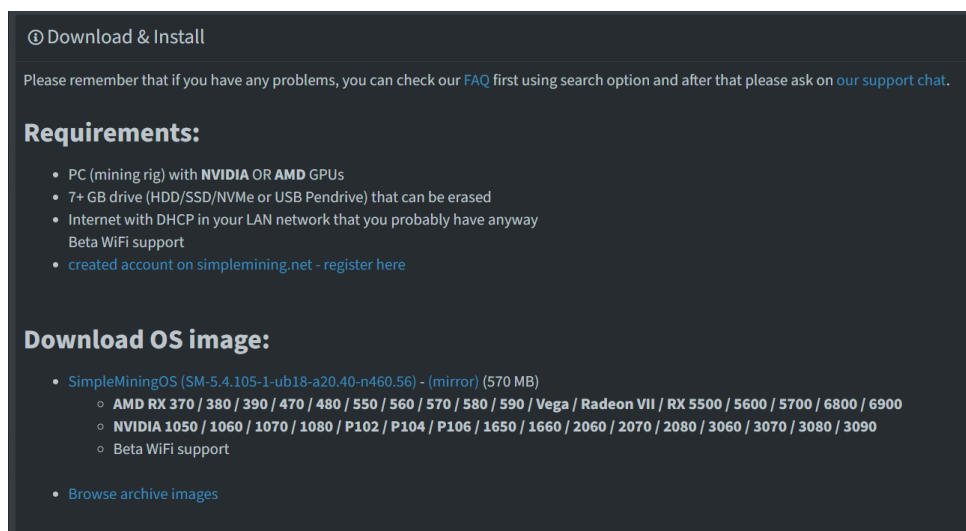


Obrázek 13 Propojené těžební zařízení ve webovém rozhraní HiveOS, Zdroj: Autor

3.2 SMOS (SimpleMining OS)

Instalace

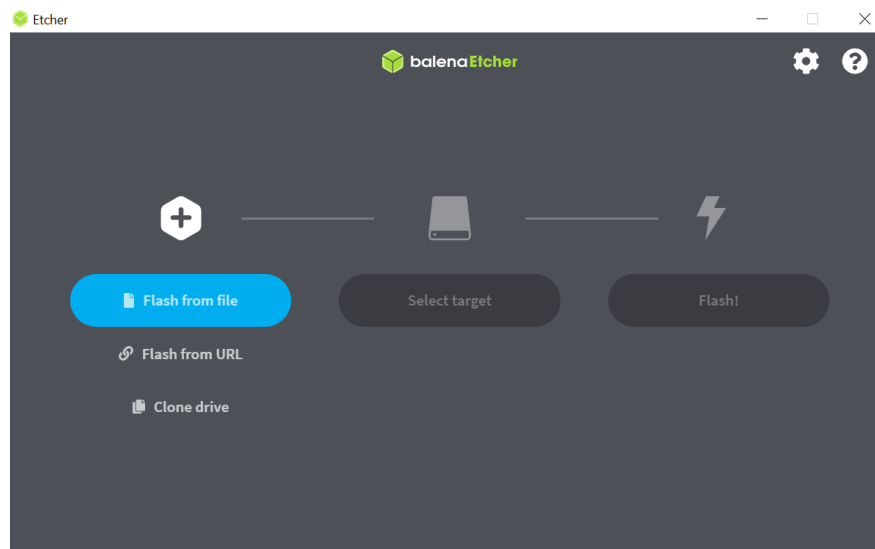
Stejně jako v případě instalace Hive OS, tak i u operačního systému SimpleMining bylo nutné navštívit stránky vývojáře ke stažení instalačního obrazu s názvem „SimpleMiningOS (SM-5.4.105-1-ub18-a20.40-n460.56)“. Po kliknutí na název souboru došlo k přesměrování na cloudové úložiště MEGA a automatickému zahájení stahování souboru. Poté přišla na řadu registrace nového uživatelského účtu, která probíhala běžnou formou vyplnění povinných údajů (email, heslo a heslo znovu) v registračním formuláři a byla dokončena odesláním požadavku po kliknutí na tlačítko „Register“.



Obrázek 14 Instalační soubor SimpleMining, Zdroj: Autor

Z důvodu nezdařených pokusů o vytvoření instalačního disku pomocí programu „Rufus“ jsem byl nucen využít jiné programové vybavení se stejnou nebo podobnou funkcionalitou. Využil jsem tedy často používanou alternativu k vytvoření instalačního zařízení s názvem „Etcher“. Uživatelské rozhraní programu je velice přívětivé a proces tvorby disku se skládá pouze ze tří jednoduchých kroků. V prvním kroku jsem vybral obrazový soubor obsahující instalační data operačního systému SimpleMining, následoval výběr úložného disku a potvrzení procesu zápisu kliknutím na tlačítko „Flash!“. Po dokončení zápisu obrazu na disk bylo nezbytné v adresáři nalézt soubor s názvem „config“ a nahradit obsah parametru

„USER_EMAIL“ uživatelským emailem předem vytvořeného SMOS účtu k zajištění konektivity počítače s webovým rozhraním.



