Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Diplomová práce

Návrh sestavy výpočetní techniky určené ke zpracování úloh stanovenými algoritmy pro těžbu kryptoměn

Bc. Stanislav Ryšánek

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Stanislav Ryšánek

Informatika

Název práce

Návrh sestavy výpočetní techniky určené ke zpracování úloh stanovenými algoritmy pro těžbu kryptoměn

Název anglicky

Design of computerized assemblies designed to handle tasks determined by algorithms for cryptocurrency mining

---

Cíle práce

Diplomová práce je tématicky zaměřena na těžbu blockchainových kryptoměn pomocí hardware. Dílčím cílem práce je návrh řešení, které bude sloužit k vytvoření optimalizované sestavy hardwarových komponentů určených pro zpracování výpočetních úloh stanovenými algoritmy pro těžbu kryptoměn tzv. „mining farmy“. Součástí bude i srovnání kryptoměnových blockchainových technologií s již využívanou podobnou technologií a provedení ekonomického zhodnocení navrhované varianty s ohledem na návratnost investice.

Metodika

Metodika řešené problematiky bude obsahovat studium a analýzu již používané decentralizované databáze a následné srovnání s blockchain technologií. Bude provedena analýza hardwarových komponent s ohledem na výběr vhodné sestavy pro výpočet úloh těžebních algoritmů. Z ekonomického pohledu budou analyzovány vhodné měny pro těžbu s ohledem na současný i historický vývoj cen a návratnosti investice. Dále pak bude také součástí vlastní práce optimalizace výkonu těžby a volba vhodného software pro těžbu. Na základě zvolené metodiky práce bude uvedeno shrnutí a doporučení vlastního návrhu řešení.

Doporučený rozsah práce

60 – 80 stran

Klíčová slova

grafická karta, kryptoměny, blockchain, těžební farma, výpočet algoritmů

Doporučené zdroje informací

ENGLANDER, I. *The architecture of computer hardware and systems software : an information technology approach.* New York: Wiley, 2003. ISBN 0471073253.

CHEN, X. – SIMCHI-LEVI, D. – BRAMEL, J. *The logic of logistics : theory, algorithms, and applications for logistics and supply chain management.* New York: Springer, 2005. ISBN 0387221999.

PATTERSON, D A. – HENNESSY, J L. *Computer organization and design : the hardware/software interface.* San Francisco, Calif.: Elsevier Science [distributor], 2007. ISBN 978-0-12-370606-5.

SEUL, M. – O'GORMAN, L. – SAMMON, M J. *Practical algorithms for image analysis : description, examples, and code.* Cambridge: Cambridge University, 2005. ISBN 0-521-66065-3.

SHEPHERD, J C. *Database management : theory and application.* Boston: Irwin, 1990. ISBN 0-256-07829-7.

Předběžný termín obhajoby

2018/19 LS – PEF

Vedoucí práce

Ing. Václav Lohr, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 10. 10. 2018

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 19. 10. 2018

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 14. 03. 2019

Čestné prohlášení

Prohlašuji, že svou diplomovou práci „Návrh sestavy výpočetní techniky určené ke zpracování úloh stanovenými algoritmy pro těžbu kryptoměn“ jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne _____

Poděkování

Rád bych touto cestou poděkoval Ing. Václavu Lohrovi, Ph.D. za pomoc a podporu během průběhu psaní práce. Dále bych chtěl poděkovat svému otci Ing. Stanislavu Ryšánkovi za jeho připomínky k obsahu práce.

Návrh sestavy výpočetní techniky určené ke zpracování úloh stanovenými algoritmy pro těžbu kryptoměn

Abstrakt

V diplomové práci je možné nalézt návrh řešení sestavy výpočetní techniky schopné těžit kryptoměny. Strukturálně je rozdělena na 3 hlavní kapitoly.

V první kapitole jsou teoretická východiska práce, které popisují fungovaní a princip kryptoměn, a další pojmy nezbytné pro pochopení uvedené problematiky.

Části vlastní práce obsahují vytvořenou analýzu a optimalizaci komponent. Je uvedeno srovnání používané technologie s novou technologií blockchainu. Součástí vlastního řešení je analýza kryptoměn vhodných k těžbě. Práce řeší pouze koncept Proof of Work, který se týká těžení kryptoměn pomocí výpočetní techniky.

V závěrečné části *„výsledky a diskuse“* je daná sestava uvedena do provozu. Je zde ukázka postupné optimalizace těžení s výstupem vhodných parametrů určených pro konkrétní navrhovanou výpočetní sestavu. Ve výsledcích je možné nalézt ekonomické zhodnocení navržené varianty a její následnou návratnost.

Klíčová slova: Grafická karta, kryptoměny, blockchain, těžební farma, výpočet algoritmu, transakce, adresa, taktování, ROI, Ethereum

Design of computerized assemblies to handle tasks determined by algorithms for cryptocurrency mining

Abstract

This diploma thesis is supposed to find a design solution for a computer technology capable of extracting cryptocurrencies. The structure is divided into three main chapters.
In the first chapter, there are theoretical bases of the work, which describe the functioning and principle of cryptocurrencies, and other terms necessary for understanding the mentioned problems.
In the part of my work is created analysis and optimization of components. There is a comparison of the technology used with the new blockchain technology. Part of the solution is the analysis of cryptocurrencies suitable for mining. The work deals with the concept of Proof of Work, which concerns cryptocurrency mining using only compute power.
In the final part, the results and discussion are put into operation. There is an example of gradual optimization of the mining with the output of suitable parameters designed for a proposed computer assembly. In the results it is possible to find the economic evaluation of the proposed variant and its subsequent return.

Keywords: Graphic card, cryptocurrency, blockchain, mining farm, algorithm calculation, transaction, address, overclocking, ROI, Ethereum

Obsah

Seznam obrázků

Seznam tabulek

1. Úvod

Dnes již známý pojem kryptoměny je neustále rostoucí fenomén, který začíná pronikat i mezi běžné lidi. Pojmy jako je Bitcoin či blockchain se objevují v novinových článcích, televizních pořadech, rádiu a v dalších médiích zabývající se touto problematikou. Rostoucí zájem veřejnosti přilákává investory, společnosti a vizionáře k této tematice. Z pohledu nováčka ochotného se touto problematikou zabývat, nemusí být vždy snadné začít, vzhledem k rozsáhlému množství různorodých informací z navzájem nesouvisejících zdrojů.

Tato práce se snaží toto téma přiblížit novým zaujatým lidem v souvislosti s těžbou těchto digitálních měn a předpokladem možné investice do tohoto odvětví. Běžný člověk se zde seznámí se základny hardware a software nutného pro těžbu. Získá představu o návratnosti investice s ohledem na reálně použitá data. Seznámí se s blíže specifickými věcmi týkajícími se těžby, jako je optimalizace grafických karet, rozdíl mezi GPU a ASIC, co je to těžící algoritmus a jak se mění náročnost vzhledem k vytížení blockchainové sítě.

Bude vysvětleno, jakým způsobem tato technologie funguje a dojde i ke srovnání již dávno používané peer-to-peer technologie.

Tyto informace mají sloužit pro úvodní seznámení se s možnostmi těžby kryptoměn a pro pochopení potřebných souvislostí při stavbě vlastní těžební soustavy. V práci je kladen důraz i na ekonomickou stránku věci, jako je výběr vhodné měny či předpokládaná návratnost dané investice.

2. Cíl práce a metodika

2.1 Cíl práce

Diplomová práce je zaměřena na těžební hardware a s tím související vhodný výběr komponent použitých k sestavě funkčního počítače, který tyto kryptoměny bude schopný efektivně těžit. V souvislosti s kryptoměnami jsou objasněny současné technologie na bázi decentralizace a porovnány s blockchainovou technologií. Důležitou součástí je i ekonomická návratnost této investice s ohledem na uplynulé časové období. Hlavním cílem práce je navrhnout funkční řešení sloužící ke stavbě zařízení schopného počítat úlohy stanovenými algoritmy pro těžbu kryptoměn.

Dílčími cíli jsou:

- Srovnání decentralizovaných technologií s blockchainem
- Výběr vhodné měny pro těžbu
- Optimalizace a návratnost těžby

Stanovené cíle jsou splněny na reálných číslech z výsledku těžby za určité časové období.

2.2 Metodika

Nejprve budou objasněny důležité pojmy pro pochopení dané problematiky. Následně budou srovnány technologie již běžně používané decentralizované databáze s blockhainovou technologií. Po srovnání technologií dojde k návrhu řešení sestavy schopné těžit kryptoměny s ohledem na ekonomickou stránku věci, a to zejména výběr vhodné digitální měny a s tím související volba algoritmu, který stanovuje dané úlohy nezbytné k samotné těžbě dané digitální mince. S návrhem tohoto řešení bude souviset optimalizace těžebního zařízení a volba vhodného software. To vše bude provedeno s ohledem na náklady, a tudíž i potencionální návratnost investice. Na závěr proběhne diskuze na dané téma a dojde k přihlédnutí k výsledkům daného vlastního řešení.

3. Teoretická východiska

V této kapitole jsou objasněny teoretické pojmy nezbytné pro pochopení dané problematiky.

3.1 Základní komponenty sestavy výpočetní techniky určené k těžbě kryptoměn

V našem případě bude nutné sestavit počítač z následujících komponent:

- Zdroj PC
- Základní deska (Motherboard)
- Procesor (CPU)
- Operační paměť (RAM)
- Pevný disk (HDR, SSD)
- Grafická karta (GPU)
- PCI redukce (Riser)

Samotný počítač nebude používat klasickou skříň (case), ale místo toho je vložen do hliníkové konstrukce z důvodu odvodu tepelného odpadu.

Zdroj

Počítač je nutné napájet stálým zdrojem elektrické energie. K tomuto účelu slouží dostatečně dimenzovaný zdroj PC. Zejména v těžební sestavě hraje zdroj velice důležitou roli, protože grafické karty běží neustále v plné zátěži a vyžadují konstantní přísun elektrické energie. Pokud by zdroj nebyl kvalitní, může dojít i k požáru. Původní AT zdroje přímo fyzicky vypínaly počítač a dodávaly výkon 200 W. Pro dnešní moderní grafické karty by tento výkon byl zcela nedostačující. V roce 1995 se objevily zdroje ATX, které jsou aktuální až do současnosti. Tyto zdroje jsou schopné dodat několikanásobně vyšší výkon. Nesdílnou a důležitou součástí zdroje je ventilátor, který ochlazuje proudem vzduchu samotnou krabičku zdroje. Těžební sestava je vystavena vysokým teplotám a zdroj je kritické místo, které je potřeba ochlazovat [1].

