Univerzita Hradec Králové
Fakulta informatiky a managementu
katedra informačních technologií

BAKALÁŘSKÁ PRÁCE

Využití grafických karet se zaměřením na těžbu kryptoměn

Autor: Jiří Kalous

Vedoucí práce: doc. Ing. Hana Tomášková, Ph.D.

Září, 2018

Prohlášení

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně a uvedl jsem všechny použité prameny a literaturu.

V Hradci Králové dne 3. září 2018 Kalous Jiří

Poděkování

Děkují paní doc. Ing. Haně Tomáškové, Ph.D. za poskytnuté informace, čas, snahu a především trpělivost, kterou mi věnovala při přípravě a při vyhotovení bakalářské práce.

Anotace

Bakalářská práce se zaměřuje na analýzu a návrh sestavy menší těžební sestavy. V práci je představen úvod aktuální problematiky těžení kryptoměn a popis s tím souvisejícího hardwaru. Následně ukazuje praktickou stavbu, testování těžební sestavy a její software konfiguraci. Výsledkem je funkční a otestovaná těžební sestava.

Annotation

This bachelor thesis, The use of graphics cards with focus on crypto mining, is dedicated to the creation of a small crypto mining rig. The thesis composes of an introduction into crypto currency mining and the description of the necessary hardware. Furthermore it depicts the practical side of building and testing of the rig and its software configuration. The result of this thesis is a functional and tested mining rig.

Obsah

1 Úvod

V dnešní době je pojem kryptoměna, Bitcoin a těžba kryptoměn již poměrně známou záležitostí, ale běžný člověk, který nemá přehled v informačních technologiích či technologiích obecně může být zahlcen kvantem informací, které téma kryptoměn a jejich těžby obnáší.

Tato práce se tedy snaží toto téma i s ním spojenou terminologii a hardware lépe nastínit, podat základní, ale důležité informace potřebné k tvorbě podnětu pro čtenáře, který by mohl vyústit ve větší zájem o kryptoměny, jejich těžbu nebo alespoň o hardware s tímto tématem spojený.

Lze zde najít jak obecné informace, které seznámí s jednoduchými základy tak i podrobné informace které navedou ke specifickým kryptoměnám či ke komplikovanějším činnostem jako přenastavení BIOS základní desky a taktování grafických karet. Tyto informace slouží k vyjasnění potřebných základů, které lze využít při vlastní stavbě těžební soustavy či zájmu se do této technologie angažovat.

1.1 Cíl práce

Cílem této práce je vybrat komponenty, postavit těžební soustavu se zaměřením na těžbu kryptoměn, kdy se otestuje těžba několika vybraných kryptoměn s výchozím nastavením grafických karet.Také se představí pojem výtěžnosti a dále se tyto grafické karty přenastaví, respektive taktují a testuje se vliv těchto změn na těžbu. Čímž se dokazuje, že taktování grafických karet má převážně pozitivní vliv na těžební sestavy.

2 Historie PC a grafické karty

Historii počítačů lze rozdělit na několik generací. Jak je uvedeno v článku Allana Bromleyho [5], lze zmínit například první generaci počítačů a to konkrétně „Analytický stroj“, který navrhl anglický profesor matematiky Charles Babbage, kterým stanovil základní framework dnešních počítačů [5]. Další vývoj samozřejmě vedl k počítačům tak jak je známe dnes.

2.1 Počítače a jejich využití

Počítače se neustále vyvíjejí a jejich využití s nimi. Počínaje vědeckými účely jako je například vývoj nových zbraní, léků, tak k dostání prvního člověka na měsíc a končící dnešní érou zmenšování, vývoje umělých inteligencí, navyšování efektivity hardware a nasazení počítačů do téměř všech aspektů našich životů.

2.2 Počítače tak jak je známe dnes

Dnes lze vidět počítače i mobilní zařízení v každodenním životě a to téměř ve všech odvětvích. Ať už používáme mobilní zařízení, které je v podstatě miniaturní osobní počítač, jako budík, či jako ranní zdroj informací.

Dále pak vidíme počítače, či jimi řízené komponenty. Potkáváme video billboardy, bankomaty, interaktivní tabule v nákupních centrech, LED informační tabule na nádražích a toto vše je řízeno počítači. Můžeme tedy říci, že počítače začínají řídit náš život.

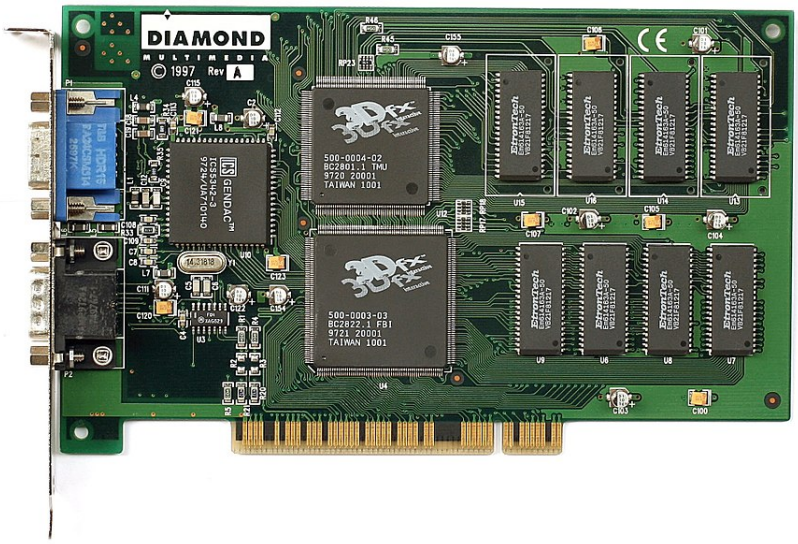
V současné době, resp. mezi roky 2014 a 2018, probíhá rozmach kryptoměn a jejich těžení. Zde je tedy třeba představit specifické komponenty počítačů, konkrétně grafický adaptér, který nám poskytuje dříve nepředstavitelné možnosti paralelních výpočtů, díky kterému je rozmach kryptoměn a umělých inteligencí možný.

2.3 Počátky grafických karet

Mezi první moderní grafické karty lze zařadit výrobek společnosti 3Dfx, kartu „Voodoo“, která byla vydána v listopadu roku 1996. Jednalo se pouze o 3D kartu, ta tedy vyžado-

vala VGA Pass through kabel pro připojení oddělené 2D karty a až poté bylo možno tuto kartu připojit k monitoru.

Grafické karty „Voodoo“ dali uživatelům a především vývojářům aplikací mocný nástroj. Karty tehdy způsobily revoluci grafiky osobních počítačů téměř přes noc a v jistém smyslu slova, nastavily standard, kterého se okamžitě chytily další společnosti. Dnes jimi jsou světoví giganti AMD a NVidia, přičemž grafické karty AMD dříve spadali pod společnost ATI, která byla převzata společností AMD.



Obrázek 2.1: 3Dfx „Voodoo“ první generace, obrázek převzat z portálu Mybroadband [21]

Za jako další milník lze považovat uvedení grafické karty Geforce 256 na trh. Jedná se o první grafickou kartu s označením GPU, tedy grafická procesorová jednotka. A to z důvodu přidání hardware transformací a světelného enginu, které obsluhovali kalkulaci náročných transformací 3D objektů a scén a s nimi spojeným osvětlením. Tato karta byla tedy první, kde došlo k využití programovatelných pixel shaderů, shadery slouží k výpočtu renderování efektů, nyní jsou součástí všech grafických karet. O rok později vyšla verze této karty s pamětí typu DDR. DDR je označení pro paměti, které využívají jak horních tak i dolních signálů, lze si představit vrchní a spodní hrany digitálního signálu. NVidia se rozhodla nahradit paměť SDR a tím dosáhli větší propustnosti dat a velikosti paměti.

3 Moderní grafické karty

Dříve se vývoj grafických karet řídil především dvěma vlivy a to bylo dosažení vyššího, v té době nevídaného výkonu a usurpování stabilní pozice na rozsáhlém trhu. Tuto bitvu samozřejmě vyhráli giganti AMD a NVidia. Společnost AMD se však do výslunní ve světě grafických karet zasloužilo převzetím společnosti ATI a navázáním na nově obdrženém duševním vlastnictví, kde se nebálo inovovat a vytvořit tak konkurenci společnosti NVidia.

Dnes tedy zbývá pouze NVidia a AMD. Tyto společnosti si stále konkurují a právě díky nim se grafické karty využívají hojně v nejrůznějších oborech a aplikacích. Jejich aplikace lze vídat ve vědě, medicíně či například v rozvoji umělé inteligence. To však není jejich limit, jelikož téměř všude, kde je potřeba vysokého paralelního výpočetního výkonu, tam lze s výhodou aplikovat grafické adaptéry.

Obrázek 3.1: Ukázka High-range grafické karty NVidia GTX 1080, obrázek převzat z portálu Pugetsystems [11]

Na trhu se výše zmínění konkurenti snaží vyhovět všemožným uživatelským požadavkům. Například co se herních počítačů týče, se firma AMD snaží uspět způsobem vydáváním grafických karet, které jsou výkonově téměř srovnatelné, avšak s velkým cenovým rozdílem, kdy lze na srovnatelné grafické kartě od AMD ušetřit 10-20 % ceny protějšku od společnosti NVidia. Samozřejmě, pokud je hledán výkon, tak nelze udělat

špatný krok při volbě High-range grafických karet společnosti NVidia.

Dále lze porovnávat grafické karty v rámci uprav různých výrobců, kdy si grafické čipy kupují společnosti jako Asus a Sapphire, které provádí změny nejen v rámci čipů ale celého tištěného obvodu, může tedy tak dojít k navýšení obnovovací frekvence GDDR pamětí či jádra.

3.1 Využití grafických karet

Grafické karty se posunuli z jednoduchých 3D akcelerátorů na specializované čipy, využitelné nejen v grafických oborech. Díky dříve nepředstavitelnému výkonu, který nám dnešní karty podávají, nastala doba kryptoměn, virtuální či upravené reality a vývoje doposud nevídaných umělých inteligencí.

Dnes můžeme říct, že grafické karty nedrží své využití pouze v grafickém světě a lze tak předpokládat, že pojem GPU, tedy Graphics processing unit se nejspíše v blízké budoucnosti vystaví změnám z důvodu další specializace tohoto hardware či naopak jeho zobecnění. Dřívější použití bylo téměř vyhrazené v počítačové grafice, nyní jsou grafické karty schopné mnoha různých úkonů a výpočtů.

3.2 Rozdělení grafických karet do kategorií

Grafické karty se dnes běžně rozdělují do několika kategorií či tříd. Jak uvádí Brad Borque na webovém portálu Digitaltrends [4], tyto kategorie lze označit jako budget, mid-range a high-range, resp. rozpočtová, střední a vyšší kategorie.Každá z těchto kategorií se řídí především podle cen grafických karet v poměru ku jejich výkonu.

3.2.1 Kategorie Budget

Jak už název této kategorie napovídá, jedná se o kategorii nejnižší. Na webovém portálu Digitaltrends se uvádí, že je to tedy kategorie, kde se vyskytují grafické karty s nízkým výpočetním výkonem, ale také s velmi nízkou cenou [4]. Jedná se často o grafické karty, které najdou své využití například v kancelářských oborech, kdy je zapotřebí propojení osobního počítače s více monitory pro umožnění efektivnějšího multitaskingu, což je provádění více operací najednou, či je lze najít v osobních počítačích v domácnostech, které počítač používají jako část domácího kina, kde jsou využity, aby počítači dodali potřebný výkon k zobrazování 4K filmů.

Samozřejmě výše zmíněné využití nemusí být jediné, tuto kategorii grafických karet, lze často vidět v sestavách nadšenců, kteří se snaží nepřesáhnout určitý práh spotřeby elektrické energie, či tvorba tiché sestavy, kdy se z osobního počítače odeberou všechny komponenty, které obsahují mechanické součástky a energeticky náročné

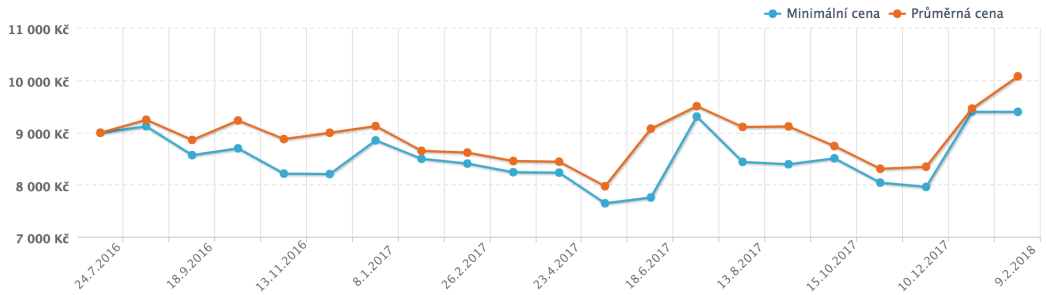
komponenty se nahradí za nenáročné, čímž se tedy dosáhne možnosti pasivního chlazení a tím tedy i odhlučnění soustavy.