Obrázek 15 Software Etcher pro tvorbu instalačního zařízení, Zdroj: Autor

Prvotní spuštění těžebního počítače s nainstalovaným operačním systémem SimpleMining se neobešlo bez úpravy vývojářem přesně definovaného nastavení biosu, které je nutné k fungování systému. Potřebné změny biosu se týkaly nastavení: 4G kódování, podpory Auto PCI-E, povolení integrované grafické karty (IGD) a podpory ERP. Po provedených úpravách nastavení bylo možné počítač spustit a navázat spojení s webovým rozhraním SimpleMining k dokončení instalace a přidání těžebního rigu.

3.3 Porovnání operačních systémů Hive a SimpleMining

Z důvodu zachování přehlednosti jsem zvolil formu hodnotící tabulky. Tabulka se skládá z jednotlivých zkoumaných kritérií, které jsou ohodnoceny stejně, jako hodnotící stupnice ve vzdělávacím systému (škálou od výborná po nedostatečná).

Hodnotící kritéria

1) Náročnost instalace

Kritérium zohledňující vynaložený čas a požadavky na znalosti uživatele. Nutné zajištění programového vybavení a nezbytných změn v nastavení.

2) *Uživatelská přívětivost*

Analýza grafického uživatelského rozhraní operačních systémů v závislosti na použitelnosti, celkové ovladatelnosti a jeho přehlednosti.

3) *Těžební výkon*

Porovnání rychlostí těžební stanice v jednotkách mega hash za sekundu (MH/s) s aktuální spotřebou elektrické energie.

4) *Dodatečná konfigurace*

Možnost změn nastavení zařízení, úprava taktování grafických karet, monitorování systému a jiné způsoby usnadnění práce s operačním systémem.

Tabulka 3 Hodnotící tabulka operačních systémů v závislosti na zkoumaných kritériích, Zdroj: Autor

KRITÉRIA	HIVE OS	SIMPLEMINING OS
NÁROČNOST INSTALACE	Výborná	Dobrá
UŽIVATELSKÁ PŘÍVĚTIVOST	Chvalitebná	Výborná
TĚŽEBNÍ VÝKON	Výborná	Chvalitebná
DODATEČNÁ KONFIGURACE	Výborná	Chvalitebná

Testování jednotlivých kritérií probíhalo vždy za totožných podmínek a na stejné pracovní stanici. Instalaci operačního systému Hive jsem ohodnotil na výbornou, jelikož proces probíhal hladce bez jakýchkoliv problémů. Na rozdíl od SimpleMining nebyla zapotřebí dodatečná konfigurace nastavení biosu, díky které působila instalace plynulejším a jednodušším dojmem bez nutnosti širších znalostí. Opakem však byla uživatelská přívětivost operačního systému SimpleMining, která převyšovala systém Hive svou přehledností, ovladatelností a celkovým pocitem z používání. Jedinou nevýhodnou v porovnání s Hive byla absence mobilní aplikace SimpleMining. Těžební výkon se základním nastavením operačních systémů vykazoval téměř identické hodnoty s rychlostí 51,3 MH/s. Problém nastal v průběhu dlouhodobého testování těžebním zatížením, kdy SimpleMining (na rozdíl od Hive) vykazoval nekonzistentní chod a drobné propady výkonu, které bylo možné vyřešit úpravou taktovací frekvence a napájení. Oba dva systémy nabízely širokou škálu dodatečného nastavení od zařízení až po správu a fungování těžební stanice, přičemž Hive značně převyšoval SimpleMining svou rozmanitou škálou monitorovacích prvků, které usnadňovaly každodenní správu těžebního rigu. Díky velké uživatelské základně nabízí Hive vestavěnou knihovnu s přednastavenými profily, určenými

pro specifické typy grafických karet, díky kterým jsem byl schopen zvýšit těžební výkon na necelých 55 MH/s, s téměř poloviční spotřebou elektrické energie a snížením teploty grafického čipu. Celkovému hodnocení dominoval operační systém Hive, který ve třech ze čtyřech testovaných kritériích obdržel hodnocení „výborná“.

V průběhu testování jsem byl schopen identifikovat nestabilní chod obou operačních systémů při dlouhodobém používání v případě, kdy byl systém zaváděn z USB zařízení nebo HDD disku. Graf zachycuje výpadky a propady výpočetního výkonu způsobeného paměťovým zařízením (Obrázek 16). Problém s nestabilitou běhu systému vyřešila instalace SSD disku do počítačové sestavy (Obrázek 17).