Základní deska

Základní deska je základním stavebním kamenem každého počítače, a tudíž i těžební soustavy. Zajišťuje komunikaci mezi dalšími komponentami. Mezi základní pojmy pro umístění patří patice, sloty a konektory, do kterých jsou tyto komponenty umístěny či připojeny. Dnešní základní desky již v sobě obvykle mají integrovány některá základní zařízení. Například v případě těžební soustavy je typicky využita integrovaná síťová karta [1].

Procesor

Hlavním „mozkem“ počítače je procesor. Nepostradatelná součástka provádějící výpočty nutné k chodu počítače, a to především operačního systému. Výkon procesoru záleží na jeho typu a nastavené frekvenci, na které běží. V těžební sestavě není nutný výkonný čip, ale spíše je brána na zřetel jeho spotřeba, která je v dnešní době poměrně vysoká. V případě těžby není nutné na počítači pracovat a postačí pouze běh operačního systému a softwaru určeného k těžbě. Běžnou součástí procesoru je aktivní chladič usazený přímo na procesoru. Mezi hlavní výrobce procesorů patří společnosti Intel a AMD [1].

Operační paměť

Pracuje průběžně s daty a instrukcemi, se kterými je vykonávána aktuální činnost. Pokud dojde k výpadku dodávky elektrické energie, všechna data uložená v této paměti jsou nenávratně ztracena. Těžební software je poměrně náročný na operační paměť, proto je důležité nepodcenit množství této kapacity. V tomto případě je vhodné raději koupit paměť větší, než je minimální požadované množství, s ohledem na budoucí aktualizace softwaru. Paměti lze na základní desce i kombinovat, ale je třeba mít na paměti, že existuje řada vzájemně nekompatibilních typů těchto paměti [1].

Pevný disk

Médium slouží k trvalému ukládání dat. Pro účely těžební sestavy je zvolen polovodičový disk – alternativa ke klasickému pevnému disku. Je to soustava energeticky nezávislých flash pamětí. Výhodou je větší odolnost díky absenci mechanických součástí a velikost samotného komponentu. Naopak negativem bývá menší životnost těchto disků. Samotné ukládání dat do polí paměťových buněk funguje na stejném principu [2].

Grafická karta

Zdaleka nejdůležitější součást těžební sestavy je grafická karta. Je to „hnací motor“ těžení. Obvykle slouží k zobrazování barevného výstupu na monitoru, 3D modelování a obecně splňuje náročné požadavky dnešních softwarů. V případě sestavy v této diplomové práci jsou v hledáčku pouze moderní grafické karty, které se staly dedikovanými počítači s vlastním procesorovým čipem a operační pamětí. Tyto grafické karty mají vysoké nároky na spotřebu elektrické energie a je důležité s tímto faktem počítat při vhodného výběru zdroje. Karta se připojuje do „PCI“ slotu na základové desce. Těchto slotů je vhodné mít k dispozici na desce více, pokud je do těžební soustavy zapojeno více grafik současně [3].

PCI Redukce

Nezbytným prvkem, pokud je v soustavě zapojeno více grafických karet těžební soustavy, jsou PCI redukce. Tento propojovací kabel mezi grafickou kartou a základní deskou rozšiřuje počet slotů a zajišťuje plynulejší výměnu dat mezi komponenty.

3.2 ASIC

V neposlední řadě je důležité zmínit ASIC v podobě těžebního zařízení, což je vlastně integrovaný obvod určený pro konkrétní aplikaci. Tento hardware bývá specificky určen pro těžbu určité kryptoměny. Čipy určené pro těžbu jsou vestavěny přímo do základové desky. To z nich dělá vynikající těžební zařízení jak z hlediska úspory energie, tak i z hlediska nákladů na hardware. Nevýhodou je jejich specializace na konkrétní těžební algoritmus. Z toho plyne fakt, že se jedná o zařízení jednoúčelové. Na rozdíl od grafických karet, kde tato omezení nejsou [4].

3.3 Operační systém a software

Pro těžební sestavu je nutný operační systém. V době psaní této diplomové práce je v podstatě na výběr ze dvou možností:

- Linux
- Windows

Každý z těchto dvou systému přináší jiný přístup, jako je údržba, aktualizace, konfigurace a dálkový přístup.

3.3.1 Linux a jeho těžební distribuce

Pro účelnou těžbu na operačních systémech Linux byla navržena speciální distribuce jménem ethOS. Je to 64bitový operační systém, který je schopný provádět těžbu kryptoměn jako jsou například Ethereum, Zcash nebo Monero. Požadavky na tento systém:

- 8 GB paměti na pevném disku
- 64bitový systém
- Grafické karty

Distribuci je možné upravovat dle svých specifických požadavků. V současné době je aktuální verze ethOS 1.3.3. Tato verze podporuje grafické karty firem AMD a NVIDIA. Přes příkazový terminál je možné provádět nejrůznější příkazy týkající se dálkového ovládání těžební soustavy jako je například konfigurace těžebního software či taktování

grafických karet. Je schopna fungovat na 5. generaci procesorových čipů a je potřeba minimálně 2 GB operační paměti, což je úspora oproti operačnímu systému Windows. Kromě taktování je také možné přes tuto distribuci flashovat bios grafických karet [5].

3.3.2 Windows a software k optimalizaci těžby

V roce 2015 byla vydána nová verze operačního systému Windows s číslem 10. Tento operační systém je vhodný pro běžné uživatele, kteří nejsou spřízněni s používáním Linuxových distribucí. Nabízí klasické grafické rozhraní s myší, na které jsou uživatelé zvyklí. Důležité programy pro optimalizaci těžby na Windows jsou:

- ATIflash
- GPU-Z
- TriXX
- Ovladače grafické karty

Tyto programy slouží k zobrazení a optimalizování grafických karet v systému Windows. Jsou k dispozici zdarma a jsou neustále dále vyvíjeny za podpory jejich tvůrců. Podrobněji jsou popsány v části vlastní práce, kde je uveden popis, jak se s těmito programy pracuje.

3.3.3 Claymore's AMD+NVIDIA Miner v12.0

Nejnovější verze těžebního software, který běží na obou operačních systémech. Na grafických kartách s operační pamětí vyšší, než 3 GB vyžaduje poplatky ve výši podílu 1% procenta z celkové těžby. Je zde možnost těžit kryptoměny duálně, což znamená, že zvládne využívat nepokrytý výkon grafické karty pro další algoritmus, který tuto možnost umožňuje. Podporuje dva hlavní výrobce grafických karet AMD i NVDIA, a to s volbou tyto různé karty zapojit současně. Program je možné nastavit rozsáhlým množstvím příkazů v konfiguračním souboru před spuštěním vlastního těžení. Podrobné nastavení tohoto souboru je popsáno v části *„vlastní práce“* [6].

Tyto těžební programy běží neustále spuštěné a zpracovávají úlohy stanovené algoritmy pro těžbu kryptoměn. Průběžně dochází k jejich aktualizaci z důvodu neustálého vývoje

grafických ovladačů, nových verzí grafických karet a vydávaní nových verzí operačních systémů. Je potřeba zmínit velké požadavky na operační paměť.

3.4 Kryptoměny

Digitální měny v posledních letech upoutaly zájem široké veřejnosti. Během náhlého růstu cen kryptoměn v roce 2017 se rozběhly diskuse o pohádkových výnosech v masových mediích, což upoutalo pozornost nejen nadšenců a investorů, ale také řadových občanů, kteří se o tuto technologii začali hluboce zajímat. Na druhou stranu stále mnoho lidí dané problematice příliš nerozumí. Je tedy vhodné vysvětlit historický vývoj těchto kryptoměn a pojmy s nimi spojené.

3.4.1 Historie

Počátky kryptoměn začaly v závislosti na rozvoji kryptografie, která tvoří základ myšlenky kryptoměn, v devadesátých letech. Jedni z prvních, kteří s touto myšlenkou přišli, byla skupina zvaná „Cypherpunks“ [8].

Důvodem vzniku tohoto hnutí byl strach z centralizované diktatury států a nadnárodních společností ovládající významné části finančního sektoru, které mohly blokovat přístup k financím nežádoucím subjektům.

Jedním z takových případů byla WikiLeaks, nezisková mediální společnost, která byla označena Pentagonem za hrozbu americké národní společnosti [7].

Tento přístup dával lidem pocit, že je jejich život řízen a že přicházejí o možnost volby využívat svobodně své finanční prostředky. To mělo za následek vznik myšlenky nového platebního systému, který by byl nezávislý na centralizovaných platebních systémech.

Zásadním úspěchem skupiny „Cypherpunks“ byla anonymizace posílání e-mailů. V důsledku práce této skupiny nakonec USA zrušilo restrikce na export kryptografických technologií mimo jejich hranice [8].

S novým nástrojem se bylo možné dostat o kousek blíže k vývoji decentralizovaného systému a přišly na řadu první pokusy s kryptoměnami. Bohužel jedny z počátečních kryptoměn DigiCash ani CyberCash v tomto směru neuspěly, jelikož nesplňovaly veškeré

náležitosti kryptoměny. První taková kryptoměna přišla až s nástupem roku 2009, kdy přišel na scénu Bitcoin [9].

3.4.2 Definice kryptoměn

Každá kryptoměna musí splňovat list pravidel, aby se mohla považovat za oficiální:

- Digitální
- Decentralizovaná
- Peer-to-peer
- Pseudonymní
- Žádný prostředník
- Zašifrovaná
- Globální

Hlavní rozdíl mezi kryptoměnou a tradičními penězi spočívá v postrádání jakékoliv centrální autority [9].

Digitální

Kryptoměny existují pouze ve virtuálním světě. Nelze s nimi pracovat jiným způsobem než za pomocí počítačů. Nemají hmotnou povahu.

Decentralizovaná

Není žádný počítač nebo server, který by bylo možné vypnout nebo odstavit. Jsou distribuované napříč sítí skrze mnoho počítačů v této síti zapojených.