3.2.2 Kategorie Mid-Range

V této kategorii lze jako využití brát výkon při hraní počítačových her. Tento výkon je samozřejmě relativní, jelikož se odráží ne jen od výkonu grafických karet, ale na komponentách celé sestavy a také na optimalizaci pro daný hardware. Avšak v této kategorii už nastupuje užití a problematika těžení kryptoměn, kde si mnoho těžařů vybírá Mid-Range grafické karty, protože se nemusí nutně vyplatit nárůst výkonu s cenou ve vyšších kategoriích grafických karet. V tomto ohledu těžaři nehledí pouze na poměr cena výkon, ale také na spotřebu, jelikož se v těžařských soustavách nevyužívají jednotlivé karty, ale většinou rovnou několik najednou.

Tato kategorie, se co se týče využití pro hraní počítačových her, často řídí trendy,dle aktuální technologie, jaký je stav trhu s hardware a také jaké byly stanovené cíle výkonu soustavy. Toto ovlivňuje mnoho aspektů, mezi ně lze zařadit například cílené rozlišení, obnovovací frekvenci displeje, či určité grafické nastavení v jednotlivých hrách.

Karty z této skupiny, jak je již výše zmíněno, jsou ovlivněny těžením kryptoměn. V roce 2017 došlo k velkému výkyvu cen grafických karet ve všech kategoriích, ale především v Mid-Range, kde například v polovině roku 2017 grafické karty GTX 1060 od společnosti NVidia měly téměř 30% nárůst cen. Příčinou tohoto, byl boom kryptoměny zvané Ethereum.



Obrázek 3.2: Graf ceny NVidia GTX 1060, převzato z portálu Heureka.cz [16]

Na výše uvedeném obrázku,lze vidět vliv růstu kryptoměny Ethereum na cenu Mid-Range grafických karet, jako je právě například výše zmíněná NVidia Gtx 1060. Toto mělo u mnoho prodejců za následek dlouhý nedostatek zboží, jelikož populace krypto těžařů zažila díky Ethereu velký růst.

3.2.3 Kategorie High-Range

Jak se uvádí na webovém portálu Digitraltrends, tato kategorie je určena především pro nadšence a fanoušky tohoto hardware, či využití, které vyžadují naprosto nejvyšší možný výkon [4]. Zanedbává se ohled na poměr cena/výkon a většinou se grafická karta volí dle požadavků sestavy. V této kategorii se často vyskytují tak zvaní „buildeři". Jedná se o lidi či týmy lidí, kteří jsou nadšenci počítačového hardware a staví tak často extravagantní či speciální počítačové sestavy.

V případě těchto speciálních sestav se velmi často grafické karty upravují. Mezi nejčastější úpravy patří způsob chlazení. Buildeři tedy volí namísto chlazení grafické karty vzduchem chlazení vodou, kdy se vymění celá chladící soustava a zbude tak tedy pouze samotná karta na kterou se montuje vodní blok, který funguje na bázi cirkulace tekutiny, ať už vody či jiných chladících kapalin [4].

Vodní chlazení lze využít k dosažení vyšších taktů jak na jádře tak i pamětích grafické karty, to však má za následek zvýšení teplot grafické karty a je jí tak třeba efektivněji chladit. Toho tedy dosáhneme cirkulací chladící tekutiny o což se stará pumpa, která je součástí oběhu a o samotné ochlazení kapaliny se stará radiátor, kterým smyčkovitě kapalina prochází přičemž na radiátor je hnán ventilátory vzduch, kapalina je tedy tímto způsobem chlazena.

Tato technologie se rovněž využívá při chlazení procesorů, kde se stejným způsobem vymění pasivní chlazení či kombinace pasivního chladiče a ventilátoru za jeden vodní blok, kterým je cirkulována chladící kapalina.

Obrázek 3.3: Ukázka grafické karty NVidia GTX 1080 s namontovaným vodním blokem, převzato z webového portálu CZC [14]

3.3 Specializované grafické karty a ASIC

3.3.1 Grafické karty NVidia Quadro

Jak uvádí autor na webové stránce Velocitymicro [12], největší rozdíl mezi obyčejnými kartami Geforce a kartami serie Quadro je jejich využití. Kdy klasické karty od AMD nebo NVidia Geforce jsou pro běžné použití, tak grafické karty NVidia Quadro jsou zaměřené pro specifické využití do pracovních stanic.

Jako rozdíly v užití mezi těmito kartami lze začít s tradičními kartami. Tyto karty jsou běžně dostupné ať už se jedná cenových kategorií tak i obecné dostupnosti na trhu. Kategorie grafických karet jsou zmíněny v předešlé části této práce.Na druhou stranu tedy grafické karty NVidia Quadro jsou grafické karty specializované a velmi drahé. Aktuální generace se začíná pohybovat s nejnižším modelem NVidia Quadro P4000 kolem ceny 20.000,- Kč a nejvyšším modelem kolem ceny 200.000,- Kč. Je tedy zřejmé, že tyto grafické karty jsou určeny profesionálům.

Grafické karty NVidia Quadro jsou zaměřeny na profesionální účely, můžeme tedy zmínit například CAD kresby v programech jako je AutoCAD. Tento hardware tedy nabízí jisté změny v renderování a především nabízí vyšší výkon. Pro příklad výkonu lze uvést Quadro GP100, která se pyšní 3584 CUDA jádry, které slouží jako jádra pro paralelní výpočty, dále 16 Gigabyty paměti typu HBM2 a vysokým výkonem výpočtu Dual Precision Floating Point, tedy výpočty s pohyblivou desetinnou čárkou.

Díky své specializaci jsou však tyto karty nevhodné pro těžbu kryptoměn. Mají jedny z nejhorších poměrů nákladů/návratnosti. Lze je nahradit obyčejnými kartami, které cenově často vycházejí i pod 50 procent ceny karet NVidia Quadro. S tímto tedy souvisí problém návratnosti počáteční investice. Tyto specializované grafické karty nejsou uzpůsobeny činnosti jako je právě těžba kryptoměn a postrádá tedy smysl je na takovéto činnosti využívat.

3.3.2 Specializovaný hardware ASIC

Těžební hardware ASIC, tedy integrovaný obvod pro specifické použití, je hardware, který jak jeho název napovídá specializovaný. V dnešní době, je tento hardware využit k těžbě kryptoměn. Jak uvádí autoři na portálu Vice Motherboard, ASIC hardware změnil způsob těžby Bitcoinu(dále jen BTC) na obří průmysl, který spotřebovává velké množství elektřiny a generuje značné množství výdělku pro výrobce tohoto hardware [22].

ASIC je tedy jak je výše zmíněno určen pouze a jedině na jednu činnost a to těžení kryptoměn a také se zaměřením na jediný typ kryptoměn. Znamená to tedy, že s ASIC na těžbu BTC nelze těžit jakékoliv jiné měny. Jejich usměrnění však přináší určitou vý-

hodu a to, díky své specializaci na pouze jednu jedinou činnost mohou poskytnout neporovnatelně vyšší výkon oproti grafickým kartám. Schází jim tak ale multifunkčnost, kterou grafické karty nabízí v možnosti využití pro těžbu jiných kryptoměn.

Lze tedy říci, že poté, co přestane ASIC miner těžit danou kryptoměnu, je tento hardware více méně dále nepoužitelný. Jeho specializace omezuje nejen jeho znovu použitelnost, ale také možnost prodeje. Grafické karty je převážně možné po určité době použití prodat a vzniká tím další vratná hodnota ze základní investice, či alespoň hodnota, kterou lze využít při vylepšení dosavadních soustav lepším hardwarem.

Tento hardware bohužel také přináší problém monopolizace, kdy investoři s větším kapitálem mohou využít ASIC sestavy v takové míře, kdy běžný těžař s klasickou sestavou není schopný konkurovat farmám, které se skládají právě z obřích propojených ASIC sestav. Tyto farmy mají nesrovnatelný výpočetní výkon oproti těžařům a mají tedy větší šanci na výdělek.

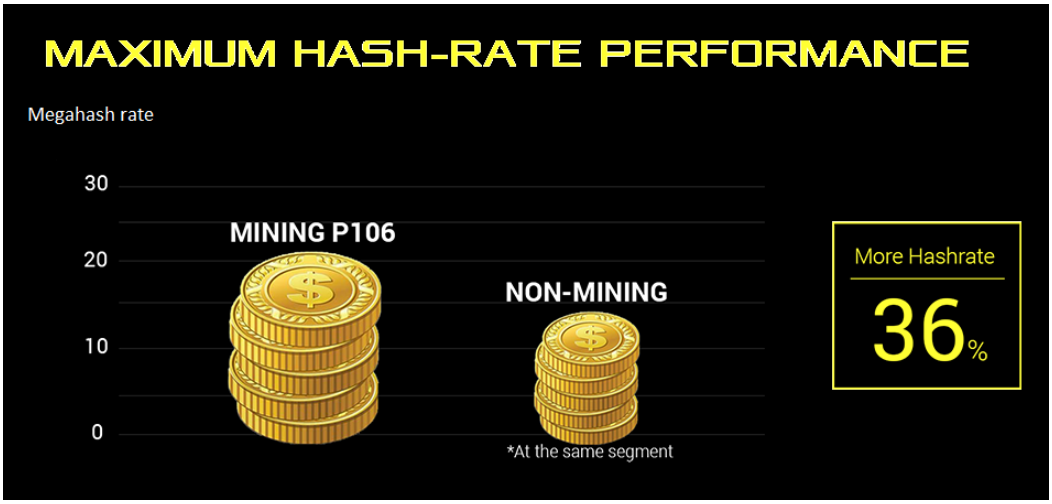
K tomuto tématu autor na serveru Beebon [19] uvádí, že s růstem kompetitivnosti těžby BTC, lidé přecházejí k těžbě jiných kryptoměn, značených Alt Coins, jako například Dash, které lze těžit snadněji. Pokud tedy BTC netěžíme pro naučné účely, je lepší těžbu BTC ponechat gigantům z Číny, Indie a Východní Evropy, kteří kontrolují většinu tohoto trhu. Běžní těžaři se tomuto mohou bránit těžbou v poolu, což lze pojat jako skupinu tvořenou jedinci se stejným zájmem. Menší těžaři tedy spojí svůj výpočetní výkon a jsou tak schopni konkurence.

Obrázek 3.4: Ukázka specializovaného hardware ASIC model Antminer 9, se zaměřením na těžbu kryptoměny BTC, převzato z webového portálu Beebom [19]

3.3.3 Specializované těžební karty Nvidia

Těžební mánie se již zúčastnili i výrobci grafických karet a to například společnost Asus, která ve spolupráci se společností NVidia upravila grafickou kartu p106-100, která je základem pro grafické karty NVidia Geforce gtx 1060. Asus, výrobce těchto specializovaných grafických karet, uvádí výhody jako zvýšení výkonu v megahash o 36 procent oproti grafickým kartám ve stejné kategorii, které ale nejsou specializovány na těžbu měn. Tyto nové grafické karty jsou také navrženy pro větší trvanlivost a nepřetržitý běh [3].

Jak je uvedeno výše, tyto grafické karty jsou stavěny pro vyšší a stálou zátěž. S vyšší sazbou megahash oproti své konkurenci ve své kategorii jsou tyto karty tedy lákavé, pro větší zisk v poměru investice ku návratu. Je ale také třeba se zamyslet, zdali bude možné tento hardware dále po určité době, kdy by mohl nastat prudký pád kryptoměn, dále prodat či jinak využít. Díky specializaci grafických karet a využití, které bývá běžně nepřetržité lze očekávat, že tyto grafické karty nebude vůbec možné prodat.



Obrázek 3.5: Graf porovnání sazby megahash tak jak je uveden na portálu výrobce ASUS. [3]

3.3.4 PCI Redukce neboli Risery

S problematikou těžení kryptoměn za pomoci grafických karet a co nejlepšího poměru investice ku návratnosti jsou spojeny i PCI redukce, díky kterým lze dosáhnout lepšího využití základních desek. Umožňují totiž zapojení většího množství grafických karet, které využívají sběrnice standardu PCI nebo PCI Express.

4 Historie a terminologie kryptoměn

Téměř každý si pod pojmem kryptoměny představí něco jiného. Pro mnoho lidí je toto téma úplně cizí a pouze si kryptoměny spojují s něčím finančně mimo dosah a bez smyslu investice, nebo jak o příliš nestabilní způsob příjmu. Je tedy třeba vysvětlit alespoň část historie kryptoměn a nezbytné pojmy. A to decentralizace, peer to peer, šifrování a pseudoanonymita.

4.1 Historie digitálních měn

Již v osmdesátých letech minulého století se řešila problematika elektronických plateb a automatizace plateb. Toto se mělo právě řešit novým způsobem kryptografie, kdy se řešily problémy jako například neschopnost určení jedince třetími stranami, počet a časy jeho transakcí.

Zároveň ale také bylo chtěné, aby bylo možné doložit důkaz o provedení platby a v krajních případech i určit identitu plátce. Toto téma rozvádí a navrhuje v článků řešení mnohých problémů již v roce 1983, David Chaum z University of California.[6].

Myšlenky o kryptoměnách vznikaly již v devadesátých letech minulého století. Kdy si skupina známá jako Cypher Punks myslela[17], že vláda spojených států a korporace měly příliš velkou nadvládu nad jejich životy.

Právě tehdy se začlo přemýšet o kryptoměnách a dosáhnutí tak větší svobody nad financemi a informacemi. Tohoto se mělo dosáhnout za pomoci kryptografie. Skupina Cypher punks se tedy především snažila o uvedení digitálních měn. Bohužel oba jejich pokusy o uvedení a udržení digitálních měn, DigiCash a CyberCash, selhaly [17]. Příčinou byl nedostatek potřebných vlastností, kterými kryptoměny disponovaly, aby mohly být opravdu kryptoměnami.