Obrázek 16 Graf běhu systému (nestabilita), Zdroj: Autor



Obrázek 17 Graf běhu systému s nainstalovaným SSD diskem, Zdroj: Autor

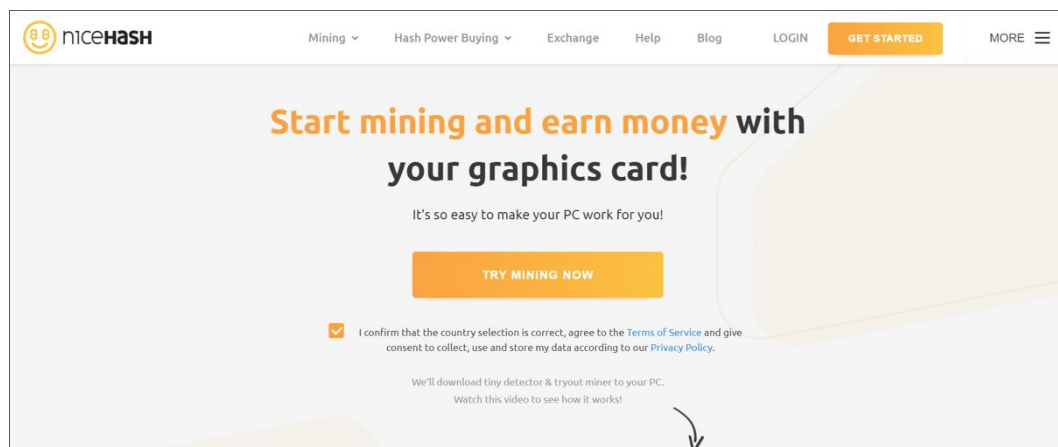
4 Těžební programy NiceHash a CGMiner

Další částí praktického testování těžby kryptoměn byla instalace a testování uživatelsky běžně dostupných programů NiceHash a CGMiner pro platformu Windows. Konkrétní druhy programů jsem vybral v rámci doporučení a recenzí po podrobnějším průzkumu trhu na diskuzních fórech, či zkušenostích uživatelů pohybujících se v oblasti těžby kryptoměn.

4.1 NiceHash

Instalace

Instalace programu NiceHash byla velice jednoduchá a probíhala v pár jednoduchých krocích. V první řadě bylo potřeba stáhnout spustitelný soubor s názvem „NicehashQuickMinerv742.exe“ dostupný na stránkách vývojáře (www.nicehash.com). Kliknutí na tlačítko „Try mining now“ automaticky zahájilo stahování bez nutnosti dosavadní registrace účtu.



Obrázek 18 Webová stránka NiceHash (stažení těžebního softwaru), Zdroj: Autor

Po úspěšném stažení a spuštění instalačního souboru nastalo zobrazení konzolové aplikace a automatické detekci nainstalovaných hardwarových komponent. V této chvíli bylo nezbytné vytvořit uživatelský účet vyplněním registračního formuláře a potvrzení emailové adresy uvedené při registraci. Přihlášením do účtu NiceHash došlo k automatickému propojení konzolové aplikace s webovým prostředím, přičemž byl počítač připraven ke spuštění těžebního procesu po kliknutí na tlačítko „Try mining now“. Z důvodu vestavěné Bitcoinové peněženky nebylo potřeba vytváření a připojování peněženek třetích stran.

```

Excavator v1.6.7c

===== www.nicehash.com =====
Excavator v1.6.7c GPU Miner for NiceHash.
Copyright (C) 2021 NiceHash. All rights reserved.
===== www.nicehash.com =====

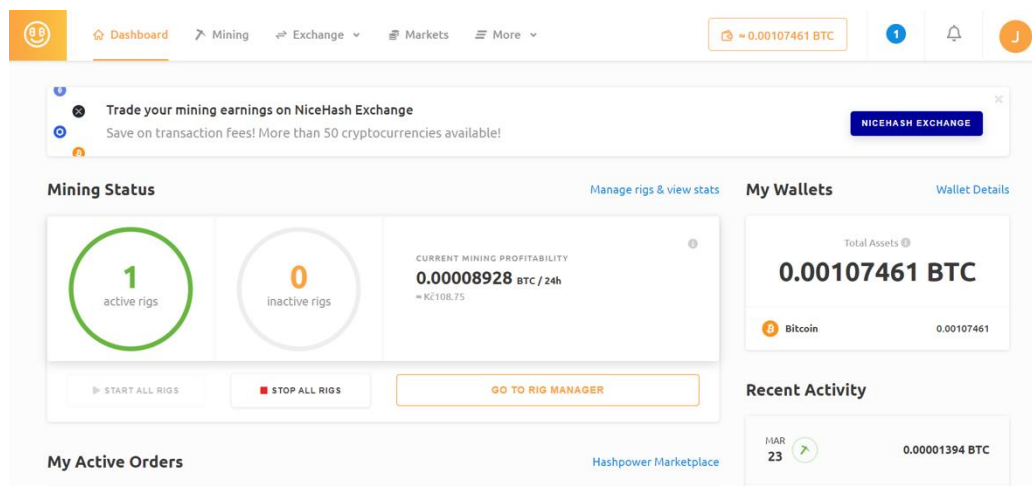
Build time: 2021-03-12 12:43:21
Build number: 742
Provided startup commandline:

    Version: NiceHash QuickMiner
    Automatic hardware detection and mining tryout.
    Please, do not close this window!
    To manage this miner, use your web browser,
    go to: https://www.nicehash.com/quick-miner

[15:40:41][0x000041b0][info] Log started, build v742
[15:40:41][0x000041b0][error] core | No compatible devices found!
[15:40:41][0x000041b0][info] http | Listening on ::1:18000
[15:40:41][0x000041b0][info] core | Initialized!