Peer-to-peer

Šíří se online z jedné adresy na druhou adresu. Fungují na principu výměnné sítě, kde je možné její prostřednictvím vyměňovat data.

Pseudonymní

Uživatel nepodává osobní informace o své osobě, ani o používaní kryptoměn. Nejsou stanovena pravidla, kdo a jak může používat či vlastnit kryptoměny.

Žádný prostředník

Uživatelé mají plnou kontrolu nad svými finančními prostředky. Žádná třetí strana není potřeba k funkčnosti systému.

Zašifrovaná

Každý účastník vlastní šifrovací kódy, ke kterým má přístup pouze on. Pomocí kryptografie je zaručena takřka absolutní ochrana proti nabouraní se do prostředků uživatele. Informace jsou schovány za šifrou.

Globální

Nic nebrání posílaní kryptoměn napříč světem po síti. Neexistují žádné hranice.

3.4.3 Kryptografie

Šifrování jsou metody a techniky zabezpečené komunikace. Ve své podstatě jde o určovaní pravidel a vytváření protokolů, které třetí straně zamezí možnost přečtení obsahu výměnných dat, narušit datovou integritu, autenticitu a nepopiratelnost.

- Integrita
- Autenticita
- Nepopiratelnost

Integrita

Možnost ověření, zda je zpráva nepoškozená a zda nedošlo ke změně ve zprávě.

Autenticita

Prokazatelnost vlastníka zprávy a jistota, že identita zprávy nebyla pozměněna.

Nepopiratelnost

Autor zprávy nemůže mít možnost popření odeslání zprávy [10].

Klasickým příkladem je přenos zprávy mezi dvěma účastníky konverzace. Účastník Alice posílá zprávu prostřednictvím sítě druhému účastníku Bobovi. Alice nechce, aby kdokoliv kromě Boba znal obsah její zprávy. Proto se rozhodne obsah zprávy zašifrovat a zároveň se podepíše pod zprávu, aby měla jistotu, že Bob pozná, že zpráva dorazila od ní.
Jeden ze způsobů, jak zprávu zašifrovat, je symetrická kryptografie. Alice šifruje zprávy pomocí tajného kódu. Zprávu pak pošle Bobovi a ten zprávu dešifruje pomocí klíče, který již od Alice obdržel dříve. Nevýhoda této metody spočívá v nutnosti předat klíč Bobovi před obdržením samotné zprávy [11].
Další způsob, jak zprávu zašifrovat, je asymetrická kryptografie. Alice požádá Boba o jeho veřejný klíč a svoji zprávu zašifruje právě pomocí tohoto Bobova veřejného klíče. Poté zprávu zašle Bobovi, který ji dešifruje pomocí svého privátního klíče. Výhoda této metody je evidentní – nemusí dojít k žádné předchozí výměně klíčů mezi Alicí a Bobem [12].
Kryptoměny využívají asymetrické kryptografie.

3.4.4 Popis kryptografické hashovací funkce

Tato funkce se specifickou třídou hashovací funkce má určité vlastnosti, které ji činí vhodnou pro použití v kryptografii. Jedná se o matematický algoritmus, který mapuje vstupní data libovolné velikosti do řetězce znaků s pevně danou délkou. Je navržen jako jednosměrná funkce. Jednosměrné funkce nelze invertovat zpět do původní podoby. Jediný

způsob, jak získat zpět vstupní data, je pokusit se o hrubé zadávání možných vstupů, aby se zjistilo, zda vytvářejí shodný výstupní řetězec znaků.
Ideální kryptografická hashovací funkce splňuje následujících pět vlastností.

Deterministická

To znamená, že opakovaně poslaná zpráva vyústí ve stejný hash.

Rychlá na výpočet

Jednoduše řečeno rychle spočítá jakýkoliv vstup bez zbytečných prodlev.

Nelze invertovat

Je nemožné generovat zprávu z její hashové hodnoty kromě pokusu o všechny možné vstupní zprávy.

Změna zprávy vygeneruje zcela rozdílný hash

Změna je tak extenzivní, že nová hodnota hash se bude jevit jako nekorelovaná s původní hodnotou hash.

Unikátní

Je nemožné najít dvě různé zprávy se stejnou hodnotou hash.

Podle předem zvoleného algoritmu dochází k vytváření hashe [10]. Konkrétní způsoby jsou popsány v další části popisující již specifické algoritmy určené pro konkrétní vybrané kryptoměny.

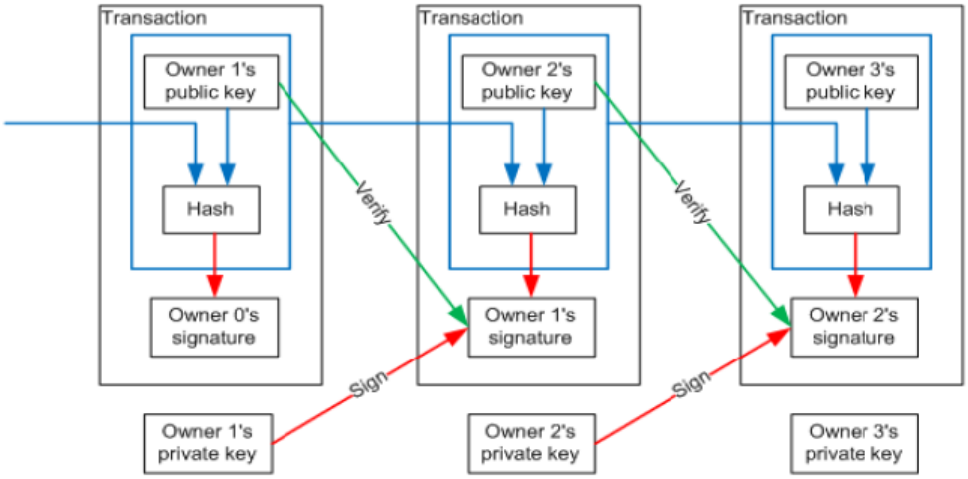
3.5 Blockchain

3.5.1 Adresa

Adresa vzniká na základě kryptografie. Podstatným prvkem je náhodně vygenerovaný privátní klíč. Z privátního klíče na základě kryptografické hashovací funkce vzniká klíč veřejný. Privátní klíč se používá k podpisu transakcí na blockchainové síti. K přijímání transakcí se používá veřejný klíč. Tyto dva klíče společně tvoří kryptoměnovou peněženku. Pokud je ztracen privátní klíč, již není možnost posílat transakce. To znamená, že veškeré prostředky vázané na ztracené adrese jsou nenávratně ztraceny.
Příklad Bitcoinového 256bitového privátního klíče
E9873D79C6D87DC0FB6A5778633389F4453213303DA61F20BD67FC233AA33262
S tímto klíčem je možné podepisovat transakce vázané k její veřejné adrese [14].

3.5.1 Transakce

Transakce v blockchainové síti znamená odeslaní či přijetí dat z jedné adresy na druhou. Transakce je podepsána privátním klíčem uživatele a jsou tam zahrnuty veškeré předchozí transakce. Jakmile uživatel transakci vytvoří, tak se dostává přímo do blockchain, kde jednotlivé uzly potvrzují, že transakci zachytily, tím že informaci o transakci zapíší do budoucího nově vytvořeného bloku. Potvrzování transakcí funguje v rámci metody Peer-to-Peer [15]. Potvrzení transakcí probíhá na bázi kryptografických metod, jakou je například metoda Proof of Work, která je vysvětlena v kapitole *„těžba“*.



Obrázek 1 - Podepisování transakcí privátním klíčem [13]

Schéma na obrázku ukazuje, jak uživatel podepisuje transakci svým privátním klíčem. Podepsání transakce zároveň určuje, kdo je jejím vlastníkem. Veřejná adresa je součástí transakce a určuje, komu je transakce adresována.

Transakce mají své priority, pokud odesílatel nastaví, obvykle přes klienta či webové rozhraní, vyšší poplatek, tak jeho transakce projde sítí rychleji. Vzorec pro výpočet priority transakce vypadá následovně.

$$\rho = \frac{\sum_{k=1}^{n}(y_k * z_k)}{v}$$

Kde,

p je priorita transakce

y je hodnota vstupu k

z je počet ověření vstupu k

v je velikost transakce v bytech

Právě tyto hodnoty je uživatel schopný ovlivnit a tím transakci uspíšit.

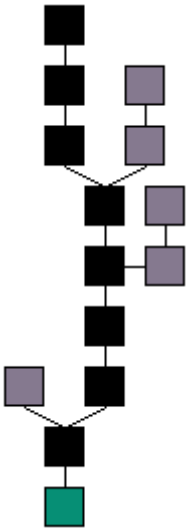
3.5.1 Blok

Transakční data jsou permanentně uložena do souborů zvané bloky. Laicky by se dalo říct, že jsou to strany účetní knihy. Bloky jsou organizovány do lineární posloupnosti v čase do tzv. blockchainu. Uchovávají v sobě veškeré informace o transakcích a o předchozím bloku. Nové transakce jsou těžebními uzly zaznamenávány do nových bloků a následně přidávány na konec řetězce. Čím je blok starší, tím je více a více zakopán do blockchainu a již ho nelze smazat nebo změnit. Vzhledem k algoritmu, pod kterým blok vznikl, obsahuje odpověď na matematickou hádanku, která je unikátní pro každý blok. Tím se stávají bloky jedinečnými. Bloky nelze do blockchainu zařadit dříve, než je matematická hádanka vyřešena. Odpověď na tyto hádanky nalézají těžební uzly procesem těžby. Více o blocích a jejich procesování je v kapitole *„těžba“* [16].