Toto se změnilo až v roce 2009, kdy vznikl první plně decentralizovaný svět digitálních financí s příchodem kryptoměny BTC.

4.2 Historie kryptoměny Bitcoin

Historie dnes snad nejznámější kryptoměny BTC není zcela úplná. Důvodem je neznámá identita prvotního jedince či skupiny, která se světu prokazuje jako jakýsi Sa-

toshi Nakamoto. Z tohoto jména lze rychle usoudit, že se jedná o muže japonské národnosti.

Od roku 2008, kdy tento jedinec či skupina poprvé vydali článek tzv. Bitcoin White Paper [17], který popisuje co to BTC je a zároveň také jak funguje, je snaha o odhalení identity Satoshi Nakamota. Dosud se krom obecných údajů jako například časová zóna, které odpovídají pohyby GITu, stále nikomu jeho pravou identitu nepodařilo odhalit.

Výše zmíněný článek Bitcoin White Paper se stal modelem pro návrh budoucích kryptoměn. Z počátku roku 2009 [17] Satoshi Nakamoto provedl první BTC transakci a po této velké události v průběhu dalších dvou let Satoshi Nakamoto zmizel a pozůstala po něm měna, která poskytuje oproti běžným měnám bezkonkurenční svobody a nezávislost na světových vládách.

Obrázek 4.1: Dorian Satoshi Nakamoto, poté co byl nařknut ze spojení s měnou BTC, převzato z portálu Mashable [24].

Na výše uvedeném obrázku 4.1, lze vidět pana Doriana Satoshi Nakamota, který poté, co byl nařknut ze spojení s BTC a jeho autorstvím toto vše zamítl a vyvrátil tím, že v té době pro nikoho a na ničem nepracoval a také že o existenci BTC nevěděl dokud ho nekontaktoval magazín Newsweek [24].

Jak je nejspíše zřejmé, tak BTC sklízí již několik let velký úspěch a jeho cena z původní hodnoty jeden dolar Spojených států amerických a méně, posunula už i přes hodnotu dvacetitisíc dolarů a nyní v roce 2018 se BTC stabilně drží kolem hodnoty osm tisíc dolarů. Jako aktuální zdroj ceny Bitcoinu, lze využít live statistik webové aplikace Cryptowatch [13].

4.3 Blockchain a jeho důležitost pro úspěch kryptoměny Bitcoin

Úvod do technologie Blockchain, dle autorů z webové stránky Bitdegree [17] Všechny kryptoměny používají technologie distribuovaných účetních knih, aby odstranili z je-

Obrázek 4.2: Ukázka pohybů trhu BTC z webové aplikace Cryptowatch, kde červné svíce značí pokles a zelené nárůst [13]

jich systémů třetí strany. Technologie distribuovaných účetních knih jsou databáze, kde se zaznamenávají informace o transakcích. Z těcho technologií je ta nejpoužívanější právě technologie Blockchain. První Blockchain technologie byla navržena Satoshi Nakamotem pro kryptoměnu BTC. .

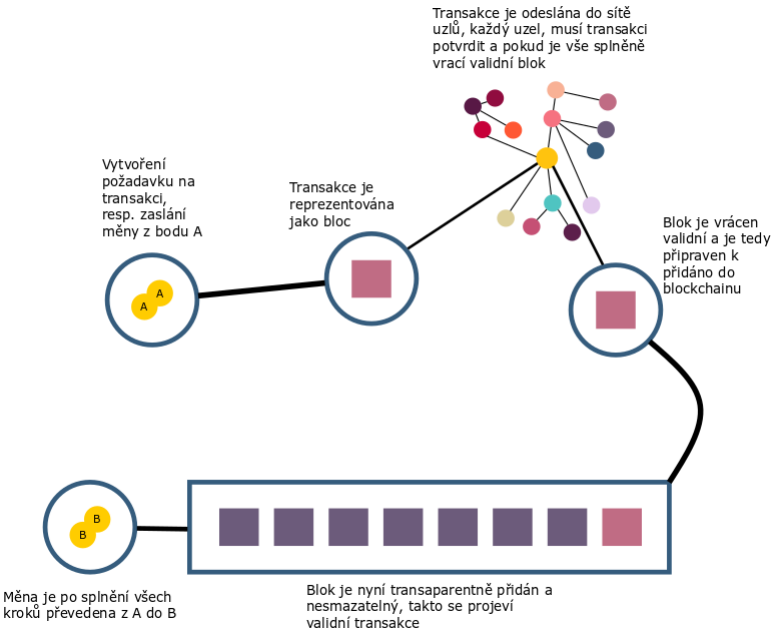
Distribuované technologie jsou takové technologie, které se skládají z mnoha malých dílčích částí, bez použití centralizace či snahy o kontrolu těchto částí.

Blockchain je distribuovaná technologie, která si pro konkrétní kryptoměny zachovává všechny transakce, které kdy byly provedeny. Toto vše je postaveno na technologii peer to peer, kde se databáze sdílí v rámci nodes, což lze v tomto kontextu přeložit jako uzly. Tyto uzly pak uchovávají danou databázy, a právě mezi nimi se konají kontroly validity a správnosti obdržených informací.

Díky tomuto tedy vzniká lineární databáze, do které lze pouze přidávat bloky informací, které nejdříve musí projít validací a schválením od uzlů. Pokud souhlasí více jak polovina uzlů v dané databázi, tak je blok informací schválen a přidán do Blockchainu, resp. databáze. A jak autoři z Bitdegree uvádějí tomuto procesu se říká consensus [17]. Tato databáze je viditelná všemi a jak je již výše zmíněno, informace lze pouze přidávat, ale nikoliv je odebírat či pozměňovat, čímž zajišťujeme jejich legitimitu.

S tímto tedy samozřejmě souvisí i spousta legálních a finančních změn, které bude třeba v blízké budoucnosti řešit. Trh jak ho známe se pravděpodobně velice změní. Zaručení anonymity při transakcích přináší mnoho dobrého pro jedince, ale zároveň se jedná i o velmi rizikové téma.

Kryptoměny již nejsou věcí budoucnosti či hobby počítačových nadšenců, kteří si snaží přivydělat. Kryptoměny a digitální měny se pomalu, ale jistě stávají běžnou součástí našeho života. V některých zemích jsou již plánované kompletní přechody do roku



Obrázek 4.3: Jednoduchá ukázka využití technologie blockchain při průběhu transakce mezi dvěma body, vlastní tvorba.

2020 z fyzických peněz na digitální měny či vypuštění oficiálních státních kryptoměn. Toto může vést nejen k modernizaci a digitalizace financí po celém světě, ale také k vlně nelegálních transakcí, vyhýbání se sankcí a obcházení práv, které brání ilegální prodeji zbraní a pohánění válek.

Na druhou stranu Blockchain je technologie téměř nekonečného využití. Dovoluje nám tvořit zabezpečené, digitální účetní knihy o nejen finančních transakcích, ale téměř o všem, co má hodnotu. Ve Spojených státech amerických mnoho společností investuje mnoho svých zdrojů do výzkumu technologie Blockchain a jejího nasazení na své produkty. Jedná se prozatím převážně o dodavatele elektřiny či přírodních zdrojů jako je plyn.

Blockhain tedy funguje tak, že se nejprve zašle požadavek na transakci, který se rozešle do sítě, tedy mezi uzly. Tato síť provede verifikaci nad daným požadavkem a zaznamená si transakci. Poté dochází k zařazení informací do existujícího blockchainu, resp. zařazení bloku do blockchainu. Jako poslední krok se transakce schvaluje.

4.4 Verifikace a úvod do průběhu transakcí

Mohli by tedy vznikat otázky jak se vlastně transakce kryptoměn verifikují. Je tedy třeba si vysvětlit na jakém principu je verifikace kryptoměn postavena a jak vlastně funguje.

Dostáváme se tedy již k samotnému miningu, tedy těžbě kryptoměn. Dle webového portálu Bitdegree se uvádí, že si pod pojmem těžení kryptoměn můžeme představit jako něco, co by se dalo považovat za fyzicky náročnou dělnickou činnost, ale jedná spíše o činnost podobnou účetnictví. [17] Znamená to, že těžaři jsou jednotlivé uzly, které provádějí speciální úkony díky kterým jsou transakce možné.

Způsob na kterém tato činnost funguje je založen na šifrování informací, tedy hashování. K informací, které mají si berou další informace o transakci a zahashují ji. Berou tedy tolik informací potřebných ke vzniku nového bloku a informace hashují.

Na webowém portálu Bitdegree [17] je tento postup popsán jako závod mezi těžaři v kterém se závodí o to, kdo jako první odhadne zašifrovaný kód nebo hash bloku, který bude přidán novému bloku, než je blok přidán do blockchainu. Šťastlivec, který jako první odhadl správný kód přidává nový block do blockchainu.

Dále následuje, jelikož se jedná o decentralizovanou peer to peer síť, verifikace od všech uzlů sítě a znovu se navazuje jak uvádí portál Bitdegree, tak že po závodu všechny ostatní uzly ověřují informace transakce v novém bloku. Kontrolují, jestli celý blockchain, aby se ujistili, že se nové informace shodují. Pokud se shodují, tak je nový blok validní a uzel, který závod vyhrál přidává nový blok do blockchainu. Tomuto se říká konfirmace. [17]

4.5 Krypto peněženky

Jak uvádí server Finder, lze obecně krypto peněženky rozdělit na dva typy a to hot a cold, tedy horké a studené [15]. Toto rozdělení značí jestli se jedná o software peněženku pro kterou platí označení horká a nebo naopak hardware či fyzickou peněženku pro kterou platí označení studená peněženka.

Z tohoto se dá téměř okamžitě usoudit, že fyzická varianta je z těchto dvou bezpečnější. Pokud má ovšem uživatel důvěru v software a online přístup k peněžence, tak má na výběr horké peněženky. Jistější volbou se tedy zdá studená peněženka v podobě hardware. Kdy ke přístupu k peněžence je zloděj oproti software peněžence dostat fyzicky. Proto se studené peněženky také často označují jako trezory.

Způsob jakým tyto peněženky fungují záleží podle typu peněženky, obecně ale lze říci, že pracují s veřejným klíčem. Pro transakci je tedy třeba znát veřejný klíč příjemce, poté se zadá množství měny k odeslání či zaplacení a dále téměř jak u chatové aplikace se použije obdoba tlačítka odeslat. Tento proces není identický pro odesílání a příjem transakcí. Pokud chceme transakci přijímat, je možné, že náš veřejný klíč není statický, ale je pro každou transakci generován klíč nový.

V každé peněžence jsou však ale klíče veřejné a soukromé. Tyto klíče se využívají při transakcích. Uživatel A předá svůj veřejný klíč uživateli B, uživatel B tedy pou-

žije veřejný klíč uživatele A k provedení transakce. Mezitím se v rámci blockchainu použije soukromí klíč uživatele A k validaci veřejného klíče uživatele B a jakmile tyto klíče odpovídají, je transakce přidána do blockchainu. Transakce je tedy validní a měna odeslaná uživatelem B je přičtena na účet uživatele A.

Jak uvádí webový portál Finder [15], bezpečí peněženky začíná u uživatele. Uživatel by tedy měl s rozumem volit své přihlašovací údaje, tvořit si bezpečné zálohy a nikdy nikde své peněženky nevystavovat.

U krypto peněženek také platí pravidlo, že si poskytovatelé těchto služeb odvádí určitý poplatek. Tento poplatek je buďto procentuální nebo přímo stanovená částka za provedenou transakci. Toto lze pochopit u peněženek spadajících pod firmy, které musí obsluhovat a udržovat peněženky zákazníků. Poplatky využijí na udržování kvality služeb a zabezpečení, jelikož právě tyto poskytovatelé služeb jsou často cíli pro hackery.

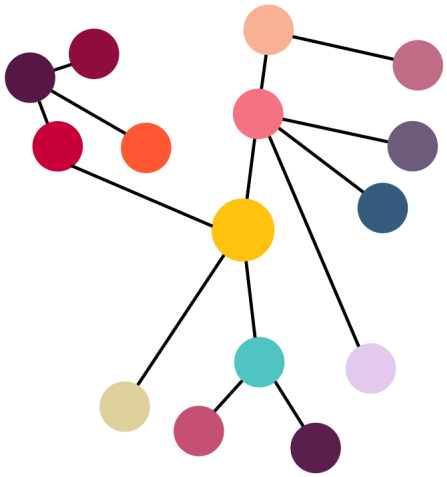
4.6 Dodatečné vysvětlení terminologie spojené s kryptoměnami

Terminologie spojená s kryptoměnami je velice rozsáhlá, ale k pochopení tohoto tématu je třeba uvést několik pojmů a to Decentralizaci, peer to peer, Hash a Hashing a posledně také pseudoanonymitu. Tyto pojmy budou popsány níže.

- Jako první lze vysvětlit výše zmíněnou decentralizaci a s ní spojený pojem peer to peer. Níže lze vidět ukázku decentralizace. Podstatou decentralizace je tedy nezávislost na třetích stranách.