```

Obrázek 19 Konzolová aplikace NiceHash, Zdroj: Autor



Obrázek 20 Webové rozhraní administrátorského účtu NiceHash, Zdroj: Autor

4.2 CGMiner

Instalace

Samotná instalace programu CGMiner se neobejde bez prvotního založení Bitcoin peněženky, a proto jsem využil k testování svou osobní peněženku od společnosti Coinbase. Dále bylo zapotřebí registrovat účet vhodného těžební poolu, který jsem zvolil na základě doporučení a recenzí, konkrétně se jednalo o Antpool. Registrace probíhala prostřednictvím jednoduchého registračního formuláře na stránkách v3.antpool.com. Po dokončení registrace a přihlášení do administrace jsem byl automaticky vyzván k vytvoření podúčtu spjatého s Bitcoinovou adresou, která slouží k vyplácení těžebních odměn. Posléze stačilo pouze vytvořit pracovní stanici kliknutím na tlačítko „Create Worker“ a zadat název a heslo dle vlastního výběru. Předešlými kroky jsem splnil veškeré podmínky, které bylo nutné splnit před začátkem instalace softwaru.

The screenshot shows the AntPool dashboard. The 'Worker' section is active, displaying a table of workers. The table has columns for Worker Name, 10m, 30m, 1h, 1d, Accepted, Rejected Shares Last 1h (Stale, Dupe, Other), Pay Method, and Diff. A worker named 'Apex.home' is listed with 0.00 H/s across all time intervals and 0 accepted shares. There are buttons for 'Create Worker', 'Delete this group', and 'Batch Operation'.

Worker Name	10m	30m	1h	1d	Accepted	Rejected Shares Last 1h	Pay Method	Diff
						Stale	Dupe	Other
Apex.home	0.00 H/s	0.00 H/s	0.00 H/s	0.00 H/s	0	0	0	0

Obrázek 21 Vytváření nové pracovní stanice v AntPool, Zdroj: https://images.saymedia-content.com/.image/c_limit%2Ccs_srgb%2Cq_auto:good%2Cw_1186/Mtc2NzIzNzYyNzgyNjc2ODU4/how-to-mine-Bitcoins-with-a-gpu-using-cgminer.webp

Samotná instalace CGMineru započala stažením a extrahováním instalačního balíčku do vybrané složky a pokračovala nalezením konfiguračního souboru s názvem „cgminer.conf“. Nalezený soubor jsem otevřel pomocí textového editoru a přepsal hodnoty v poli „pools“ vygenerovanými údaji z uživatelského účtu AntPool. Konkrétně se jednalo o hodnoty atributů url, user a pass. V této fázi procesu instalace stačilo pouze spustit konzolovou aplikaci dvojitým kliknutím na soubor „cgminer.exe“, přičemž došlo k automatickému spojení se serverem a zahájení těžby.

```

F:\cgminer-3.7.2-windows\cgminer.exe
cgminer version 3.7.2 - Started: [2014-01-31 21:04:35]
<5s>:1.390M <avg>:1.132Mh/s ! A:1792 R:0 HW:0 WU:981.6/m
SI: 2 SS: 0 NB: 3 LW: 35 GF: 0 RF: 0
Connected to eu2.multipool.us diff 256 with stratum as user yourworker.1
Block: 3e29b69c... Diff:1.26K Started: [21:06:06] Best share: 3.21K

[P]ool management [G]PU management [S]ettings [D]isplay options [Q]uit
GPU 0: 64.0C 2562RPM ! 693.3K/579.9Kh/s ! A:1024 R:0 HW:0 WU:548.9/m I:13
GPU 1: 66.0C 3381RPM ! 697.1K/582.8Kh/s ! A: 768 R:0 HW:0 WU:452.1/m I:13

[2014-01-31 21:04:35] Switching to pool @ stratum+tcp://eu2.multipool.us:7777
[2014-01-31 21:04:42] Network diff set to 1.26K
[2014-01-31 21:04:52] Accepted b0983ade Diff 371/256 GPU 1 pool @
[2014-01-31 21:04:52] Stratum from pool @ requested work restart
[2014-01-31 21:05:23] Accepted 71c47438 Diff 576/256 GPU 1 pool @
[2014-01-31 21:05:24] Accepted c63468e2 Diff 331/256 GPU 0 pool @
[2014-01-31 21:05:24] Accepted daedae15 Diff 299/256 GPU 0 pool @
[2014-01-31 21:05:43] Accepted 24251b58 Diff 1.81K/256 GPU 0 pool @
[2014-01-31 21:05:44] Accepted 1470ae8f Diff 3.21K/256 GPU 1 pool @
[2014-01-31 21:05:53] Stratum from pool @ detected new block
[2014-01-31 21:05:55] Accepted 6c8f3f94 Diff 604/256 GPU 0 pool @
[2014-01-31 21:06:06] Stratum from pool @ detected new block
  
```

Obrázek 22 Konzolová aplikace CGMiner, Zdroj: <http://cryptomining-blog.com/wp-content/uploads/2014/01/cgminer-3-7-2-gpu.jpg>

4.3 Porovnání těžebních programů NiceHash a CGMiner

Obdobně jako u předešlého hodnocení operačních systémů, tak i zde jsem použil jednoduchou a přehlednou hodnotící tabulku se zkoumanými kritérii.