3.5.2 Princip blockhainu

Řetězec bloků funguje jako transakční databáze sdílená mezi všemi zúčastněnými uzly pracující ve stejném protokolu. Kompletní kopie blokového řetězce kryptoměny obsahuje úplně každou transakci, která kdy byla spuštěna. Díky tomu je možné zpětně dohledávat hodnotu adres v každém bodě bloku historicky. Každý blok totiž obsahuje hash předchozího bloku. Od prvního bloku „Genesis block“ se všechny předešlé bloky kopírují až do aktuálního bloku. Je možné tedy zaručit chronologické pořadí jednotlivých bloků, protože musí obsahovat identický předchozí hash. Transakce v blockchainu jsou nevratné, jakmile je jednou transakce spuštěna, již se uloží navždy do historie těchto bloků. Aktuální blok odkazuje pouze na předchozí blok a musí se jednat o poslední blok v nejdelším platném řetězci. Řetězec je platný, pokud jsou všechny transakce a bloky v něm platné, za předpokladu, že řetězec bloků začal od prvního bloku. V blockhainu může nastat situace, kdy vzniká tzv. „fork“. Pokud jsou bloky vytvořeny pár vteřin po sobě, tak některé z uzlů mohou začít přijímat rozdílný blok, jelikož obdržely zprávu o tomto bloku dříve. Vznikají tak dva vytěžené bloky. Nastane krátkodobý závod o nejdelší řetězec bloků. Vždy se počítá nejdelší řetězec bloků, transakce v kratším bloku jsou předány znovu do nejdelšího bloku. Kratší řetězec bloků se stává neplatným a těžební kapacity, které tyto bloky počítaly přijdou o odměnu. Těmto osiřelým blokům se také někdy říká „sirotci“. Aby se zamezilo

nejasnostem ohledně těchto odnoží blockchainu existuje síťově vynucena doba zrání. Pro Bitcoin je tato doba stanovena po generacích 100 bloků [13].



Obrázek 2 - Schéma vytěžených bloků [13]

3.6 Těžba kryptoměn

V rámci tématu této diplomové práce je v této zahrnuta pouze metoda Proof of Work. Ostatní metody jako je například Proof of Stake nejsou uvedeny, jelikož se netýkají návrhu těžebního zařízení ani dílčích cílů. Koncept Proof of Work je vysvětlen na Bitcoinové síti, stejně tak jako těžba jednotlivých bloků. Každá kryptoměna, kterou lze touto metodou těžit, tyto koncepty z části nebo úplně mění pro svoje vlastní účely.

Těžbu kryptoměn je možné vykonávat hardwarem společně se specifickým softwarem určeným pro těžbu. Jedním z rozlišovacích faktorů kryptoměn je právě způsob jejich těžby. Způsob těžby určuje jejich algoritmus, který vytváří matematické hádanky. Vybrané jednotlivé algoritmy:

- Ethash
- CryptoNight

Tyto algoritmy se týkají konkrétních kryptoměn ETH a XMR. Dále jsou objasněny důležité pojmy běžně využívané v oblasti těžení kryptoměn.

Mining

Proces za účelem vypočítat úlohu stanovenou těžebními algoritmy.

Miner

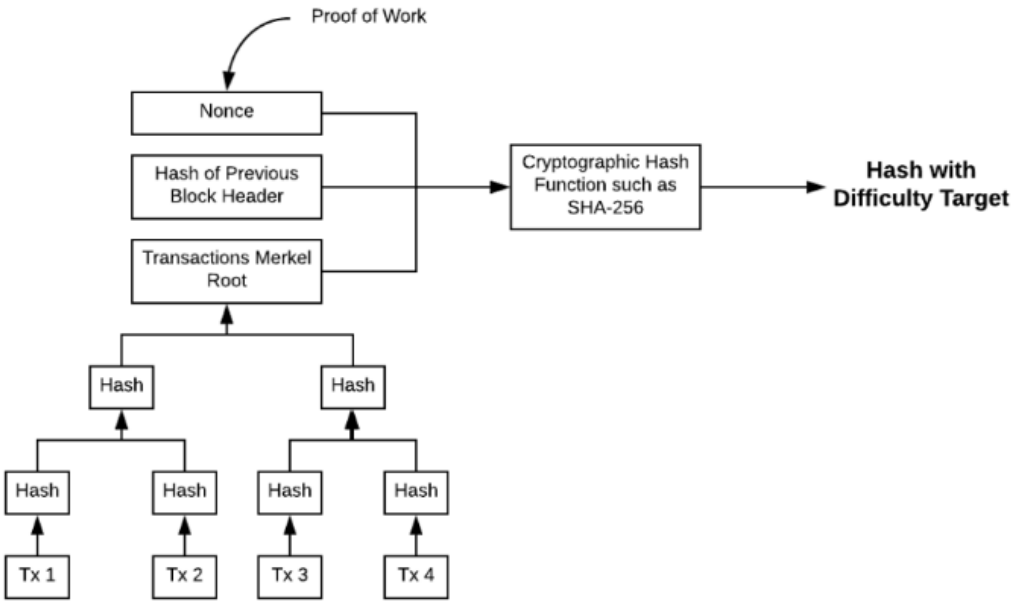
Nespecifikované množství těžebních soustav zapojených do miningu v rámci jedné blockchainové sítě. Miner znamená těžební uzel, který počítá úlohy zadané těžebními algoritmy.

Těžební rig

Výpočetní sestava určená k výpočtu úloh stanovenými algoritmy pro těžbu kryptoměn.

3.6.1 Proof of work

Tato metoda byla původně jako obrana proti emailovému zasílání hromadných zpráv. Každá kryptografická funkce má svoji slabinu, která spočívá v tom, že útočník se může donekonečna pokoušet o odhad vstupu za předpokladu, že zná algoritmus, který vytvořil ze vstupu hash [17]. Tento postup se nazývá Brute Force metoda. Při jejím použití dochází k systematickému testování všech kombinací, čí podmnožiny kombinací.
Proces hledání vhodného vstupu se nazývá mining. Pokud je zadaný určitý 32bitový podřetězec v binární reprezentaci hashe, tak je potřeba vyzkoušet 2^{32} pokusů možných vstupů, než je objeven vstup se správným výsledkem. Hledání toho výsledku zabere mnoho energie a času, proto se tato metoda nazývá Proof of Work.



Obrázek 3 - Ukázka principu POW [36]

Miner, který se účastní Proof of Work hlasuje svým výpočtem o transakční historii. Jeho výpočty se pak shodují s výpočty dalších minérů a dochází k potvrzení výsledku úlohy stanovené těžebními algoritmy.

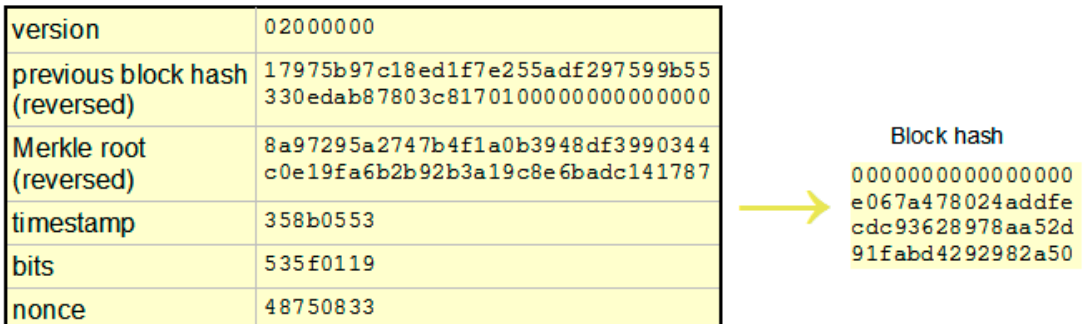
První miner, který přichází na řešení úlohy dostává odměnu formou mincí dané kryptoměny, kterou těží. Je důležité, aby svůj výsledek oznámil v síti jako první a ostatní mineři následně tento výsledek potvrdili [18].

3.6.2 Těžební blok

Vytěžené bloky obsahují provedené transakce a hlavičku. V hlavičce bloku lze nalézt následující informace:

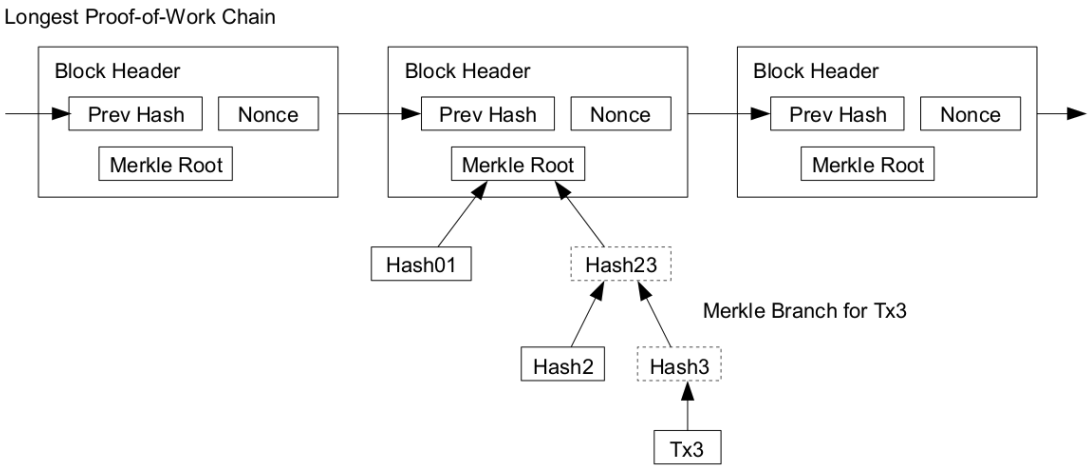
- Verze
- Předchozí vytěžený blok
- Hash (Merkle root) hlídá integritu dat v bloku

- Časové razítko
- Obtížnost (Bits) závisející na metodě Proof of Work
- Měnící se hodnota (Nonce) během hledání vstupu při miningu



Obrázek 4 - Hlavička bloku [37]

Merkle root je kořenová hash samotného Merkle tree. Merkle tree je vypočítaný soubor všech transakcí v daném bloku. Vytváření Merkle tree probíhá tak, že se z každé transakce v bloku vytvoří hash. Potom se takto vytvořené hashe skládají po párech do binárního stromového konceptu. Každý pár následně vytvoří další hash a tak se to opakuje, dokud nezbývá poslední hash bez páru. Tato poslední hash se tedy nazývá Mekle root a je umístěna v hlavičce bloku. Tento proces je efektivní způsob, jak standardizovat pevnou velikost bloku, což vede k celkové úspoře paměti, jelikož není potřeba k ověření transakce celý blockchain. Tato metoda se nazývá Simlified payment Verification [18]. Na následujícím obrázku je znázorněn, jak se postupně vytvoří Merkle root a jak je vložen do hlavičky bloku.