- Díky tomuto je tedy s decentralizací spojen i pojem peer to peer. Jedná se o typ připojení či komunikace, kdy jsi jsou oba účastníci jak už transakce či nějaké komunikace rovni a komunikují mezi sebou, nezávisle na nějaké třetí straně. Kryptoměny tedy nemají nějaký hlavní server, který vše řídí, ale jedná se o obrovskou síť tvořenou tisíci na sobě nezávislých jedinců. Tito jedinci tedy nepotřebují ke zprostředkování transakcí banky ani jiné jim podobné instituty a stávají se tak nezávislými a schovávají se za pseudoanonymitu, tedy například za své online přezdívky.

- Jako další pojem je třeba popsat Hash a s ním spojení hashing. Pod hashem si lze ve světě kryptoměn představit klíč, či sadu znaků, jelikož hash je tvořen kombinací čísel a písmen. Hash tedy vzniká při transakcích, kdy těžaři vezmou informace a šifrují je. Hashing lze jednoduše popsat tak, jak je uvedeno na webové stránce Coindesk: „Abstraktně vzato, hashovací funkce je matematický proces, který bere teoreticky jakkoliv velké množství dat a provádí nad nimi určité ope-



Obrázek 4.4: Ukázka Decentralizace kde každý bod v grafu představuje jeden uzel v síti, vlastní tvorba.

race po kterých vrací výstupní data o fixní velikosti. [8]“ Jak lze tedy určit z citace, výstup bude vždy stejně velký, ať už jsou vstupní data jeden znak či dlouhá věta.

- Pseudoanonymita znamená, že jako jedinec, není třeba vystavovat či sdílet své osobní informace, abychom mohli obchodovat s kryptoměnami.

  Můžeme se tedy považovat za téměř anonymní jedince a společně díky decentralizaci by nikdo neměl být schopný přesně sledovat transakce. Získáváme tedy pseudoanonymitu při jakékoliv transakci.

5 Úvod do těžby kryptoměn

K uvedení do těžby kryptoměn bude třeba uvést níže uvedené body a to například co to je Proof of Work, tedy důkaz práce a dále rozdíl mezi proof of work(dále PoW) a proof of stakes(dále PoS). V případě PoS se jedná o důkaz podílu, podobně jako je to s akciemi. Dále budou zmíněny ostatní základní pojmy a činnosti, které s těžbou kryptoměn souvisejí.

5.1 Měření výkonu a odměn

Měření výkonu a odměn je úzce spjato a to z důvodu vlivů jak hardware, tak i software částí těžební soustavy. Jak uvádí webový portál Coindesk, proces těžení kryptoměn se zaobírá řešením kryptografických hádanek. Touto činností těžaři poskytují tak zvaný PoW, neboli důkaz práce a jsou podle něho odměňováni kryptoměnou. Obecně řečeno existují dva nejznámější a největší PoW hashovací algoritmy a to SHA-256 a Scrypt [7]. U tohoto lze poznamenat existenci alternativních algoritmů, kterými se tato práce bude právě zaobírat a jedná se o Ethash, Equihash a Cryptonight.

Podle výše zmíněných algoritmů, lze vybrat co nejefektivnější hardware. Některé algoritmy jsou převážné náročné na RAM paměti a schopnost paralelních výpočtů, jiné zase například preferují čistý výpočetní výkon. Z tohoto lze usoudit základní rozhodnutí mezi běžnou těžební soustavou, tedy klasický počítačový hardware s větším počtem grafických karet a nebo naopak nestandardní a specializované sestavy které využívají hardware ASIC.

S těmito možnostmi je tedy nutné počítat odměny. Pod odměnami si lze představit čistě návratnost nebo výtěžnost těžící soustavy. Toto však ovlivňuje mnoho faktorů, typ těžební soustavy a její efektivita, cena elektřiny a také obecná návratnost, která je pro každou měnu jiná a velmi pohyblivá. K zamyšlení je zde tedy i budoucí vývoj vybrané kryptoměny. Samozřejmě nikdy nemůžeme přesně odhadnout, co se stane, ale je dobré si o měnách nejprve udělat výzkum a prověřit tak jestli má smysl měnu těžit a nebo do ní investovat.

Odměny tedy lze vypočítat, jak uvádí webový portál Coindesk, tak že si vezmeme hashovací rychlost své těžební soustavy a vydělíme ji energetickou spotřebou za měsíc a tím tak získáme těžební účinnost [7]. K těžební účinnosti lze dodat, že je závislá na

měnách a tarifu energií. Každá měna má jinou návratnost. Trh je velmi dynamický a ceny kryptoměn se mohou rapidně měnit v rámci dní či i hodin. Dále lze těžební účinnost také ovlivnit změnou energetického tarifu, či změnou dodavatele energie. Je tedy třeba brát v potaz i spolehlivost dodavatele elektrické energie. Výpadky dodávky či časté odstávky nebo změny cen za kWh, tedy kilowatthodinu mohou účinnost těžební soustavy zcela zvrátit.

5.2 Proof of work a Proof of stakes

PoW je jak je již výše zmíněno důkaz o činnosti. V tomto případě se tedy jedná o dokázání zpracování transakcí. Provádí se tedy proces hashování, kdy sestava zpracovává transakce a tvoří blok. Pokud proběhne validní hashovací proces, tedy těžební soustavě se podaří odhadnout správný hash je těžař odměněn block odměnou. Ta se vždy liší podle typu kryptoměny. Je tedy zapotřebí těžebních soustav, které tuto práci provádí. Každá těžební sestava podá jiné výsledky a taktéž každá kryptoměna poskytne rozdílné odměny.

Jak uvádí webový portál Sitepoint, PoW je výhodný v tom, že lze využít těžení v poolu, tedy v nějakém uskupení těžařů, díky kterému lze zajistit větší šanci odměny, jelikož šance odměny úzce závisí na těžebním výkonu sestav [25].

Bohužel s přístupem PoW přichází také problém spotřeby. Jelikož přístup PoW je čistě postaven na těžebním výkonu, tedy na běžícím hardware, který nepřetržitě provádí operace. Díky tomuto tedy s každým rozšířením sestavy, či přibytím dalších těžařů vzniká větší spotřeba elektrické energie. Toto je bohužel elektrická energie z které nevzniká nic jiného než výdělek pro těžaře a je tedy třeba tento problém řešit a zabránit tak velké spotřebě elektrické energie.

Jako další zápor lze také uvést centralizaci těžby, kdy například webový portál Sitepoint uvádí čínské magnáty, kteří mají 80 procentní podíl na hashování kryptoměny BTC.

Tomuto problému se snaží předejít přístup PoS, tedy důkaz podílu. S tímto přístupem není třeba provádět žádné složité výpočty a tím se zbavujeme potřeby těžebních soustav. Tímto se zároveň také odboural problém enormní spotřeby, kterou přináší přístup PoW.

PoS, tedy důkaz podílu, lze uvést na kryptoměně Ethereum. Jak uvádí webový portál Blockgeeks, tento přístup funguje na principu validace a náhodné volby validátora, za kterého volí jedince s dostatečným množstvím kryptoměny. Zároveň také platí, že čím více kryptoměny validátor vlastní a také čím déle ji vlastní, roste jeho šance pro zvolení na pozici validátora [23].

Validátor tedy zabírá po nějakou dobu kryptoměnu a zaručuje, že dodrží pravidla

zvolené kryptoměny, respektive že provede validaci transakcí a za tuto činnost je následně odměněn. Jak již tento a předchozí postupy naznačují, nelze věřit pouze jedinci a validace neprobíhá pouze v rámci jediného uzlu. Transakce se tedy vždy přidá do bloku, provede se validace a tento blok je díle poslán dalším validátorům ke konfirmaci. Tímto se tedy předchází falšování transakcí a jejich validací. Validátoři jsou totiž povinni znovu konfirmovat provedené transakce.

Tomuto dále předchází snaha odstranění kohokoli ze sítě, kdo se snaží falšovat transakce a rozesílat tedy falešné informace. Nejen, že je validátor odstraněn ze sítě, ale je mu také sebrána jeho kredibilita a především kryptoměna kterou ručí svým podílem.

K přístupu PoS lze dále zdůraznit jeho důležitost. PoS by totiž měl dosáhnout opravdové decentralizace, úspoře energií díky výpočetní nenáročnosti a také se lépe vypořádat se škálováním, respektive s příbytkem nových "těžařů".

5.3 Obtížnost těžby

Obtížnost těžby je postavena na kompetici těžařů. Webový portál Blockgeeks uvádí, že obtížnost těžení je přímo úměrná sazbě kterou jsou těženy bloky. Tedy čím více lidí těží a čím více těžebního výkonu jsou schopni poskytnout tím vyšší bude obtížnost těžby. Tato obtížnost je upravena každých 2017 bloků.

Toto samozřejmě přináší další problém a to nemožnost další těžby. Jelikož složitost těžby roste exponenciálně, může se stát, že tato složitost dosáhne takové úrovně, kdy nastane nemožnost další těžby a až tento čas nastane budou nuceni těžaři přejít z konceptu PoW na koncept PoS.

5.4 Těžba samostatná nebo v pool

S těžbou v dnešní době úzce souvisí pojem pool, tedy skupina se stejným zájmem. Jak uvádí webový portál Cryptocompare, těžební skupina neboli pool se skládá z mnoha menších těžařů, kteří kompenzují menší výpočetní výkon tak, že zapojí svůj výkon do jedné skupiny. Tato skupina je tedy kolektivně konkurovat těžebním magnátům a zaručit tak zisk a jedincům, či menším skupinám těžařů. [20].

Tyto těžaři tedy nemusí řešit problém s větší spotřebou energie nebo s koupí dražšího, ale výkonnějšího hardware. Tyto skupiny tedy společně těží za odměnu, která se mezi těžaře spravedlivě rozdělí podle toho, jak k této činnosti přispávají, respektive podle jejich těžebního výkonu.

V těchto skupinách se z často vyskytují poplatky za jejich využití a to z pravidla 1 procento z odměny. Toto je však malá cena za umožnění zisku, který by byl jinak pro menší těžaře nemožný. Dá se tedy říct, že tyto skupino přináší svou hodnotu pro těžaře

ve stálejším a stabilnějším příjmů, ušetření na nákladech a také poskytují potenciál vyššího výdělku.

Těžaři této možnosti samozřejmě využít nemusí a mohou se rozhodnout těžit samostatně. S tímto tedy nemusí těžař odevzdávat žádný podíl poolu a celý výdělek patří jedinci. Toto však ale přináší problém, který vzniká s obtížností těžby. Jako jedinec může mít těžař v dnešní době díky náhodnosti těžení tak malou pravděpodobnost úspěchu, že se nevyplácí těžit a těžba je spíše ztrátová. Právě z tohoto důvodu se mnoho těžařů zapojuje do těžebních skupin. Jako příklad jednoho z těžebním poolů lze uvést Nanopool.

6 Těžební algoritmy, s nimi spojený software a měny

Každá kryptoměna používá svůj vlastní šifrovací algoritmus a specifický hardware i software který šifrování provádí. Toto vše tedy spěje k funkci blockchainu, zpracování transakcí a odměnám. Dnes mezi nejpopulárnější šifrovací algoritmy patří například Ethash, CryptoNight a Equihash.

6.1 Equihash

Dešifrovací algoritmus Equihash je používán pro těžbu měny Zcash. Webový portál Zcash blog uvádí, že důvod pro využití algoritmu Equihash je efektivita verifikace [26]. Equihash je tedy PoW dešifrovací algoritmus, který je jak uvádí webový portál Coinguides odolný proti využití specializovaného hardware ASIC [9]. A to právě díky využití počítačové pamětí.

Není to tedy algoritmus, který by nabýval efektivity s čistým výpočetním výkonem, ale naopak s vyšší kapacitou paměti. Tento algoritmus je tedy více optimalizovaný a je výhodnější pro těžbu běžnou těžební sestavou, což je výhodné pro malé těžaře, kteří nemají dostatečný kapitál, či zájem těžit za pomoci specializovaného hardware ASIC.

Pokud tedy chceme těžit měnu ZCash za pomoci algoritmu Equihash je třeba vybrat i správný software, respektive těžební klient. Těžební klienti jsou počítačové programy, které využívají těžaři a starají se o samotný proces těžby. Jsou samozřejmě unikátní dle specifikací měny a hardwaru, který k těžbě využívají. U této měny lze využít služeb těžebního klienta EWBF, který byl napsán pro grafické karty výrobce NVidia s čipem Pascal. Vyžaduje minimální kapacitu video paměti alespoň 1 Gigabyte.

Tato měna a algoritmus dále používají unikátní identifikátor těžební sazby. Jedná se o Sol za vteřinu, což lze pochopit jako solution tedy řešení za vteřinu. Toto je pouze kosmetická úprava a jedná se standardně o hash rate tedy hash sazbu, která se nepočítá v rámci hodiny ale vteřiny.

6.2 CryptoNight

Dešifrovací algoritmus CryptoNight je používán pro těžbu například měn Monero a Bitecoin. Tento algoritmus je zajímavý tím, že k těžbě využívá procesory běžných stolních počítačů. U většiny jiných těžebních algoritmů se využívá totiž téměř vždy schopnosti paralelních výpočtů a je tedy výhodnější využít grafických karet nebo specializovaného hardware ASIC.

V případě CryptoNight se tedy jedná o algoritmus využívající PoW a využívá se tedy výpočetního výkonu procesoru. Autoři na webovém portálu Steemit uvádí, že algoritmus CryptoNight spoléhá na náhodný přístup k pomalým pamětem s dobrou úrovní latence. Každý nový block je tedy závislý na všech předchozích blocích. Tento algoritmus tedy potřebuje přibližně 2 Megabyty pro instanci bloku.[18].