Tabulka 4 Hodnotící tabulka těžebních programů NiceHash a CGMiner, Zdroj: Autor

KRITÉRIA	NICEHASH	CGMINER
NÁROČNOST INSTALACE	Výborná	Chvalitebná
UŽIVATELSKÁ PŘÍVĚTIVOST	Výborná	Dobrá
TĚŽEBNÍ VÝKON	Chvalitebná	Chvalitebná
DODATEČNÁ KONFIGURACE	Dostatečná	Dobrá

Po důkladném testování dvou zmíněných programů určených k těžbě jsem došel k výsledkům zaznamenaných v tabulce 3, kdy náročnost instalace programu NiceHash

probíhala mnohem jednodušší formou bez nutnosti vytváření účtů třetích stran na rozdíl od alternativy CGMiner. Kritérium uživatelské přívětivosti daných programů se značně lišilo v způsobu ovládání. Zatímco veškeré operace s těžebním procesem v programu NiceHash probíhaly pomocí intuitivního grafického rozhraní webové aplikace, tak v případě ovládání konzole CGMineru jsem se neobešel bez znalosti vývojářem definovaných příkazů, které značně limitovaly práci se softwarem. Hlavním a podstatným kritériem při objevování nových bloků kryptoměn je rychlost těžby v závislosti na které probíhá určování profitu. V obou případech byla těžební rychlost velmi podobná. NiceHash dokázal operovat s rychlostí 50,3 MH/s, zatímco CGMiner s rychlostí 50,6 MH/s. Přesto, že NiceHash nabízí intuitivní rozhraní, dodatečná konfigurace zařízení byla velice omezená, bez možnosti rozšířeného nastavení ovladačů a správy grafické karty. Přísné omezení konfigurace překvapivě neplatilo u programu CGMiner, který nabízel řadu příkazů k dodatečnému nastavení zařízení, monitoringu a také správě ovladačů skrze konzolovou aplikaci. Jak již vyplývá z hodnotící tabulky, každý software nabízel určité výhody a nevýhody. Nicméně NiceHash svou náročností instalace a uživatelskou přívětivostí očividně překonal CGMiner a stal se tak ideálním programem pro začínající těžaře.

5 Operační systém vs software určený pro těžbu

Po dlouhodobém testování způsobů těžby jsem byl schopen vymezit rozdíly mezi využíváním operačních systémů a programů pro MS Windows. V případě vlastnictví počítačové sestavy zaměřené pouze na proces těžby, bez nutnosti využití jiné funkcionality počítače, je ideální způsob instalace operačního systému z důvodu větší stability a možnosti rozšířeného nastavení. Přičemž instalace OS vyžaduje vyšší požadavky na schopnosti uživatele. Jestliže požadavky na instalaci značně převyšují schopnosti uživatele a je vyžadována i jiná funkcionality počítačové sestavy, je preferováno využití těžebního softwaru.

Závěr

V rámci bakalářské práce jsem se věnoval základní charakteristice vybraných druhů kryptoměn, principům fungování a historickému vývoji. Prohloubení znalostí týkajících se této problematiky mi umožnilo vypracovat bakalářskou práci s velice přínosnou praktickou částí z oblasti těžby kryptoměn.

V prvním dílčím cíli jsem se zaměřil na charakteristiku jednotlivých pojmů vyskytujících se v oboru kryptoměn. Definoval jsem fungování blockchain systému a stanovil základní rozdíly mezi digitální měnou, virtuální měnou a kryptoměnou.

Následoval druhý dílčí cíl, ve kterém jsem analyzoval způsoby těžby v závislosti na využití programů, cloudových služeb a fyzických těžebních rigů. Kapitola také definovala rozdíly mezi využitím těžebního výkonu procesoru, grafické karty, logického obvodu a ASIC zařízení. Pomocí takto definovaných rozdílů jsem byl schopen upřednostnit vyhovující typ zařízení splňující těžební požadavky. Pro úplnou orientaci v oboru bylo nezbytné pochopení dílčích pojmů týkajících se provozu těžby a digitálních měn. Vysvětlil jsem fungování tvorby jednotek na principu Proof of work, nezbytné dělení kryptoměn neboli Halving a řešení problému s vysokou náročností těžby prvního bloku pomocí Mining poolu.

V dalším dílčím cíli bakalářské práce jsem se zaměřil na výběr optimální grafické karty na základě výkonnostní tabulky a online kalkulátoru profitability od společnosti NiceHash. V rámci výběru komponent jsem zvolil zakoupení kombinace již použité počítačové sestavy z důvodu nižších finančních nákladů a nové grafické karty RX 5700 XT s 8 GB grafické paměti a dvouletou záruční dobou v případě poruchy. Poté jsem pokračoval kompletací počítačové sestavy určené k těžbě v domácích podmínkách a vyřešení provozních problémů s pevným diskem, či napájecím zdrojem. Následovalo testování stability výkonu těžebního počítače formou benchmark testů, díky kterým jsem byl schopen odhalit negativní účinky spjaté s chlazením komponent, které se mi podařilo odstranit vhodným umístěním ventilátorů a vytvořením jednoduchého vzduchového tunelu z tvrzené PVC fólie. Správné rozvržení ventilátorů a zpracování tunelu zajistilo rovnoměrné proudění nasávaného vzduchu, jenž vedlo k řešení teplotního problému.