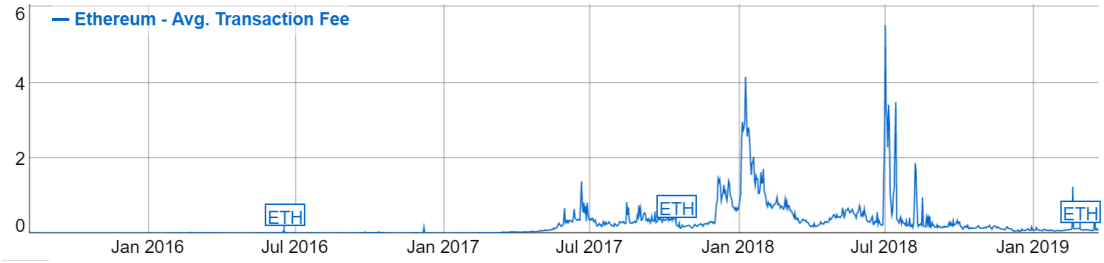
Obrázek 5 - Ukázka půlení hashe do Merkle Root [38]

Bloky jsou základním stavebním kamenem každé těžitelné kryptoměny. Důležité je také zmínit „fork“ (viz. kapitola 3.5.2 Princip blockchainu). Toto oddělení se od původního účelu může být záměrné, když se část skupiny minerů rozhodne od původního blockchainu upustit a pokračovat ve svém vlastním blockchainu s novými pravidly.

3.6.3 Odměny

Těžení kryptoměn není zadarmo. Mineři musí investovat do těžebních soustav. Platit poplatky za energie, internet a za prostory. Na druhou stranu blockchain bez minerů, kteří potvrzují transakce nemůže existovat, proto je vytvořený systém odměn za vytěžení bloků. Velikost odměny se liší dle dané kryptoměny a může se v průběhu času měnit.

Kromě získání odměny za vyřešení úlohy nového bloku si může miner v daném bloku také přičíst poplatky za transakce. Není žádná povinnost zahrnovat poplatky do vytěženého bloku, stejně tak jako vyslané transakce uživateli sítě. Poplatek je motivace tyto transakce v bloku zahrnout. Čím větší je poplatek, tím rychleji bude miner chtít tuto transakci potvrdit. Čím větší poplatek, tím bude transakce rychlejší [19].

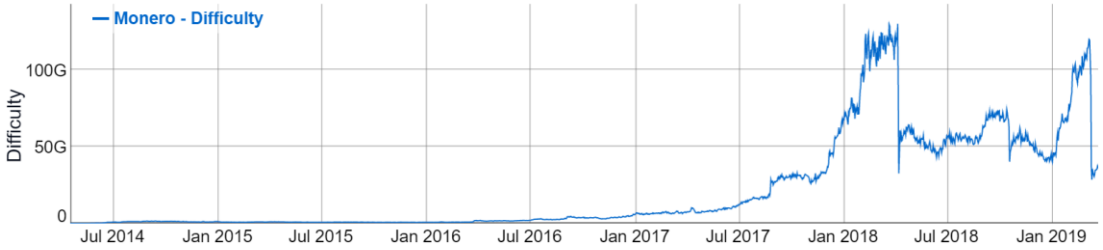


Obrázek 6 - Znázorněný graf poplatků za transakci v síti ETH v dolarech [39]

Na obrázku grafu je vidět, že ceny poplatků u ETH se skokově mění podle období. Z pravidla se cena poplatku zvedá s rostoucím množstvím požadovaných transakcí.

3.6.4 Obtížnost

Tuto vlastnost jednotlivých bloků určuje algoritmus blockchainu. Obecně se používá koncept závisející na počtu aktivních minerů. Obtížnost těžení je přímo úměrná sazbě vytěžených bloků. Na obrázku grafu je znázorněna obtížnost těžby XMR v průběhu času.



Obrázek 7 - Graf obtížnosti XMR [40]

Obtížnost je měřena v počtu vypočítaného hashe za sekundu. Rychlost počítaní hashe se nazývá hashrate. Bloky kryptoměn mají ve svých algoritmech nastaveno, za jaký časový úsek bude vytěžen nový blok [20].

3.6.5 Pool

Protože většinou miner nedisponuje dostatečným hahsrate, aby zvládl vytěžit blok samostatně, vznikly skupiny minerů spojené do velkých poolů. Těžení v poolu je zaručený způsob, jak dosáhnout jistého podílu z odměny za vytěžený blok. Toto spojení je výhodné pro malé těžaře, kteří spojí svůj výpočetní výkon dohromady. Těžení v poolu šetří náklady

na provoz i na investici. Pooly si většinou za poskytnutí služeb berou malé procento z odměny [21].
Způsob společného těžení probíhá, tak že miner posílá své výsledky matematických úloh. Tyto vypočtené výsledky nemají žádnou hodnotu, každopádně v poolu znamenají právě vykonanou práci na potencionálním vytěženém bloku. Těmto výsledkům se říká share. Pokud miner pošle již evidovaný výsledek, tak vznikne stable share, která se do odměny nepočítá [22].

3.7 Těžební algoritmy

Kryptoměny jsou specifické, tím že používají rozdílné algoritmy pro svoji funkci. Tyto algoritmy určují, jak bude nastavena těžba těchto bloků. Z toho plyne, jak vypadá celkový blockchain

3.7.1 Ethash

Algoritmus, se kterým se těží kryptoměna Ethereum. Původně měl být ASIC rezistentní, ale v době psaní této diplomové práce se již na trhu objevily funkční ASIC, které jsou schopny tento algoritmus počítat. Samotný algoritmus je velice náročný na paměť grafických karet a vyžaduje moderní grafické karty s pamětí alespoň 3 GB. V Průběhu času neustále narůstají požadavky na tuto paměť a starší karty postupně odpadávají. Hashovací funkce je standardizována na SHA-3. Každých 30 000 bloků je generován nový DAG soubor, který zatěžuje grafické karty složitým matematickým vyobrazením a tím zvyšuje nároky na grafické karty [23].

3.7.2 CryptoNight

Algoritmus, se kterým je možné těžit kryptoměnu Monero. Tento Algoritmus je původně určený na těžbu přes procesor. CryptoNight spoléhá na náhodný přístup k pamětem a nevyžaduje náročné výpočty, jak je tomu u Ethash [24].

3.8 BitTorrent

Je to distribuční Peer-to-peer síť, která slouží ke sdílení souborů. Přes tuto síť se posílají velké objemy dat, protože se datové přenosy rozkládají mezi všechny klienty. Terminologie:

- Torrent – soubor metadat o sdílených souborech. Velikost a kontrolní součet dán hashem
- Seed – Sdílení dat, uživatel posílá potřebným data po síti
- Leech – Stahování dat, uživatel přijímá potřebná data
- Tracker – Služba pro spojení mezi klienty na základě seznamu IP

Leech stahuje data od seedera. Leech může volit pořadí data bloků. Nejprve je lepší požádat o ty méně dostupné. Leech se již během stahování mění také v seedera, pokud další leech data po síti poptává [31].

3.9 Návratnost investice

Ve výsledcích vlastní práce byl užit vzorec pro výpočet ROI. Tento pojem znamená v anglickém jazyce Return On Investment. ROI se využívá všude, kde probíhá nějaká investice a záleží na její návratnosti. Porovnáváme výši našeho zisku s výší investice pro jeho dosažení.

ROI = (výnosy – celková investice) /investice * 100

Pokud vyjde ROI menší jak 0 v procentech, tak je investice ztrátová. Pokud klesne pod -100 procent, tak je celá částka proinvestována [35].

4. Vlastní práce

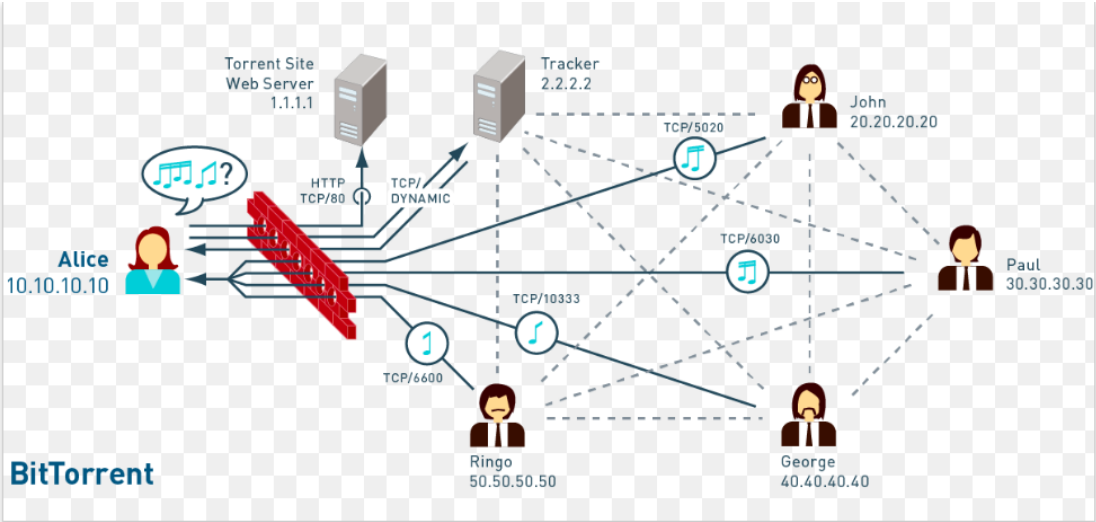
4.1 Srovnání technologií

Tato část je věnovaná porovnání již známé BitTorrent technologii, kterou porovnává s blockchainovou technologií. Mnoho lidí nechápe rozdíl mezi těmito technologiemi, a

proto je zde snaha se tento rozdíl vysvětlit. Na první pohled se může zdát, že je to úplně to stejné, ale blockchain pouze využívá některé principy Bittorentového protokolu. Funkčnost je v zásadě odlišná.

4.1.1 Bittorentová síť

BitTorrentový protokol slouží k Peer-to-peer komunikaci mezi počítači. Vytváří síť serveru, která je určená ke sdílení elektronických souboru přes internet. Pokud se chce nový účastník připojit do takové sítě potřebuje klientský program. Jeden z nejznámějších je přímo program Bittorrent. S tímto programem je možné začít sdílet a stahovat obsah na internetu takřka bez hranic. Hranice jsou pouze fyzické možnosti sítě a omezení providera.