Při těžbě za pomoci tohoto algoritmu a měny Monero, lze využít těžební klient XMR-Stak. Tento těžební software je naprogramován tak, že lze těžit více měn a za pomoci různých hardware. Lze tedy těžit za pomoci grafických karet i procesorů a nejsou ani omezeny na výrobce. Je tu tedy možnost využití hardwaru od společností Intel, AMD i NVidia.

6.3 Ethash

Tento algoritmus využívá měna Ethereum, která je dnes mezi nejpopulárnějšími kryptoměnami. Jak uvádí webový portál Coinguides, v případě Ethash se jedná o PoW algoritmus vytvořený přímo pro měnu Ethereum. Jeden z nejdůležitějších důvodů proč vznikl tento algoritmus je odolný proti těžbě za pomoci specializovaného hardwaru ASIC [10].

Jedná se tedy o těžení algoritmus, který je určen pouze pro grafické karty a je velmi náročný na paměti. Je tedy vhodný k těžbě na běžných těžebních soustavách. K těžbě kryptoměny Ethereum za pomoci algoritmus Ethash lze využít těžební klient Claymore. Při těžbě za pomoci tohoto algoritmu se využívá grafických karet. Jedná se o grafické karty AMD nebo NVidia. Samozřejmě jaký typ grafické karty je k většímu zamyšlení jelikož nezáleží jenom na čistém výpočetním výkonu grafických karet.

Lze se zde zamyslet na podporou vybraných grafických karet, provedení výzkumu trhu a zjištění jak si obecně grafické karty vedou v těžbě. Dále je třeba brát v potaz ne jen tedy podporu grafických karet, ale také jejich spotřebu. Grafické karty AMD mohou často vést, co se čistého výkonu týče, ale často také mívají o mnoho vyšší spotřebu, čímž jsou nepraktické. Na druhou stranu grafické karty NVidia bývají často úspornější a také získávají lepší návratnou hodnotu z důvodu větší šance na prodej grafické karty dalším těžařům či běžným uživatelům.

7 Těžební soustava - praktická část

V této části práce jsou uvedeny postupy, kterými se řešila problematika stavby, testování těžební soustavy a její software konfiguraci, jejíž výsledkem je funkční a otestovaná těžební sestava. Je tedy třeba vybrat hardware z kterého bude tato sestava složena, dále také určit proč si právě zvolený hardware chceme vybrat a k jakému účelu tuto stavbu chceme použít. Už jen toto může ovlivňovat všechny další kroky a to například volbu operačního systému, volbu těžené kryptoměny a zvolený těžební software.

Součástí řešení tedy bude samotná volba hardware, kdy se bude obhajovat a vysvětlovat jeho výběr, dále názorná ukázka výpočtu návratnosti, tedy jak si dopředu zjistit odhad zisku z těžení a porovnání grafických karet dvou největších výrobu Amd a NVidia v rámci této soustavy. Dále se bude řešit samotná stavba těžební sestavy, která je podložena fotodokumentací. V této části se také bude řešit správné nastavení BIOS pro těžbu a s tím spojená dokumentace, tedy screenshoty nastavení BIOS.

Samotné testování těžební soustavy se bude skládat z porovnávání spotřeby a výtěžnosti, které se budou lišit podle těžené měny, použitého těžebního software a nastavení grafických karet. Dále se zde řeší volba operačního systému dle optimalizace a specifických výhod pro těžení specifických kryptoměn. Poté jsou řešeny samotné testy těžby měn, tyto testy se provádějí pro specifické kryptoměny a také v rámci Nanopool.

Dále se řeší taktování grafických karet a jeho vliv na výkon grafických karet, respektive jeho vliv na výtěžnost celé soustavy, jelikož se ovlivní nejen výpočetní výkon grafických karet, ale také jejich spotřeba. V taktovací části se samozřejmě neřeší pouze navyšování například hodnot taktu pamětí a čipu, ale také jejich snižování.

Poté se názorně za pomoci fotodokumentaci a screenshotů promítne vliv taktování a jeho přínosy, což bude spjato s porovnáním výtěžnosti po taktování grafických karet oproti výchozímu nastavení grafických karet.

7.1 Volba Hardware

V této části práce je třeba uvést v míru vliv volby hardware na celou těžební soustavu. Výkonově se mohou zdát jisté komponenty velmi podobné. Dokonce se někdy i tváří jedna strana převážně výhodnější, ale díky optimalizaci či chybějícím úpravám například BIOS se tyto komponenty nemusejí vždy vyplatit. Záměrem je tedy vybrat vhodné

komponenty, které by splnili účel a zároveň jsou v rámci možností studenta. Znamená to tedy, že v této části je především brán velký ohled na návratnost sestavy.

Je tedy potřebné zmínit znovu prodejnost komponent, či se i zamyslet nad směrem, kterým se těžení kryptoměn udává. Tímto se tedy naráží na budoucí přechod z PoW na PoS, kdy může mít určitý hardware výhodu nad jiným. Toto tedy především vedlo k výběru grafických karet společnosti NVidia.

Tabulka 7.1: Náklady na stavbu těžební soustavy

Typ Hardware	Ks	Cena za kus
Grafická karta	4	12 000 Kč
Základní deska	1	2 000 Kč
Zdroj	1	2 800 Kč
Risery	4	129 Kč
Procesor	1	700 Kč
RAM paměť	1	1 170 Kč
Pevný disk	1	700 Kč
Celkem		**55 886 Kč**

Podle tabulky 7.1 lze vidět vybrané komponenty, tedy grafické karty NVidia 1070ti, základní desku společnosti Asus typu Z270-A. Typ základních desek nám určuje nejen možnosti taktování, ale také specifikuje jaké další technologie jsou na základní desce přítomné a které naopak chybí. Velmi důležité risery, tedy rozšíření PCI slotů, které nám umožní napájení i zapojení většího množství grafických karet do jedné soustavy.

Dále je také uveden procesor, který spadá společně s pevným diskem a RAM pamětmi mezi nejlevnější komponenty, jelikož pro vybraný typ těžby a samotný běh systému jsou tyto komponenty nezbytné, ale zároveň jeho chod nijak zásaditě neovlivňují.

Dále je také třeba větší pozornosti zdroji této soustavy, jelikož k této komponentě nebude připojena jak je běžné pouze jedna grafická karta ale za pomoci riserů budou připojeny čtyři .

7.1.1 Výpočet návratnosti

V této sekci je názorná ukázka u které poslouží tabulka 7.2 díky které lze nastínit základní výpočty které se využívají k odhadovému výpočtu návratnosti, což lze také označit jako výtěžnost soustavy. Tímto si lze dopředně usoudit, zdali se nám těžba určitě měny či využití specifického těžebního software a nebo také zapojení se do těžebního poolu vyplatí.

Tabulka 7.2: Výpočet návratnosti pro vybrané měny, pro grafickou kartu Gtx 1070Ti 4x a cenou za 1kWh = 1,14 Kč

Kryptoměna	Hash Rate	Těžební SW	Spotřeba	Návratnost	
				Za den	Celková
Monero	2309 H/s	Xmr-stak	364 W	$1,07	$ 31,96
Ethereum	107 Mh/s	Claymore	491 W	$1,53	$ 46,00
Zcash	1830 Sol/s	Zec EWBF	391 W	$1,50	$ 45,00

Pří výpočtech je třeba dopředu znát alespoň průměrné hodnoty Hash Rate a spotřeby grafických karet. Dále je také třeba vědět jaký těžební software bude použit a pokud bude těžba probíhat v rámci poolu, kdy se část výtěžku odevzdává. Jako průměrná hodnota, která se průměrná odevzdává poolu bývá často jedno procento výtěžku.

Vzorec nebo postup, kterým se tedy řídíme je tento: Odhadovaný výtěžek za den vynásobený počtem dnů v měsíci od čehož se odečte hodnota odevzdaná poolu což dohromady lze označit za výtěžek. Dále se počítá spotřeba, kterou zjistíme obecně za pomoci ceny za 1 kWh elektřiny a dle odhadované spotřeby těžební soustavy, díky těmto hodnotám si lze vypočítat měsíční spotřebu elektřiny. Na konec tedy odečteme od měsíčního výtěžku měsíční spotřebu a tak získáme odhadovanou průměrnou hodnotu, kterou můžeme měsíčně získat či ztratit.

7.1.2 Porovnání NVidia proti AMD v rámci této soustavy

V této soustavě se mohlo vybrat mezi dvěma typy karet. A to buďto grafické karty společnosti NVidia a nebo grafické karty společnosti AMD. Jako konkrétní modely lze uvést NVidia GTX 1070Ti a AMD RX 580 GB.

Rozdíly mezi těmito kartami rozhodují v dalších volbách a možnostech celé soustavy. Při rešerši těchto dvou modelů se narazilo na potřebu flashovat BIOS, což je tedy výměna základního firmware grafické karty, u grafických karet AMD. Flashování biosu je velmi náročné a hardware se při flashování může i nezvratně poškodit.

Naopak grafické karty společnosti NVidia jsou k těžbě připravené tzv. způsobem plung 'n play, kdy stačí grafické karty zapojit do sestavy, nainstalovat základní ovladače od výrobce karet a začít těžit.

Dále také bylo bráno v potaz budoucí využití jak grafických karet, tak i celé soustavy. V tomto také vyhrály grafické karty společnosti NVidia. Díky dříve zmíněnému přechodu Etherea z PoW na PoS je také výhodnější volba strany NVidia, kdy si použité modely grafických karet NVidia déle drží svou cenu. Díky tomuto lze po přechodu z PoW na PoS grafické karty, z důvodu ztráty využití, prodat a získat tak vyšší hodnotu návratnosti. Právě díky těmto bodům bylo zvoleny do sestavy právě grafické karty spo-

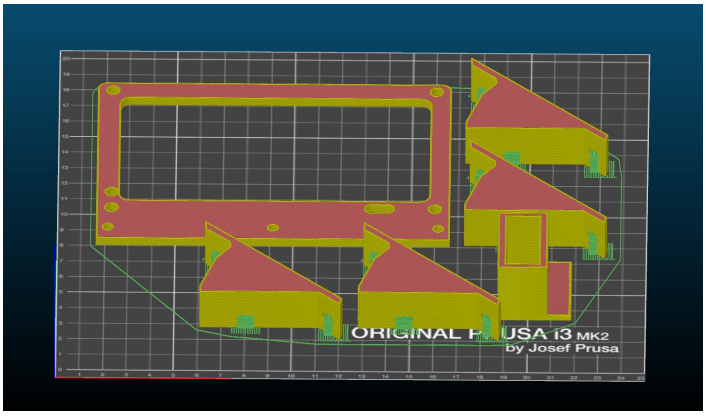
lečnosti NVidia.

Jako zajímavost bylo za pomocí webového portálu CryptoCompare [2] provedeno porovnání odhadovaného těžebního výkonu na kryptoměně Ethereum. Porovnané byly výše zmíněné grafické karty AMD RX 580 8GB(dál RX 580) a NVidia GTX 1070ti(dále Gtx1070ti), kdy obě karty při průměrné spotřebě 135 Watt, podávali téměř stejný těžební výkon. Těžební výkon Gtx1070ti byl 30.50 MH/s a těžební výkon RX 580 byl 30.20 MH/s.

Po tomto porovnání se zdálo jako výhodnější volba grafické karty modelu RX 580 a to díky své podstatně nižší ceně. Cena jedné RX 580 je v průměru o 42 procent nižší než cena jedné GTX 1070ti. Vzhledem k výše zmíněným potížím, problémech karet RX 580 a také širší možnosti těžby grafických karet Gtx1070ti bylo v rámci této sestavy a práce nevýhodné vybrat grafické karty RX 580.

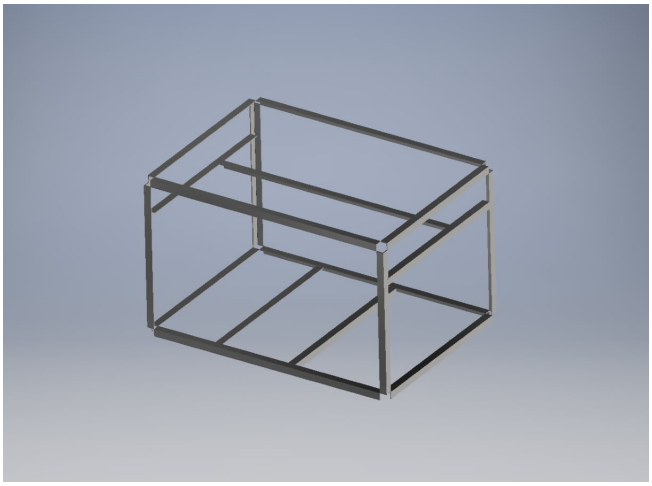
7.2 Stavba těžební sestavy

Při stavbě těžební soustavy se také narazilo na možnost 3D tisku a vlastní výroby lepšího a levnějšího racku, jedná se často o serverové regály (dále pouze rack), viz obrázek 7.1, ve kterém se využilo náklonu zapojených grafických karet tak, aby se pozměnil směr proudu taženého vzduchu a také tímto vznikne větší mezera mezi kartami, respektive se tímto lehce šetří hardware a snižují náklady běhu soustavy.



Obrázek 7.1: Ukázka modelů nástavců, byly vytisknuty a použity při těžební stavbě sestavy, vlastní tvorba.