Poslední dílčí cíl zahrnoval instalaci operačních systémů a programů tak, aby bylo možné zahájit porovnávání ve formě hodnotící tabulky s předem určenými kritérii. Provedená analýza porovnání systémů na základě definovaných kritérií odhalila preferovaný operační systém Hive, který poskytoval jednodušší formu instalace, lepší uživatelskou přívětivost a rozšířenou

dodatečnou konfiguraci zařízení. Díky těmto faktorům převyšoval konkurenční operační systém SimpleMining. Praktické testování dále pokračovalo stejnou formou u těžebních programů pro platformu Windows. Porovnání programů NiceHash a CGMiner mi umožnilo za použití hodnotících kritérií odhalit vhodnou variantu v podobě softwaru NiceHash.

Z celkové analýzy a porovnání všech kritérií jsem byl schopen stanovit ideální postup pro začínající těžaře. V první řadě je nejdůležitější správná volba hardwarového vybavení počítače, kterou lze značně zjednodušit využitím online nástrojů a informací na výpočet profitability zařízení. Dále je nezbytné stanovení primární specializace sestavy. V případě zaměření počítačové sestavy pouze na těžební proces se jako nejvíce přívětivá forma jeví využití operačního systému Hive. Naopak za podmínek nezbytného využití jiných funkcí stanice, poskytuje vysoký potenciál program NiceHash.

Zdroje a literatura

Seznam použité literatury

BENSON, Jared. *Cryptocurrency mining: The beginner's guide to mining cryptocurrency coins, how to start, mining rigs, ASIC, the best coins to mine*. 1. Kalifornie: CreateSpace Independent Publishing Platform, 2018. ISBN 13:978-1985063228.

G. SOLOMON, Michael. *Ethereum: for dummies*. 1. Kanada: John Wiley, 2019. ISBN 978-1-119-47412-8.

LEWIS, Antony. *The Basics of Bitcoins and Blockchains: An Introduction to Cryptocurrencies and the Technology That Powers Them*. 1. Florida, USA: Mango Publishing Group, 2018. ISBN 978-1-63353-800-9.

PRYPTO. *Bitcoin for dummies*. 1. New Jersey: John Wiley, 2016. ISBN 978-1-119-07613-1.

SÖZE, Keizer. *Blockchain: Novice to Expert*. 1. Sabi Shepherd, 2019. ISBN 978-1839380419.

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

Internetové zdroje

A brief history of Ethereum [online]. 2018 [cit. 2021-03-18]. Dostupné z: <https://coinrivet.com/guides/cryptocurrencies/a-brief-history-of-ethereum/>

A short history of Bitcoin [online]. 2020 [cit. 2021-03-18]. Dostupné z: <https://www.bernardmarr.com/default.asp?contentID=1237>

Alza, Jak funguje těžba Bitcoinu a jak těžit profitabilně? [online]. 2019 [cit. 2021-03-20]. Dostupné z: <https://www.alza.cz/jak-funguje-tezba-Bitcoinu#pool>

An Introduction to Smart Contracts and Their Potential and Inherent Limitations [online]. 2018 [cit. 2021-03-18]. Dostupné z: <https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/>

Benchmark Computer [online]. [cit. 2021-03-19]. Dostupné z: <https://www.techopedia.com/definition/27137/benchmark-computer>

Bit2me, *What is the Ethash mining algorithm* [online]. [cit. 2021-03-19]. Dostupné z: <https://academy.bit2me.com/en/what-is-the-algorithm-of-ethash-mining/>

Bitcoin vs. Litecoin: What's the Difference? [online]. 2021 [cit. 2021-03-18]. Dostupné z: <https://www.investopedia.com/articles/investing/042015/Bitcoin-vs-Litecoin-whats-difference.asp>

Bitcoin.cz, *Princip tezení Bitcoinu* [online]. 2017 [cit. 2021-03-19]. Dostupné z: <https://Bitcoin.cz/index.php/2017/02/24/princip-tezeni-Bitcoinu-teorie-ii/>

BitcoinWiki, *Ethash* [online]. 2020 [cit. 2021-03-19]. Dostupné z: <https://en.Bitcoinwiki.org/wiki/Ethash>

Cloud mining [online]. 2020 [cit. 2021-03-18]. Dostupné z: <https://www.investopedia.com/terms/c/cloud-mining.asp>

Cryptocurrency [online]. 2021 [cit. 2021-03-18]. Dostupné z: <https://www.investopedia.com/terms/c/cryptocurrency.asp>

Cryptorival, *SHA-256* [online]. [cit. 2021-03-19]. Dostupné z: <https://cryptorival.com/algorithms/sha256/>

Cryptorival, *Skrypt* [online]. [cit. 2021-03-19]. Dostupné z: <https://cryptorival.com/algorithms/scrypt/>

Digital currency [online]. 2020 [cit. 2021-03-18]. Dostupné z: <https://www.investopedia.com/terms/d/digital-currency.asp>

Distributed ledger technology (DLT) [online]. 2017 [cit. 2021-03-18]. Dostupné z: <https://searchcio.techtarget.com/definition/distributed-ledger>

Ether (ETH) [online]. 2021 [cit. 2021-03-18]. Dostupné z: <https://www.investopedia.com/terms/e/ether-cryptocurrency.asp>

FILLNER, Karel. *Jak na Bitcoin: Krok za krokem* [online]. 2017 [cit. 2021-03-18].