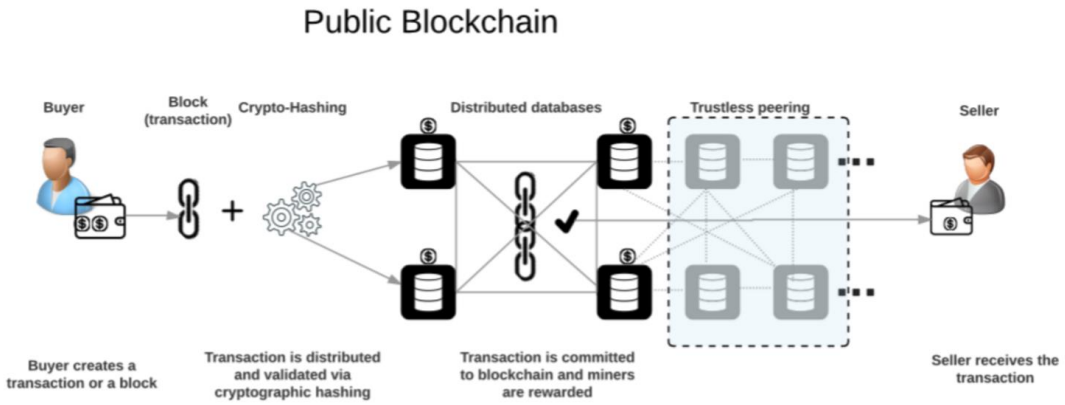


Obrázek 8 - Stahování souboru po BitTorentové síti [41]

Na obrázku nahoře je vyobrazený model torrentové sítě. Alice si zřejmě chce stáhnout písničku. Proto navštíví torrentový server, kde je možné stáhnout soubor s příponou .torrent. Soubor v sobě nese URL a kontrolní součty dat pro možné přeposílání dat. Alice soubor spustí přes svého klienta. Ten kontaktuje Tracker server, který vytváří spojení s ostatními uživateli sítě tzv. seedery. Alice se stala součástí Peer-to-per spojení. Je vidět, že v případě Bittorent protokolu se uživatelé, kteří písničku Alici posílají, chovají jako servery. Jakmile od trackeru obdrží zprávu, tak se automatický spojí s novým uzlem a začnou posílat potřebná data.

4.1.2 Blockchainová síť

V případě blockchainu je potřeba peněženka s privátním klíčem a veřejnou adresou. Tu lze vygenerovat přes náhodný generátor. Je vřele doporučeno si generátor stáhnout do počítače a privátní klíč si vygenerovat offline. Je potřeba brát v ohled i bezpečnost zařízení, kde je klíč generován. Pro získání prostředků do peněženky je nutné předat veřejný klíč odesílateli, který bude posílat prostředky do peněženky. Pro opravdovou bezpečnost se doporučuje použit adresu pouze jednou. Počet generování adres není takřka ničím omezen. Blockchain je veřejně dostupná databáze, kde lze všechny transakce zpětně dohledat.



Obrázek 9 - Ukázka posílání transakce po blockchainové síti [42]

Na výše uvedeném obrázku je ukázka celé transakce na blockchainu. Na levé straně je kupující. Ten vytváří transakci. K vytvoření transakce jsou dnes již mobilní aplikace, webová rozhraní a počítačové softwary. Transakce je podepsána privátním klíčem odesílatele. Transakce je v hashovací funkci zapsána do bloku. Jakmile se objeví v novém bloku, začne být potvrzována sítí minerů po celém světě. Prodávající může vidět odeslanou částku hned po prvním potvrzení od minera. Každopádně například většina burz či směnáren transakci připíše až po 30 potvrzeních. Je to z důvodu zabránění double-spendu. Mohlo by se totiž stát, že by se kupující pokusil se stejnou transakcí koupit zboží dvakrát. Na rozdíl od torrentové sítě nedochází mezi internetovým propojením mezi kupujícím a prodávajícím.

4.1.3 Rozdíly

Ve dvou předešlých kapitolách je vysvětleno použití každé technologie zvlášť. V zásadě během použití torrentové sítě dochází k tomu, že uživatel ze svého počítače vytvoří server, který se stane součástí Peer-to-peer sítě. V blockchainové síti uživatel pouze zašle požadavek mezi uzly minerů a procesu předávání dat se nezúčastní. Je pravda, že obě sítě posílají šifrovaná data a využívají struktury Peer-to-peer, takže z hlediska technologického jde o velice podobné technologie. Každopádně na torrentové síti si víceméně nelze zachovat anonymitu v rámci fungování posílání informací po síti. U blockchainové technologie lze do jisté míry anonymitu zaručit, pokud uživatel dodrží všechna pravidla bezpečnosti a použitý klíč od použité adresy zničí.
Dalo by se oponovat, že Alice si poslechne písničku a soubor smaže. V případě toho, kdyby některý z uzlů nebo tracker byl kompromitovaný, tak Alice prozradila svojí IP adresu, polohu, providera a to, že její počítač byl třeba jen malý okamžik členem Peer-to-peer sítě uzlů, které si navzájem sdílejí data.

4.2 Návrh sestavy výpočetní sestavy

Diplomová práce si klade za cíl navrhnou výpočetní sestavu schopnou řešit úlohy stanovené těžebními algoritmy. Pokud máme v plánu sestavit těžební sestavu, musíme si v prvé řadě uvědomit několik věcí:

- Účel těžební sestavy
- Výběr a analýza hardware
- Volba software
- Optimalizace těžby

Kryptoměny jsou velice volatilní a jejich cena se dramaticky mění během krátkých časových úseků. Přestože se investice do hardware jeví jako méně riziková než rovnou za danou investovanou částku kryptoměny nakoupit, může se stát těžba časem nevýnosná.

4.2.1 Účel těžební sestavy

Těžební sestava má za úkol nepřetržitě těžit. Měla by mít možnost přechodu na jiné měny v rámci pohybu cen jednotlivých kryptoměn. Sestavit těžební zařízení z grafických karet je vhodné zejména při následné změně účelu zařízení či jeho případném odprodeji. V tomto případě je pořízení ASIC nepřijato z důvodu jeho specializace a značným omezením co se týče využití za jiným účelem, než je těžba. ASIC se spíše hodí do firem, které se hodlají těžbou zabývat na profesionální úrovni. Jeden z účelů těžebního rigu je jeho návratnost investice. Více na toto téma v části ekonomické zhodnocení. Těžení lze brát jako hobby, kdy si člověk hraje s taktováním karet a učí se, jak funguje počítač.

4.3.1 Výběr a analýza hardware

Rozpočet je v zásadě jedna z nejdůležitějších věcí. Nejdražší položkou na těžebním stroji jsou grafické karty. Je proto důležité vybrat vhodného výrobce s ohledem na stanovené parametry. Vzhledem k situaci na trhu s grafickými kartami během stavby těžebního rigu a celkovým rozpočtem, který neměl přesahovat částku 100 000 Kč byla na výběr možnost mezi výrobci AMD a Nvidia. Jednalo se o konkurenční modely Nvidia GTX 1070Ti a AMD RX 580 8 GB. V benchmarkových hodnocení na internetu Nvidia GTX 1070Ti předčila svého konkurenta na plné čáře. Problém je v tom, že hodnocení vznikala na základě hraní her na vysoké detaily. Těžení není hraní her a grafická karta nebude sloužit k vykreslení obrazu s co možná nejrychlejším FPS. Po technické stránce parametrů jsou na tom karty dle uvedené tabulky níže

Tabulka 1 - Srovnání technických parametrů grafických karet AMD (modrá) a Nvidia (zelená), vlastní zpracování

1070 Ti	Název	RX 5080
1607 MHz	Base clock	1257 Mhz
1683 Mhz	Boost memory	1340 Mhz
8 GB	Memory	8 GB
2002 Mhz	Memory clock	2000 Mhz
256 Bit	Memory bus	256 Bit
GDDR5	Memory type	GDDR5
256.3 GB/s	Memory bandwidth	256 GB/s
2432	Shading units	2304
180W	TDP	185W
1x 8-pin	Power connerctors	1x 8-pin
11 700	Cena	6750

Tabulka ukazuje, že grafická karta od Nvidie je lepší, ale její cena je takřka dvojnásobná. Ze zkušeností jiných uživatelů s těžbou bylo řečeno, že:

RX 580 dává 24.6 MH/s a po taktování 29 MH/s

GTX 1070 dává 27 MH/s a po taktování 32 MH/s

S tím, že RX 580 má větší spotřebu a dělá větší hluk. Spotřeba bohužel uvedená nebyla [25]. Dalším faktorem při výběru byla optimalizace grafických karet. Karty společnosti Nvidia jsou vyrobeny jako plug and play, kdy stačí grafické karty pouze zapojit do sestavy a začít těžit. Naproti tomu AMD nabízí možnost flashovat BIOS, což je úprava základního firmware. Tímto způsobem lze karty upravit individuálně dle požadavků těžby. Flashování BIOS může být velice riskantní a lze tímto způsobem přijít o záruku a v horším případě karty nenávratně poškodit. Poslední skutečností je fakt, že karty Nvidia půjdou v budoucnosti spolehlivě lépe prodat díky jejich vyšší zůstatkové hodnotě.

Výsledkem těchto dat bylo rozhodnutí investovat do grafických karet od společnosti AMD z důvodu nižší pořizovací ceny. Ostatní hardware je vybrán na základě splnění požadavků těžebního software a vysokých nároků na vytížení během nepřetržitého provozu.

Zvolený typ grafické karty byl SAPPHIRE NITRO+ RX 580 8GB LIMITED EDITION, který byl o něco dražší než původní obyčejná RX 580 uvedená ve srovnání. Limitovaná

edice představovala výhodnější investici do budoucna z hlediska odprodeje. Výrobce uvádí, že tyto grafické karty dosahují vyšších výkonů a mají delší životnost.

Procesor AMD Sempron X2 2650 je dvoujádrový procesor běžící na frekvenci 1,45 GHz. Spotřeba ve specifikaci je uvedena 25 W, což byl hlavní důvod zvolení tohoto komponentu [26]. Konkurenční procesor od společnosti Intel měl větší spotřebu.