Dále je také ukázka základního modelu racku v obrázku 7.2 do kterého byla celá stavba složena a to včetně využití výše zmíněných 3D tisknutých nástavců. Tento model sloužil především k představě samotného racku a také k ověření přesnosti, kdy se podle modelu mohl rack složit z různých materiálů či za pomoci 3D tisku.



Obrázek 7.2: Ukázka modelu racku, který byl použit při stavbě těžební sestavy, vlastní tvorba.

Takovéto neoficiální racky, které si tvoří často menší těžaři bývají hojně využity právě díky úsporám, které díky tomu vzniknou. Jediný omezují faktor je představivost a myšlenka budoucího rozšiřování či prodeje ať už racku nebo celé těžební soustavy.

7.2.1 Nastavení BIOS pro těžbu a ukázka soustavy

Je nutné zmínit, že tento postup se týká pouze vybrané základní desky, která je použita v této těžební soustavě. Pro každý jiný model může být průběh nastavení BIOS odlišný a tento postup může být kompletně nepoužitelný.

Nejdříve je třeba nastavit vše v BIOS na základní a doporučené hodnoty za pomoci set default values. Dále se musíme přepnout do Advanced Mode, do záložky Advanced a v menu vybrat Platform Misc Configuration, zde má být vše ve stavu "Disabled". Poté se přepneme do záložky Tool , kde v menu zvolíme ASUS EZ Flash 3 Utility, což je nástroj k aktualizaci BIOS, tedy firmwaru základní desky, kde zvolíme patřičnou metodu aktualizace.

Máme možnost aktualizace pomoci USB disku a nebo za pomoci Internetu pokud máme sestavu připojenou ethernet kabelem k internetu. Při volbě aktualizace za pomoci internetu, se musí pokračovat výběrem typu konektivity, kdy se doporučuje použít nabídku DHCP a potvrdíme, že chceme BIOS aktualizovat. Poté proběhne stáhnutí a instalace nového aktualizovaného BIOS.

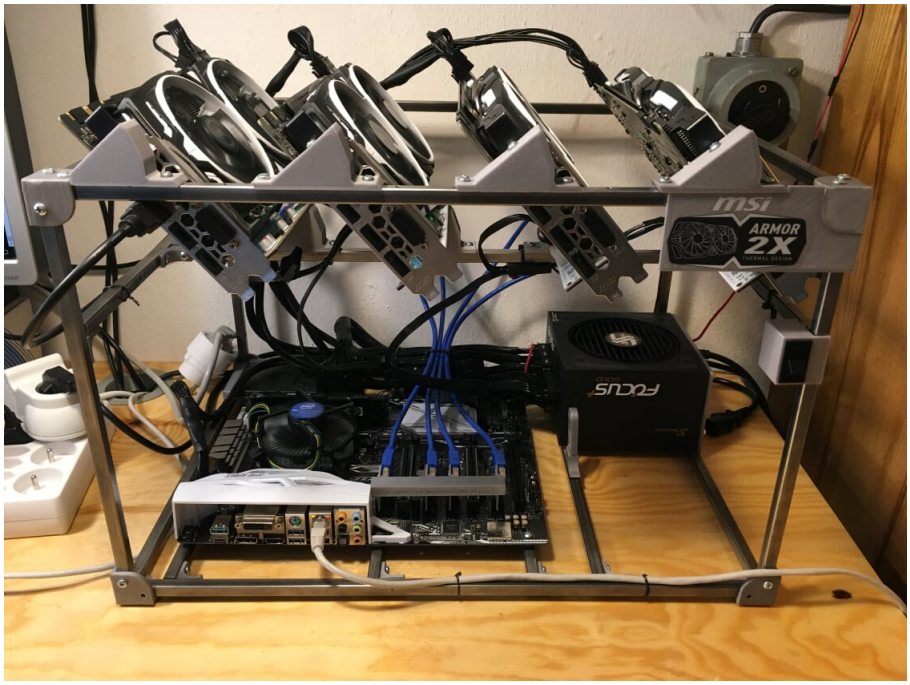
Zkontrolujeme že předchozí zmíněné nastavení v Advanced zůstalo ve vypnutém

stavu. Dále se přepneme v záložce Advanced v nabídce do možnosti Advanced/System Agent(SA) Configuration, zde se přepneme do nabídky DMI/OPI Configuration, kde na DMI Max Link Speed nastavíme Gen2 Vrátíme o úroveň zpět a zvolíme nabídku PEG Port Configuration, zde nastavíme PCIEX16 na Gen2. Také je třeba se vrátit o úroveň zpět a přepnout se do nabídky PCH Configuration a zde upravit možnost PCIe speed na Gen2.

Dále se přepneme do záložky Boot, nastavím možnost Fast Boot na zapnutý stav. Pokud chceme mít zapojených více než čtyři grafické karty také zde nastavíme možnost Above 4G Decoding na zapnutý stav. Lze zde nastavit Setup mode na nastavení Advanced Mode, kdy se po postu a zmáčknutí BIOS tlačítka dostaneme rovnou do pokročilého zobrazení narozdíl od běžného zobrazení BIOS.

Poté co provedeme všechny tyto změny je zapotřebí je také uložit, což se v tomto případě provádí tlačítkem F10. Čímž nastavení BIOS dokončíme.

Dále si uvedeme dvě názorné ukázky soustavy po složení a také jak soustava vypadá při chodu. Na obrázku 7.3, lze vidět celou zapojenou těžební soustavu. Tato soustava využívá výše zmíněných 3D vytisknutých komponent a také racku, který byl sestaven dle výše zmíněného modelu.



Obrázek 7.3: Ukázka hotové a zapojené soustavy, vlastní tvorba.

V druhé ukázce, na obrázku 7.4 se jedná o zapojenou a běžící soustavu, kde lze vidět monitorování stavu těžby a také stavu grafických karet za pomoci monitorovacího software. Tímto si lze kontrolovat správnou spotřebu, teploty, využití a také lze manuálně pro každou komponentu, která k chlazení využívá ventilátory nastavit otáčky jednotlivých ventilátorů.

Obrázek 7.4: Ukázka běžící soustavy při monitoringu těžby a hardwaru, vlastní tvorba.

Tato soustava, kterou lze vidět výše na obrázku 7.4 je připravena k těžbě. Je tedy třeba soustavu otestovat na vybraných kryptoměnách. Jak lze také vidět na výše uvedeném obrázku, soustava je připravena k jak těžení, tak i měření potřebných hodnot díky patřičnému softwaru a také měřidlu spotřeby, přes který je celá soustava zapojena k elektrické síti.

Bude tedy možné přesně získat hodnoty spotřeby, teploty, těžebního výkonu a například také celkové zátěže hardwaru ať už se jedná o procesor, pevný disk či jednotlivé grafické karty.

8 Testování těžební soustavy

Tato část práce se bude zaobírat především o ukázkách reálné spotřeby a výtěžnosti těžební soustavy. Tyto výsledky jsou získány při výchozích nastaveních grafických karet, tedy bez jakýchkoli úprav či zásahů do grafických kareta jejich výkonu.

Dále budou zmíněny další možnosti operačních systému, kde bude zmíněn operační systém specializovaný na těžbu kryptoměn. Na závěr této části práce budou předvedeny testy těžby vybraných kryptoměn v rámci Nanopool.

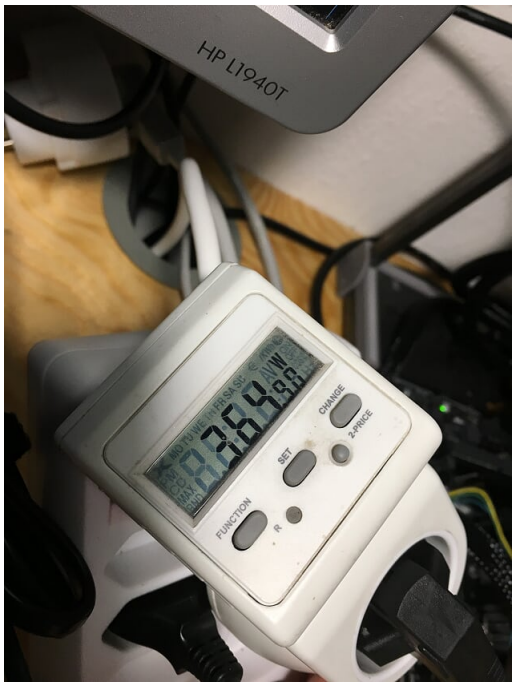
8.1 Reálná spotřeba a výtěžnost soustavy

Těžební soustava byla testována na několika kryptoměnách, při každé z nich byly získány jiné výsledky. Při těžbě Etherea vznikla průměrná spotřeba 391,20 Watt, při ZCash 391,88 Watt a při těžbě kryptoměny Monero vznikla spotřeba 364,90 Watt.

Lze tedy jednoduše vypočítat spotřebu za měsíc neustálého běhu a to tímto způsobem. Převedením Wattů na kiloWatty, tedy naměřená spotřeba dělená tisícem. Dále je třeba toto číslo vynásobit počtem hodin jak dlouho bude tato těžební soustava aktivní. Tímto získáme u Etehera 0,39120 kW, u Zcash 0,39188 kW a u Monero 0.36490 kWatt, tyto hodnoty dále vynásobíme hodinami v měsíci, jelikož víme, že sestava je nepřetržitě aktivní a měla by neustále těžit. Víme tedy, že rok 2018 má 365 dní a délka jednoho měsíce je tedy 30,41 dní, respektive 30 dní což se rovná 730 hodinám.

Můžeme tedy kiloWatty násobit hodinami a získáváme tak pro Ethereum hodnotu 282,576 kWh, pro Zcash 286,072 kWH a pro Monero 266,377 kWH. Znamená to tedy, že při průměrné české ceně za kWh, což je v roce 2018 zhruba 1,14,- Kč si můžeme spočítat výdaje za elektřinu. Tyto výdaje si samozřejmě vypočítáme vynásobením ceny za kWh a vypočítanou měsíční spotřebou.

Vznikají nám tedy tyto měsíční výdaje za elektřinu. Pro Ethereum tato hodnota činí 322,- Kč, pro Zcash 326,- Kč a posledně pro Zcash hodnota 304,- Kč. Jako ukázku naměřené spotřeby, lze ukázat obrázek 8.1. Tato hodnota byla naměřena při těžbě měny Monero s výchozím nastavením grafických karet.



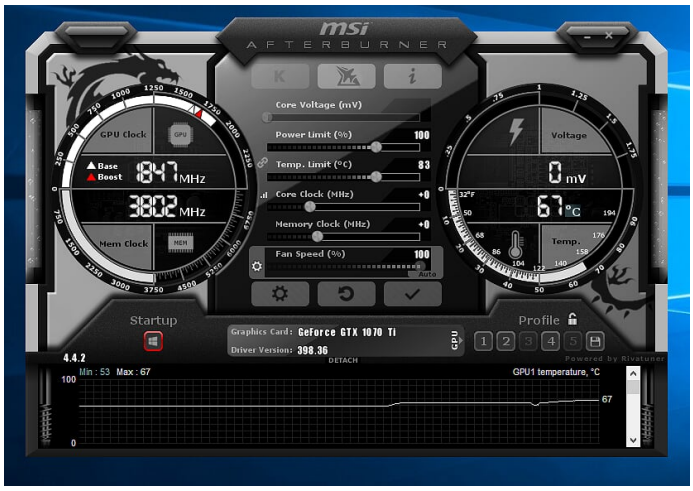
Obrázek 8.1: Ukázka naměřené spotřeby při těžbě kryptoměny Monero s výchozím nastavením grafických karet, vlastní tvorba.

8.2 Testy těžby měn Ethereum, ZCash a Monero v rámci Nanopool

K testování těžby těchto měn bylo použito výchozí nastavení grafických karet. Karty tedy nejsou nijak ovlivněny či laděny a toto jsou de facto naměřené kontrolní hodnoty. Je tedy třeba uvést potřebné snímky, kde lze vidět jednotlivou a hromadnou výtěžnost grafických karet.

Jako první ukázka je uveden obrázek 8.2 softwaru MSI Afterburner, který slouží jak k monitorování hardware, tak i k jeho úpravám neboli taktování. Tento software často používaný také při stavbách herních soustav a to především díky své jednoduchosti a nenáročnosti.

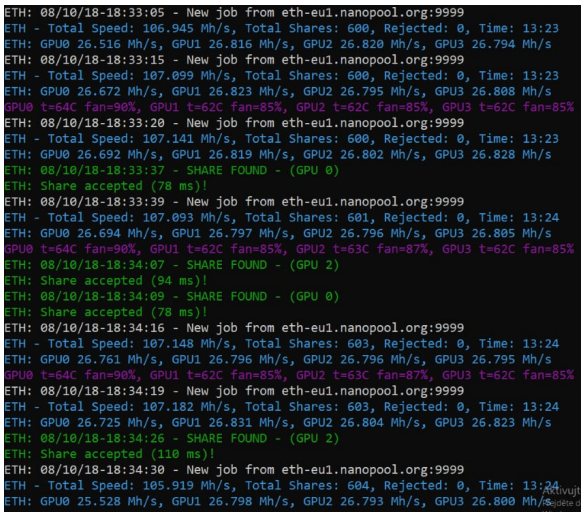
Tento software obsahuje jednoduché grafické rozhraní, která nám za pomoci posuvníků umožňuje jak taktovat grafické karty, tak i měnit otáčky jejich ventilátorů. Dále poskytuje možnost živého sledování a vykreslování grafů teplot, spotřeby, snímků za vteřinu a zátěže hardwaru. Teploty a zátěž hardware lze zobrazit pro procesor, grafické karty, severní můstek a nebo i pevné disky.