Finance, *Ekologie a kryptoměny – čeká nás zajímavá budoucnost?* [online]. [cit. 2021-03-27]. Dostupné z: <https://www.finance.cz/499524-ekologicke-kryptomeny/>

Fungibility Monero [online]. 2021 [cit. 2021-03-18]. Dostupné z: <https://www.getmonero.org/resources/moneropedia/fungibility.html>

Fxstreet, *Cloud mining jednoduché a levné s platformou Hashtoro* [online]. 2018 [cit. 2021-03-20]. Dostupné z: <https://www.fxstreet.cz/zpravodajstvi-98053.html>

Gleton, *Software v oblasti kryptoměn* [online]. [cit. 2021-03-20]. Dostupné z: <https://gleton.cz/blog/software-v-oblasti-kryptomen>

Hashgains, *Cryptocurrency mining algorithms* [online]. [cit. 2021-03-19]. Dostupné z: <https://www.hashgains.com/wiki/c/what-is-cryptocurrency-mining-algorithms>

History of Litecoin [online]. 2021 [cit. 2021-03-18]. Dostupné z: <https://www.coinhouse.com/Litecoin-price/>

Is Bitcoin anonymous [online]. 2020 [cit. 2021-03-18]. Dostupné z: <https://Bitcoinmagazine.com/learning-Bitcoin/is-Bitcoin-anonymous>

Kryptoguru, *Plaforma HiveOS* [online]. 2020 [cit. 2021-03-20]. Dostupné z: <https://kryptoguru.cz/platforma-hive-os-videonavod-registrace-instalace-a-nastaveni/>

Kryptomagazin, *Co je to ASIC miner a jak funguje?* [online]. [cit. 2021-03-20]. Dostupné z: <https://kryptomagazin.cz/co-je-to-asic-miner-a-jak-funguje-kvalitni-informace-pro-vsechny-zajemce-o-tezbu-kryptomen/>

Kryptoměna Ripple (XRP) [online]. 2021 [cit. 2021-03-19]. Dostupné z: <https://finex.cz/kryptomena/xrp-ripple/>

Kurzy, *Co je to Bitcoin* [online]. 2021 [cit. 2021-03-20]. Dostupné z: <https://www.kurzy.cz/Bitcoin/co-je-to-Bitcoin>

Kurzy, *Halving - halving Bitcoinu a ostatních kryptoměn* [online]. 2021 [cit. 2021-03-19]. Dostupné z: <https://www.kurzy.cz/kryptomeny/halving/>

Litecoin (LTC) [online]. 2021 [cit. 2021-03-18]. Dostupné z: <https://www.investopedia.com/terms/l/Litecoin.asp>

Malone, David & O'Dwyer, K.J.. (2014). *Bitcoin Mining and its Energy Footprint*. 280-285. 10.1049/cp.2014.0699.

Mining pool [online]. 2020 [cit. 2021-03-18]. Dostupné z: https://en.Bitcoin.it/wiki/Pooled_mining

Mining rig [online]. 2015 [cit. 2021-03-18]. Dostupné z: https://en.Bitcoin.it/wiki/Mining_rig

Proof of Work [online]. 2020 [cit. 2021-03-18]. Dostupné z: <https://www.investopedia.com/terms/p/proof-work.asp>

QUEST, Martin. *Cryptocurrency master bundle: The art of hodling crypto mining mindset the ico approach cryptocurency 101 blockchain dynamics* [online]. 2018. [cit. 2021-03-18].

Security tokens vs. Utility tokens: a concise guide [online]. [cit. 2021-03-19]. Dostupné z: <https://www.blockchain-council.org/blockchain/security-tokens-vs-utility-tokens-a-concise-guide/>

SerHack, *Mastering Monero: The future of private transactions* [online]. 1. 2020 [cit. 2021-03-18]

SerHack, *Mastering Monero: The future of private transactions* [online]. 1. 2020 [cit. 2021-03-18]

Stable coins [online]. [cit. 2021-03-19]. Dostupné z: <https://www.alza.cz/stable-coins>

Virtual Currency [online]. 2020 [cit. 2021-03-18]. Dostupné z: <https://www.investopedia.com/terms/v/virtual-currency.asp>

What is Altcoin [online]. [cit. 2021-03-19]. Dostupné z: <https://www.techslang.com/definition/what-is-an-altcoin/>