Úsporná základní deska AM1M-A s technologií 5x protection, využívající kvalitní komponenty, jako je digitální napájení DIGI + VRM zaručující správnou úroveň napětí, jednotky ESD, které chrání před elektrostatickým rušením a vydrží náročné testování, což jsou důležité vlastnosti vzhledem k tomu, že základní deska bude spuštěna několik let v nonstop provozu. Vratné pojistky kolem pozic DRAM zabraňující přepětí a poškození v případě zkratu. Samozřejmostí jsou vstupní a výstupní porty odolné vůči korozi [27].

PATRIOT FLARE 60 GB, 2,5", SSD je malý rychlý pevný disk s dostatečnou velikostí pro instalaci operačního systému a log z těžby. Podporující rozhraní SATA 6 GB/s [28].

Zdroj EVGA GQ 750 W. Poměrně výkonný zdroj od kvalitního výrobce s aktivním chlazením. Níže položená tabulka zobrazuje parametry zdroje.

Tabulka 2 - Parametry proudu, napětí a výkonu zdroje, vlastní zpracování

AC Input	100 - 240 VAC, 10A, 50 - 60 Hz				
DC Output	+3.3V	+5V	+12V	+5Vsb	-12V
MAX Output	24A	24A	62.4A 748.8W	3A	0.5A
Combined	120W		748.8W	15W	6W
Output Power	750W @ +50C				

Operační paměť Crucial 4GB DDR3L 1600MHz byla vybrána s ohledem na nižší cenu v porovnání s ostatními operačními paměti stejné velikosti také s ohledem na požadavky operačních systémů a těžebního software. Do těžební soustavy byla možnost vložit menší operační paměť, ale to by mohlo v budoucnosti přivést k nutnosti výměny za větší paměť. Vybraný model o 204 pinech je typu Dual Voltage a dokáže pracovat v režimu 1.35V.

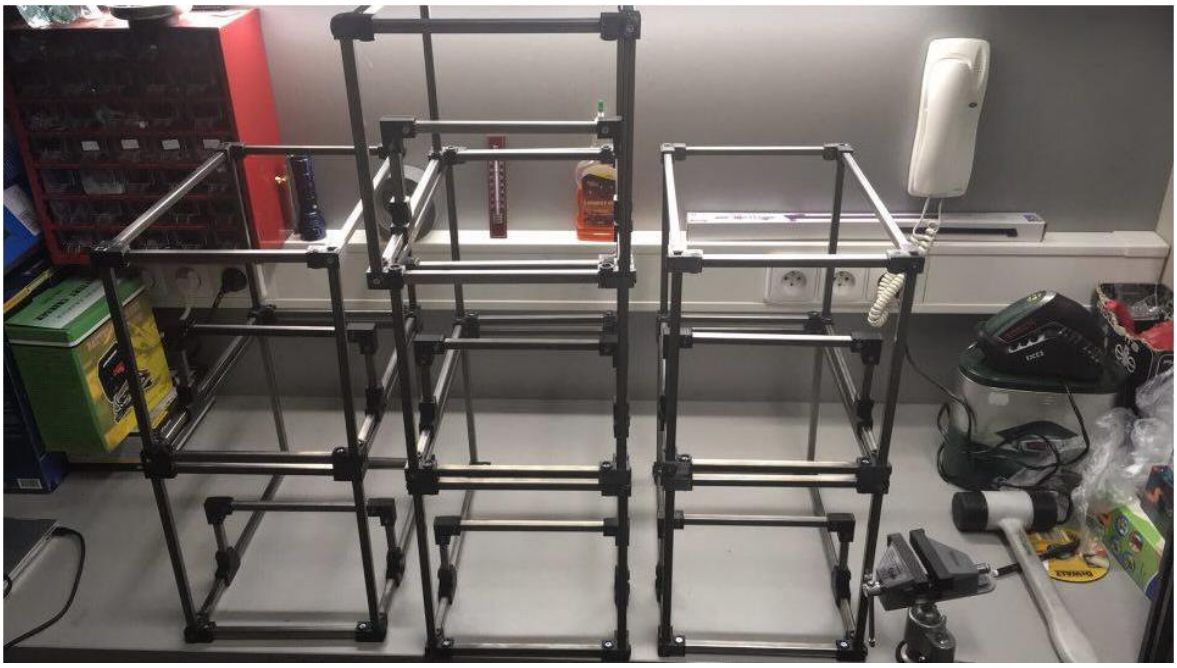
V případě, že je zařízení schopné v rozpětí tohoto napětí pracovat, dosáhneme větší úspory energie [29].

Ceny jednotlivých komponent v roce 2017 jsou představeny v tabulce níže.

Tabulka 3 - Cena komponent návrhu sestavy, vlastní zpracování

580 nitro+ 8GB	7,490
sempron	660
AM1M-A	900
EVGA GQ	2,470.00
Crucial 4GB DDR3L 1600MHz	720

Celá těžební soustava bude umístěna do ocelové konstrukce vytvořené na zakázku.



Obrázek 10 - Ukázka modulární ocelové kontrukce rigu, vlastní zpracování

Výše uvedená analýza komponent posloužila k návrhu funkčního řešení pro těžební sestavu schopnou počítat úlohy stanovenými algoritmy pro těžbu kryptoměn.

4.3.2 Volba software

Jak již bylo zmíněno v teoretické části práce, pro těžbu je možné zvolit Windows nebo Linux. V rámci co možná nejlepšího řešení byly postupně vyzkoušeny obě tyto varianty. V této časti bude vypsána pouze programová výbava pro oba typy operačních systému. Práce s těmito programy bude zahrnuta v další části *„optimalizace těžby“*.

Windows

Operační systém Windows 10 má následující minimální požadavky:
Procesor: 1 GHz
Operační paměť: 1 GB 32bit nebo 2 GB 64bit
Místo na disku: 16 GB 32bit nebo 20 GB 64bit
Lze úspěšně říci, že vybraný hardware požadavky uspokojuje více než dostatečně [30].
Další vhodný program pro přípravu těžení na Windows je ATIflash. Přes tento malý prográmek je možné flashovat. Lze jej stáhnout například na stránce https://www.guru3d.com/files-details/amd-ati-atiflash.html. Slouží ke flashování grafických karet Radeon, tudíž i zvolené RX 580.
Pro zobrazení grafických karet a sledování jejich chování je vřele doporučen program GPU-Z ke stažení zde https://www.techpowerup.com/download/gpu-z/. Je to program schopný najít grafické karty zapojené do počítače a sledovat vestavěné senzory na kartách. Během těžby je důležité sledovat tiky jádra a paměti anebo teploty a rychlost větráku. V programu je možné ověřit typy paměti - u Radeon je to Hynix nebo Samsung.
Posledním a podstatným programem je TriXX, což je alternativní varianta k známému programu MSI Afterburner. Není důležité, který program bude nakonec zvolen, jelikož oba plní stejnou funkci. Tyto programy slouží k taktovaní grafických karet. Lze v nich nastavovat tiky jádra a paměti, voltáž, limitovat napájení a určovat rychlost větráčku. Odkaz ke stažení programu TriXX https://www.techspot.com/downloads/7029-sapphire-trixx.html.
Na stránkách výrobce AMD Radeon software je pak posledním krokem možné stažení ovladačů grafických karet, které optimalizují výkon. Společnost AMD v jeden čas vydala i speciální verzi ovladačů určenou právě k těžbě.

K provozu těžební soustavy, jelikož se předpokládá také dálkový přistup, je vhodný i TeamViewer, přes který se obsluha těžebního rigu jednoduše připojí na plochu. Pro osobní užití je tento program k dispozici zdarma na oficiálních stránkách https://www.teamviewer.com.

Linux

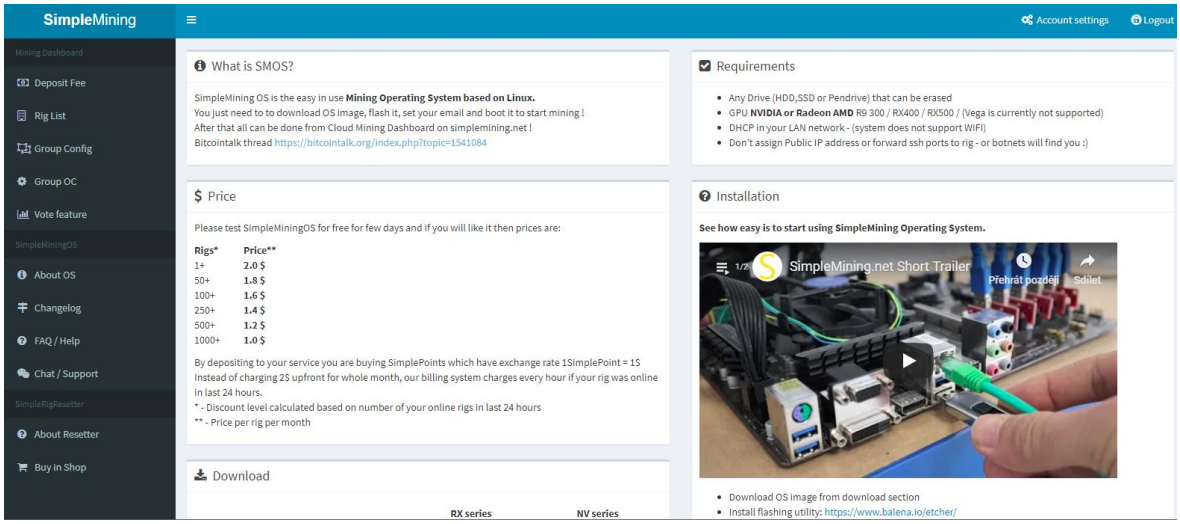
EthOS Mining OS je distribuce Linuxu vydaná specificky pouze pro těžbu kryptoměn. Minimální požadavky jsou již zmíněny v teoretické časti diplomové práce. Zde je v případě navrhované sestavy nutné pouze odpojit SSD disk s nainstalovaným Windows a zapojit USB-flashdisk s pamětí přichystanou pro podporu 64bitového systému a velikostí 8 GB. Distribuci nelze jen tak snadno nahrát na flashdisk. Je potřeba si stáhnout ISO soubor distribuce EthOS Mining OS a poté flashdisk s pomocí programu Etcher nainstalovat. Z flashdiskku se poté stane médium schopné ihned po zapojení do sestavy těžit. Odkaz na stažení Etcher 1.3.1 je zde https://www.filehorse.com/download-etcher-64/33717/. ISO soubor se objevuje v různých verzích na internetu a většinou je spojený s placenou službou. Dobrým příkladem takové placené služby je SimpleMining.