Obrázek 8.2: Ukázka naměřené spotřeby při těžbě kryptoměny Monero s výchozím nastavením grafických karet, vlastní tvorba.

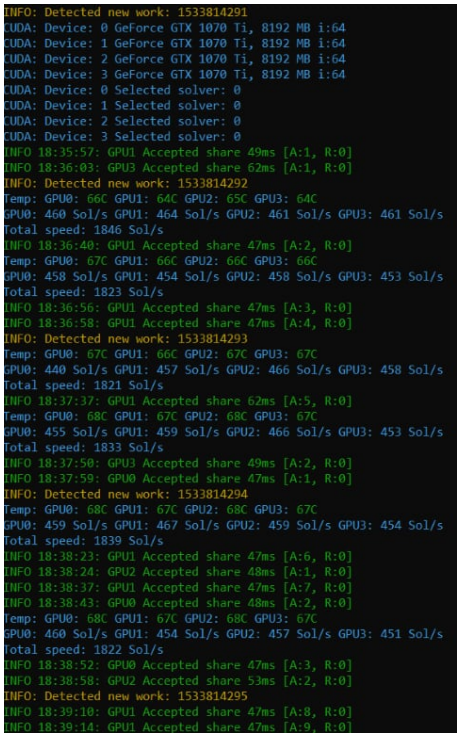
Níže uvedený obrázek 8.3 je snímek z windows příkazové řádky, kde je spuštěn vybraný těžební software (dále miner) Claymore miner. Tento miner je připojen k poolu, který se jmenuje Nanopool. Díky tomuto poolu si zvyšujeme šanci na možný výdělek a je to optimální volba pro malé těžaře.

Díky poolům lze také konkurovat větším těžařům, kteří využívají specializovaný hardware ASIC. Dále lze na tomto snímku vidět proces těžby a výtěžnost jednotlivých grafických karet, tedy GPU0 až GPU3. Jejich výtěžnost je tedy suma jednotek Mh/s, která průměrně činí 107 Mh/s.



Obrázek 8.3: Ukázka naměřené výtěžnosti při těžbě kryptoměny Ethereum s výchozím nastavením grafických karet, vlastní tvorba.

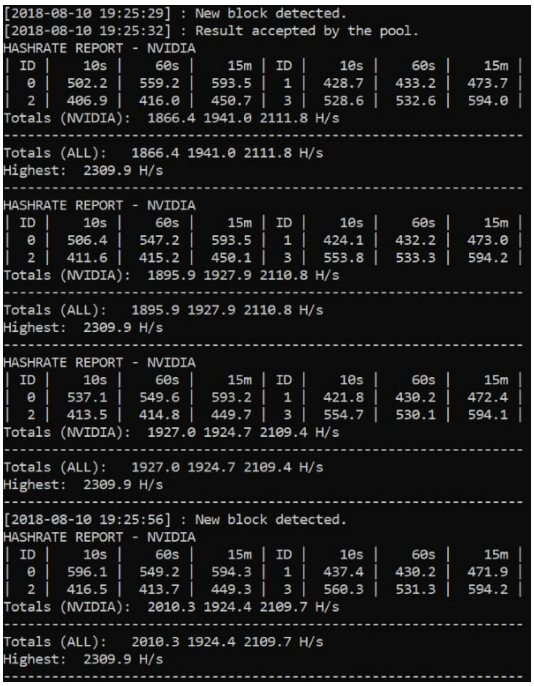
Dále je uveden obrázek 8.4, na kterém je vidět proces těžby za pomoci mineru ZEC EWBF, kterým se těží měna Zcash. Tentokrát je to výtěžnost v jednotkách Sol/s. Opět lze vidět výtěžnost mezi kartami GPU0 až GPU3 a miner je připojen k Nanopool. Celkově karty dosahují výtěžnosti průměrné hodnoty 1830 Sol/s. Tento miner je sice také spuštěn ve Windows příkazové řádce, ale oproti mineru Claymore obsahuje i teplotní status grafických karet, což je vhodné, pokud nechceme mít nainstalovaný žádný další monitorovací software třetí strany.



Obrázek 8.4: Ukázka naměřené spotřeby při těžbě kryptoměny Zcash s výchozím nastavením grafických karet, vlastní tvorba.

Jako poslední je uveden obrázek 8.5, kde je uveden snímek z příkazové řádky, kde je spuštěn miner XMR stak, napojený na Nanopool, kterým se těží měna Monero. Na tomto snímku lze vyčíst hodnoty výtěžnosti H/s. Tyto hodnoty jsou uvedeny k patřičným ID, které reprezentuje grafické karty.

Z tohoto snímku lze určit nejvyšší hodnoty výtěžnosti v daných úsecích a také hodnoty výtěžnosti jednotlivých karet. Maximální hodnota výtěžnosti je tedy 2309 H/s.



Obrázek 8.5: Ukázka naměřené spotřeby při těžbě kryptoměny Monero s výchozím nastavením grafických karet, vlastní tvorba.

8.3 Volba operačního systému

K těžbě a využití různých minerů či možností, které nabízí pouze specifický operační systém, lze také využít možností open-source, tedy otevřeně vyvíjeného operačního systému. Například lze uvést portál Hiveos [1], kde vývojáři nabízí stejnojmenný operační systém. Tento systém je specializovaný těžební operační systém, který najde své využití v případě větších těžařů či těžebních farem, kdy je třeba monitorovat či ovládat velké množství těžebních sestav najednou. Tento operační systém lze také využít k automatickému zasílání zpráv při jakékoliv poruše ať už v rámci mobilní sítě či za pomoci chatovací aplikace jako na například Telegram.

Pro tuto soustavu se však vybral běžný a současný 64 bitový operační systém Windows 10. Pro potřeby této soustavy je více než postačující. Je to snadno nastavitelný systém a také má skvělou podporu různých ovladačů pro těžební hardware, tedy grafické karty a různé ostatní aplikace, které lze při těžbě využít jako právě například monitorovací a taktovací software MSI Afterburner.

9 Taktování grafických karet a vliv na výkon

Posledním bodem této práce je taktování grafických karet. K tomuto účelu bude využit již výše zmíněný software MSI Afterburner. Tento software nám jednoduše a zřetelně umožní měnit chtěné hodnoty. Tímto tedy dosáhneme změn jako například snížení příkonu, navýšení frekvence jader grafických karet a nebo jejich pamětí.

9.1 Základní nastavení grafických karet

Základní neboli výchozí nastavení grafických karet je uvedeno již výše na obrázku 8.2 kde lze vidět snímek softwaru MSI Afterburner. Tento software byl použit k nastavení výchozího nastavení, které představuje maximální příkon 100 procent, teplotní limit čipu 83 stupňů Celsia, hodnotu jádra bez žádného přidání, tedy 1885MHz, hodnotu pamětí bez žádného přidání, tedy 3802 MHz a statickou rychlost ventilátorů grafických karet nastavenou na 90 procent své kapacity.

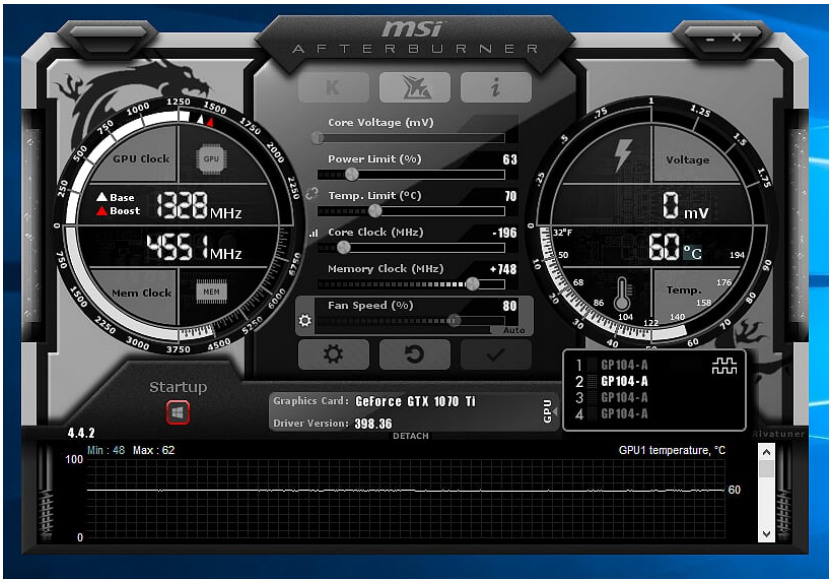
Jak je zřejmé, tyto hodnoty byly použity při všech základních testovacích běžích sestavy při těžbě měn Monero, Ethereum a Zcash. Nyní se však budeme pokoušet o odladění taktování grafických karet tak, aby se co nejvíce zvýšila výtěžnost grafických karet, ale co nejméně zvětšila spotřeba těžební soustavy.

9.2 Taktování a jeho přínosy

Taktování je obecně používáno pro zisk většího výkonu hardware komponent jako jsou paměti, procesor nebo grafický čip či paměť na grafické kartě. Jeho druhé nejčastější použití je přesný opak, kdy se hardware a to především procesor a grafický čip taktují tak, aby se snížil jejich výkon.

Toto může mít více důvodů, ať už thermal throttling, což je snižování výkonu komponent z důvodu přehřívání a snaze zabránit jejcih poškození. Další důvod může být například ten, kvůli kterému je taktování využito v tomto testu. Jedná se o taktování oběma směry, kdy se nepotřebná část hardware taktuje záporně, tedy snižujeme hodnotu a chtěné části hardware taktujeme kladně, tedy zvyšujeme jejich hodnoty.

V této části se jsou zobrazeny snímky softwaru MSI Afterburner,kde budou porovnávány změněné hodnoty v rámci taktování grafických karet s ohledem na zvolenou krypto měnu, jelikož některé měny požadují více a rychlejší paměti a jiné zase více a rychlejší paměti a zároveň vyšší výkon grafického jádra.

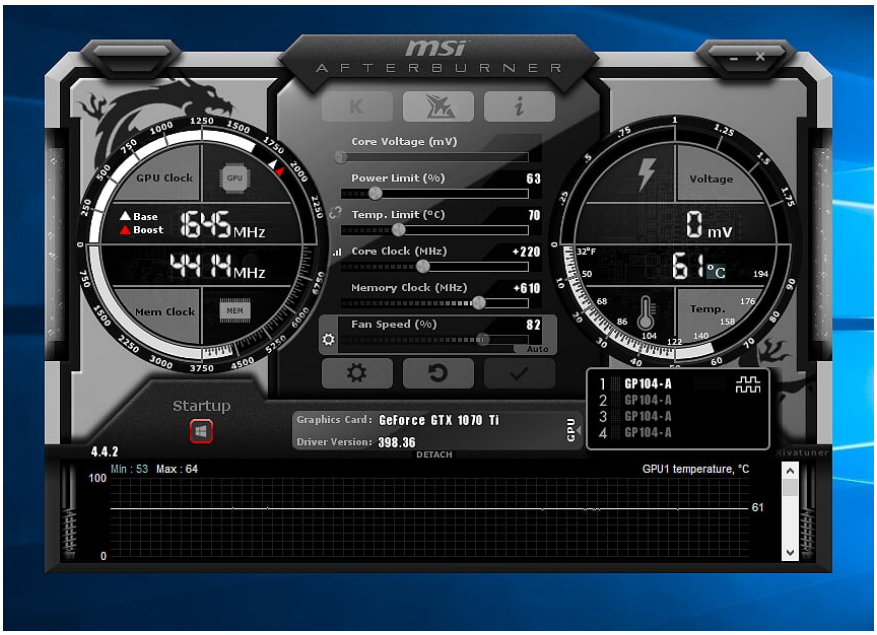


Obrázek 9.1: Ukázka konfigurace grafických karet pro těžbu kryptoměn Ethereum a Monero, vlastní tvorba.

Výše uvedený obrázek 9.1 představuje snímek MSI Afterburneru, kde lze vidět konfiguraci použitou pro těžbu kryptoměn Monero a Ethereum. Touto konfigurací se dosáhlo nejen nižších teplot grafických karet, ale také větší výtěžnosti, což lze vidět na obrázků 9.4 pro Ethereum a 9.3 pro Monero.

Dále je obrázek 9.2 na kterém lze vidět provedené změny pro těžbu kryptoměny Zcash. Na rozdíl od změn pro kryptoměny Ethereum a Monero, kde se snižovala frekvence jádra o 196 Mhz a navyšovala frekvence pamětí o 748 MHz, jelikož těžba těchto dvou měn je více stavěna na výkonu pamětí grafických karet, ale těžba Zcash je závislá jak na výkonu pamětí, tak i na výkonu grafického čipu.

Na tomto obrázku tedy vidíme taktování čipu i pamětí, kdy se čipu přidalo 220MHz a pamětem 610MHz. Dále je také důležité podotknout změnu horních tepelných hranic pro grafické karty. Tímto zajistíme, že se vytvoří efektivnější křivka pro chlazení a hardware tím pádem degraduje pomaleji. V obou konfiguracích se snížil příkon na 63 procent.