What is Bitcoin and how does it work [online]. 2021 [cit. 2021-03-18]. Dostupné z: <https://www.bbc.co.uk/newsround/25622442>

Wikisofia, *Blockchain* [online]. [cit. 2021-03-26]. Dostupné z: <https://wikisofia.cz/wiki/Blockchain>

Seznam obrázků a tabulek

- Obrázek 1 <https://bitpanda-academy.imgix.net/null19b43d8e-81e7-487a-a776-3c887d4c6450/bitpanda-academy-intermediate-16-segwit-infographic.png?auto=compress%2Cformat&fit=min&fm=jpg&q=80&w=2100>
- Obrázek 2 Spotřeba elektrické energie těžbou Bitcoinu v porovnání s běžnou spotřebou konkrétních zemí, Zdroj: <https://powercompare.co.uk/wp-content/uploads/Bitcoin-mining-as-share-world.png>
- Obrázek 3 Kalkulátor NiceHash, Zdroj: Autor
- Obrázek 4 Výstup kalkulátoru NiceHash, Zdroj: Autor
- Obrázek 5 Původní teplotní výstup benchmark testu 3DMark, Zdroj: Autor
- Obrázek 6 Problematické proudění vzduchu v těžební sestavě, Zdroj: Autor
- Obrázek 7 Vzduchový tunel k chlazení horní části grafické karty, Zdroj: Autor
- Obrázek 8 Teplotní výstup benchmark testu 3DMark s nainstalovaným vzduchovým tunelem, Zdroj: Autor
- Obrázek 9 Typy instalace operačního systému HiveOS, Zdroj: Autor
- Obrázek 10 Program na tvorbu bootovacích zařízení, Zdroj: Autor
- Obrázek 11 Seznam souborů vytvořeného bootovacího USB softwarem Rufus, Zdroj: Autor
- Obrázek 12 Formulář přidávání pomoci „Add worker“, Zdroj: Autor
- Obrázek 13 Propojené těžební zařízení ve webovém rozhraní HiveOS, Zdroj: Autor
- Obrázek 14 Instalační soubor SimpleMining, Zdroj: Autor
- Obrázek 15 Software Etcher k tvorbě bootovacího zařízení, Zdroj: Autor
- Obrázek 16 Graf běhu systému (nestabilita), Zdroj: Autor
- Obrázek 17 Graf běhu systému s nainstalovaným SSD diskem, Zdroj: Autor
- Obrázek 18 Webová stránka NiceHash (stažení těžebního softwaru), Zdroj: Autor
- Obrázek 19 Konzolová aplikace NiceHash, Zdroj: Autor
- Obrázek 20 Webové rozhraní administrátorského účtu NiceHash, Zdroj: Autor
- Obrázek 21 Vytváření nové pracovní stanice v AntPool, Zdroj: https://images.saymedia-content.com/.image/c_limit%2Ccs_srgb%2Cq_auto:good%2Cw_1186/MTc2NzIzNzYyNzgyNjc2ODU4/how-to-mine-Bitcoins-with-a-gpu-using-cgminer.webp
- Obrázek 22 Konzolová aplikace CGMiner, Zdroj: <http://cryptomining-blog.com/wp-content/uploads/2014/01/cgminer-3-7-2-gpu.jpg>

Tabulka 1 Srovnání grafických karet vhodných na těžbu, Zdroj: https://www.computerlounge.co.nz/data/media/images/blog//gpu_hash_rates.png

Tabulka 2 Srovnání původního způsobu chlazení a chlazení s nainstalovaným vzduchovým tunelem, Zdroj: Autor

Tabulka 3 Hodnotící tabulka operačních systémů v závislosti na zkoumaných kritériích, Zdroj: Autor

Tabulka 4 Hodnotící tabulka těžebních programů NiceHash a CGMiner, Zdroj: Autor

Abstrakt a klíčová slova

Bibliografický údaj: BLABLA, Jiří. Kryptoměny a porovnání způsobů těžby. Olomouc, 2021.

Bakalářská práce. Moravská vysoká škola. Vedoucí práce PhDr. Jan Lavrinčík, Ph.D.

Moravská vysoká škola Olomouc	
Název práce:	Kryptoměny a porovnání způsobů těžby
Autor:	Jiří Blabla
Vedoucí práce:	PhDr. Jan Lavrinčík, Ph.D.
Počet stran:	54
Abstrakt:	Hlavním cílem této bakalářské práce je analýza způsobů těžby v závislosti na druhu použitého operačního systému nebo softwarového vybavení. Na základě analýzy určit nejvhodnější a nejefektivnější typ těžby
Klíčová slova:	Kryptoměna, blockchain, těžba, Bitcoin, ASIC

Moravská vysoká škola Olomouc	
Title:	Cryptocurrencies and comparsion of mining methods
Author:	Jiří Blabla
Supervisor:	PhDr. Jan Lavrinčík, Ph.D.
Number of pages:	54
Abstract:	The main goal of this thesis is the analysis of mining methods depending on the type of operation system or software. Determine the most suitable and efficient type of minig based on the analayzes.
Keywords:	Cryptocurrency, blockchain, mining, Bitcoin, ASIC