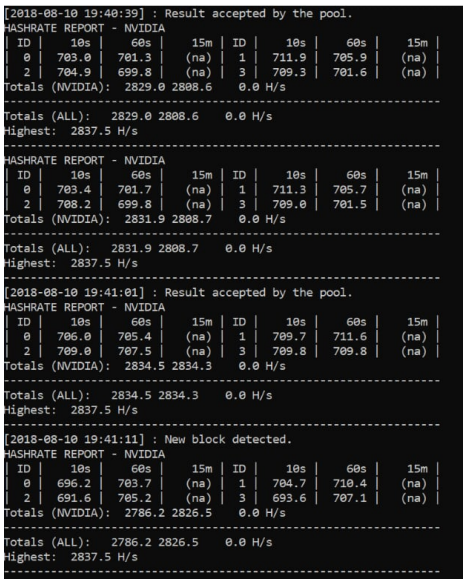


Obrázek 9.2: Ukázka konfigurace grafických karet pro těžbu kryptoměn Zcash, vlastní tvorba.

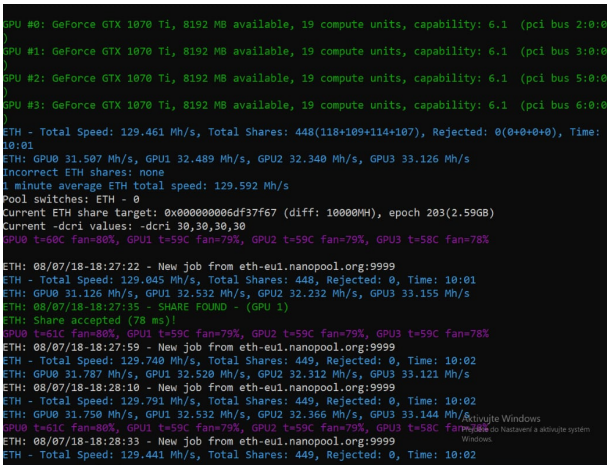
9.3 Porovnání výtěžnosti po taktování oproti základnímu nastavení

Tato část práce se zaobírá porovnáním výtěžnosti po proběhlém taktování grafických karet a zároveň již po proběhlém testu při výchozí konfiguraci. Tyto změny bude možné porovnat díky snímkům pořízeným Windows příkazové řádky, kde jsou spuštěny minery. Tyto minery nám přímo vypisují aktuální výtěžnost dle konfigurace karet.

Jako první lze uvést porovnání výtěžnosti při těžbě kryptoměny Monero. Po taktování vidíme růst výtěžnosti na níže uvedeném obrázku 9.3 a pokud tyto hodnoty porovnáme s již dříve zmíněnými hodnotami z testu při výchozí konfiguraci, zjistíme nárůst průměrně 700 H/s, což je podstatně velký procentuální nárůst výtěžnosti. Čímž dokazujeme, že taktováním lze dosáhnout vyšší výtěžnosti grafických karet na zvolených kryptoměnách.



Obrázek 9.3: Ukázka výtěžnosti grafických karet při těžbě kryptoměny Monero po provedení taktování, vlastní tvorba.

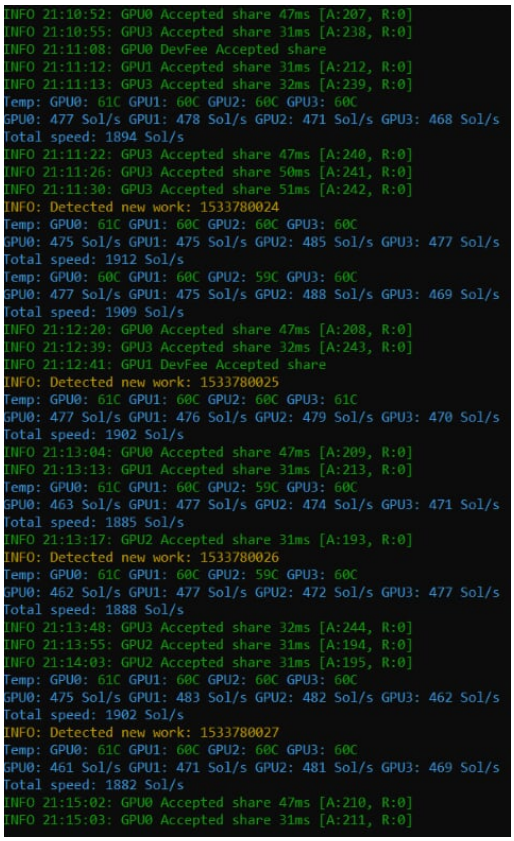


Obrázek 9.4: Ukázka výtěžnosti grafických karet při těžbě kryptoměny Ethereum po provedení taktování, vlastní tvorba.

Jako druhé máme porovnání výtěžnosti na obrázku 9.4 po taktování při těžbě kryptoměny Ethereum. Opět po taktování lze vidět změny výtěžnosti a nyní se jedná o nárůst z průměrné celkové výtěžnosti při výchozím nastavení 107 Mh/s vzrůst na 129 Mh/s při použití upravené konfigurace pro taktování grafických karet. Toto lze opět označit za úspěch, kdy jsme taktováním dosáhli vyšší výtěžnosti.

Poslední porovnání výtěžnosti se týká kryptoměny Zcash. Změny výtěžnosti lze vidět na obrázku 9.5, kde můžeme vyčíst změnu oproti výchozí konfiguraci, kde výtěžnost dosáhla průměrně 1830 Sol/S a po upravení konfigurace a taktování grafických karet výtěžnost stoupla na průměrných 1890 Sol/s, což je oproti oběma předchozím kryptoměnám zanedbatelná a nečekaně malá změna.

V takové situaci jako která nastala s kryptoměnou Zcash je důležité zvážit nárůst spotřeby těžební soustavy oproti nárůstu výtěžnosti soustavy. Jelikož při takto malé změně výtěžnosti se může soustava přesunout z výdělečné kategorie do prodělečné kategorie.



Obrázek 9.5: Ukázka výtěžnosti grafických karet při těžbě kryptoměny Zcash po provedení taktování, vlastní tvorba.

10 Shrnutí a závěr

Cílem této bakalářské práce bylo ukázat praktickou stavbu počítačové soustavy se zaměřením na těžbu kryptoměn , její otestování pří těžbě specifických kryptoměn za pomoci vybraných těžebních softwarů a její software konfiguraci. Počínaje nastavením BIOS až po taktování grafických karet. Jako výsledek této práce je funkční, otestovaná a těžby schopná počítačová sestava.

V teoretické části bylo uvedeno vše důležité pro porozumění základům grafických karet jako komponenty osobních počítačů a jejich role v těžbě, dále je úvod do kryptoměn, jejich těžby a také obecné seznámení s terminologií těchto technologií a jejich obecná historie.

V praktické části se už nachází samotná volba hardware komponent těžební soustavy, porovnání grafických karet společností AMD a NVidia v rámci této soustavy. Bylo zde pojato a popsáno nastavení BIOS základní desky pro lepší těžební výsledky.

V testování těžební soustavy a při porovnávání grafických karet, byli použity poznatky, získané samotným během a taktováním těžební soustavy. Během soustavy byla tedy dokázána její funkčnost a také jaký vliv má taktování grafických karet na výtěžnost grafických karet při těžbě vybraných kryptoměn.

Bylo tedy ověřeno, že taktování grafických karet nemá vždy pro každou kryptoměnu smysl ale u dvou kryptoměn ze tří testovaných byl po taktování úcty hodný nárůst výtěžnosti. Tímto se potvrdilo taktování jako kladný způsob navýšení výtěžnosti těžebních sestav.

Literatura

[1] Hive os is monitoring and management platform for mining rigs.

[2] Mining calculator bitcoin, ethereum, litecoin, dash and monero.

[3] Asus.com. Mining-p106-6g | graphics cards | asus global, 2018. https://www.asus.com/Graphics-Cards/MINING-P106-6G/.

[4] Bourque, B. Graphics cards: A beginner's guide to getting the best gpu for you, May 2014. https://www.digitaltrends.com/computing/graphics-card-guide-best-low-mid-and-high-end-graphics-cards-out-now/.

[5] Bromley, A. G. Charles babbage's analytical engine, 1838. *IEEE Annals of the History of Computing 20*, f4 (1998), 29–45.

[6] Chaum, D. Blind signatures for untraceable payments. *Advances in Cryptology* (1983), 199–203. https://link.springer.com/chapter/10.1007/978-1-4757-0602-4_18.

[7] Coindesk. How to calculate mining profitability, Jan 2016. https://www.coindesk.com/information/mining-profitability/.

[8] CoinDesk. Bitcoin hash functions explained, May 2017. https://www.coindesk.com/bitcoin-hash-functions-explained/.

[9] CoinGuides.org. Equihash pow mining algorithm - list of all equihash coins, Apr 2018. https://coinguides.org/equihash-coins/.

[10] CoinGuides.org. What is ethash? a list of all ethash coins - ethash pow algorithm, Mar 2018. https://coinguides.org/ethash-coins/.

[11] Computer, P. C. Configure pc w/ nvidia geforce gtx 1080 ti 11gb video card.

[12] Covington, J. Geforce vs quadro – what's the difference?, Jun 2018. http://www.velocitymicro.com/blog/geforce-vs-quadro-whats-the-difference/.

[13] Cryptowat.ch. Cryptowatch, july 2018. https://cryptowat.ch/.

[14] CZC.cz. Zotac geforce gtx 1080 arcticstorm. https://www.czc.cz/zotac-geforce-gtx-1080-arcticstorm-8gb-gddr5x/207489/produkt utm source=heureka.cz&utm medium=cpc&utm campaign=Graficke karty&utm term=Zotac GeForce GTX 1080 ArcticStorm 8GB GDDR5X.

[15] Finder. 2018's best cryptocurrency wallets | 70 compared, Jul 2018. https://www.finder.com/cryptocurrency/wallets.

[16] Heureka.cz. Grafické karty, 2018. https://graficke-karty.heureka.cz/.

[17] King, R. What is cryptocurrency: Cryptocurrency explained the easy way, Jul 2018. https://www.bitdegree.org/tutorials/what-is-cryptocurrency/#Crypto Definition.

[18] Knyaz. Cryptonight algorithm and how to mine cryptocurrency monero, bytecoin etc. - steemit, 2016. https://steemit.com/bitcoin/knyaz/cryptonight-algorithm-and-how-to-mine-cryptocurrency-monero-bytecoin-etc.

[19] Kundu, K. What is asic and how it is taking over bitcoin mining?, Sep 2017. https://beebom.com/what-is-asic/.

[20] Madeira, A. Mining pools and how they work, Oct 2017. https://www.cryptocompare.com/mining/guides/mining-pools-and-how-they-work/.

[21] MyBroadband. How graphics cards have evolved over the years. https://mybroadband.co.za/news/hardware/196964-how-graphics-cards-have-evolved-over-the-years.html.

[22] Oberhaus, D. What is an asic miner and is it the future of cryptocurrency?, Apr 2018. https://motherboard.vice.com/en us/article/3kj5dw/what-is-an-asic-miner-bitmain-monero-ethereum.

[23] Schmidt, K. Ethereum mining: Proof of stake/proof of work hybrid model, Nov 1969. https://blockgeeks.com/guides/ethereum-mining-proof-stake/.

[24] Schroeder, S. Dorian nakamoto: I am not the creator of bitcoin, Mar 2014. https://mashable.com/2014/03/07/dorian-nakamoto-bitcoin/?europe=true#VLM43ZB1Iiqc.

[25] Skvorc, B. Proof of stake vs proof of work, Jul 2018. https://www.sitepoint.com/proof-of-stake-vs-proof-of-work/.

[26] ZeroCoin. Why equihash? – zcash blog. https://blog.z.cash/why-equihash/.

Přílohy

Seznam obrázků

Seznam tabulek

Univerzita Hradec Králové
Fakulta informatiky a managementu
Akademický rok: 2017/2018

Studijní program: Aplikovaná informatika
Forma: Prezenční
Obor/komb.: Aplikovaná informatika (ai3-p)

Podklad pro zadání BAKALÁŘSKÉ práce studenta

PŘEDKLÁDÁ:	ADRESA	OSOBNÍ ČÍSLO
Kalous Jiří	Hynčice 24, Hynčice	I14085

TÉMA ČESKY:

Využití grafických karet se zaměřením na těžbu kryptoměn

TÉMA ANGLICKY:

The use of graphics cards with focus on crypto currency mining

VEDOUCÍ PRÁCE:

doc. Ing. Hana Tomášková, Ph.D. - KIT

ZÁSADY PRO VYPRACOVÁNÍ:

Obsahem teoretické části práce je nastínění vývoje a historie grafických karet a jejich možnosti využití k těžbě kryptoměn. Obsahem praktické části je výběr optimálního hardwaru, stavba těžební soustavy, a taktování grafickách karet s následným testováním hardwaru na specifických kryptoměnách.

OSNOVA:
Úvod
1.Historie a vývoj grafických karet
2.Popis grafických karet a specializovaného hardware pro těžbu
3.Úvod do kryptoměn
4.Problematika těžby kryptoměn
5.Volba hardware, stavba a testování těžební sestavy
Závěr,zdroje

SEZNAM DOPORUČENÉ LITERATURY:

John B. Purcaru - Games vs. Hardware. The History of PC video games: The 80's. Purcaru Ion Bogdan, 2014.

Sameer Shaikh - Complete Computer Hardware Only PediaPress.

Podpis studenta: ..... **Datum:** .....

Podpis vedoucího práce: ..... **Datum:** .....