SimpleMining

Na webových stránkách https://simplemining.net/ je se možné zaregistrovat se svojí emailovou adresou a heslem. Tuto emailovou adresu je pak nutné zadat i do konfiguračního souboru, který je obsažen v nainstalovaném médiu s distribucí EthOs Mining OS. Po registraci je uživateli k dispozici webové rozhraní Simplemining. Na levé straně je k dispozici menu. Důležité položky jsou:

- Group Config
- Rig list
- Deposit Fee

Simplemining je způsob, jak za malý poplatek jednoduše obsluhovat těžební zařízení bez nutnosti se připojovat k počítači například přes SSH klienta.



Obrázek 11 - Webové rozhraní SimpleMining, vlastní zpracování

V položce Group Config List se vytvářejí těžební skupiny. Na výběr je velké množství těžebních programů včetně klasického Claymore. Podle vložených parametrů je pak možné pracovat s příkazy těžebních programů.

Po vytvoření skupiny v Group Config List je v položce Rig list vyobrazen každý rig s nainstalovanou těžební distribucí Linuxu. Zde je možné si zobrazit aktuální těžbu, optimalizovat vzdáleně těžbu, rebootovat rig nebo restartovat těžební program.

V položce Deposit Fee se platí poplatky formou kryptoměn. SimpleMinig přijímá BTC, ETH, ZEC, LTC a ETC. Poplatky za službu činí 2$ měsíčně za jednu připojenou těžební stanici. Vzorec pro výpočet poplatku je jednoduchý 2$*1/720 = 0,0027$ za hodinu.

Claymore's Dual Ethereum AMD+NVIDIA GPU Miner v12.0 (Windows/Linux)

Tento program je dostupný pro oba operační systémy. Tento program je stabilní těžební nástroj s 1% poplatkem z podílu těžby. Pro fungovaní tohoto programu je potřeba nastavit několik konfiguračních souborů. Program nabízí možnost těžení duálně, ale vzhledem k nárůstu spotřeby elektrické energie se tato možnost nevyplatí, a proto využita nebude.

Soubory, které je důležité nastavit jsou start.bat a config.txt. Soubor start.bat by měl obsahovat tyto parametry, kde se specifikuje využití grafických karet programem Claymore.

Do souboru start.bat je vloženo:

setx GPU_FORCE_64BIT_PTR 0

setx GPU_MAX_HEAP_SIZE 100

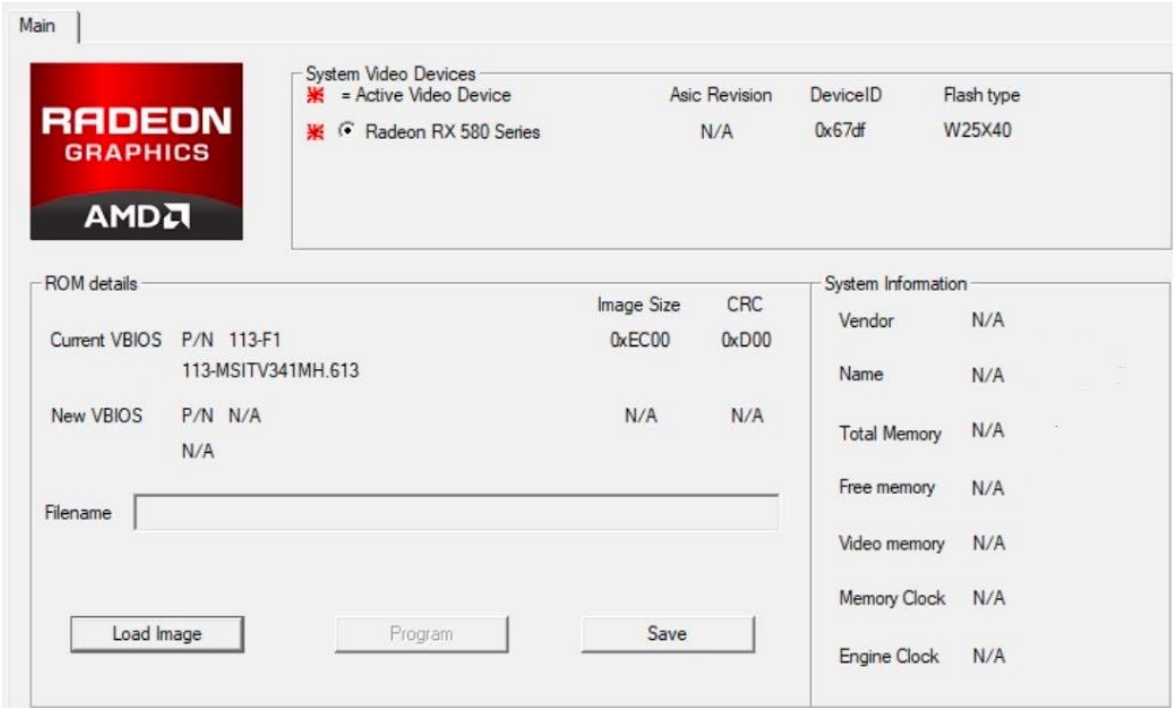
setx GPU_USE_SYNC_OBJECTS 1
setx GPU_MAX_ALLOC_PERCENT 100
setx GPU_SINGLE_ALLOC_PERCENT 100
EthDcrMiner64.exe

Tímto souborem se spouští těžba, poslední řádek příkazů spouští spustitelný program Claymore. Nastavení si program bere z textového konfiguračního souboru config.txt. Pokud je Claymore na operačním systému Windows, je doporučeno přidat soubor start.bat do složky po spuštění. To má za následek, že se vždy po rebootu zařízení těžba automaticky spustí.
Zbývá už jen nastavit konfigurační soubor config.txt. Do konfigurace je možné zadat velké množství parametrů, včetně přímé optimalizace přes těžební program. V této části jsou zadány pouze nezbytné parametry pro těžbu.
V souboru config.txt jsou přednastaveny následující parametry:
#-epool us1.ethpool.org:3333
#-ewal 0xD69af2A796A737A103F12d2f0BCC563a13900E6F
#-epsw x

První řádek s příkazem -epool xx.xxx.xx:xxxx je adresa poolu, kde bude miner posílat své výpočty.
-ewal je adresa kam pool bude posílat odměny za vypočtené výpočty. -epsw x defaultně je nastavené heslo na x, ale může se lišit podle pravidel poolu. Některé pooly vyžadují registraci a heslo.

4.3.3 Optimalizace těžby

Poslední částí návrhu výpočetní sestavy je její optimalizace. Předpoklady pro optimalizaci jsou splněny. Sestava je funkční a potřebný software nainstalovaný. Nastává tedy otázka, jak získat co možná nejlepší možný výkon z grafických karet. Optimalizace proběhne na operačním systému Windows v několika krocích.
Změna BIOS na grafických kartách pomocí programu ATIflash.



Obrázek 12 - Prostředí aplikace ATIflash, vlastní zpracování

Úprava BIOS je z hlediska optimalizace velmi výhodná, protože v některých případech zvedne výkon až o 10 % a sníží spotřebu. Ideální je vytvořit si svůj vlastní BIOS v programu PolarisBiosEditor, ale jak bylo zmíněno (viz. 4.3.1 Výběr a analýza hardware), je doporučeno si vybrat některý z volně dostupných souborů, doporučovaných v internetových diskuzích, kde si mineři tyto již odzkoušené BIOS soubory navzájem sdílejí. Výborná stránka týkající se této tématiky je https://1stminingrig.com/. Předtím než je BIOS flashováním změněn je dobré si udělat zálohu originálního BIOS. Grafická karta uvedená v této diplomové práci má na straně speciální tlačítko, které vrací změny BIOS do původního nastavení. Teoreticky je tak možné mít dvě místa pro zkoušení změn v nastavení BIOS. Původní nastavení lze totiž také přepsat. Mít originální verzi BIOSU je důležité z hlediska záruky. Kdyby nastala situace, že grafická karta přestane fungovat, je možné, že se výrobce odvolá na vlastní úpravy BIOS.

Práce v programu ATIflash je snadná. Víceméně stačí dvě tlačítka zobrazená na viz obrázek č. 12. Load Image a Save. Těmi se nahrávají a přepisují soubory BIOS. Přepisování chvíli trvá a po přepsání BIOS je nutné počítač vždy restartovat. Pro každou kartu je tento krok nutný udělat zvlášť. Soubor zabírá pár bytů a má příponu .rom.

Součástí optimalizace je taktování. Taktování je zdlouhavý proces, kdy uživatel postupně mění parametry pomocí zmíněných programů. Spočívá v nastavování 3 parametrů:

- Core clock
- Memory clock
- Voltage

Popřípadě je možné uvést ještě rychlost otáčení větráčku. Každá karta má svoje ideální individuální nastavení, které je závislé od toho, jak se výrobcům karta kvalitně povedla vyrobit. Ačkoliv se to může zdát nepravdivé, neexistují 2 identické karty. Vlivů na výkon a stabilitu karet je celá řada, obzvlášť pokud jsou maximálně vytíženy. Těžební soustavu je nutné testovat celé týdny, než je možné s určitostí říci, že je optimalizována.

Obrázek 13 - Prostředí aplikace TriXX, vlastní zpracování

Nainstalované nejnovější ovladače jsou samozřejmostí. Ty lze vyhledat přímo na stránkách výrobce. Nyní, když je těžební soustava otestována je potřeba neopomenout prostředí. Grafické karty vytvářejí skutečně velké množství odpadního tepla. Pokud větráky na

grafických kartách nezvládají teplý vzduch odvětrávat, klesá jejich výkon, a pokud se dokonce přehřejí, těžební soustava se vypne. Grafiky by měly být v sestavě nastaveny jedním směrem a mít mezi sebou dostatečnou mezeru, aby větráky přes svého souseda odvětrávaly teplo – viz obrázek č. 14. V krajních případech může dojít i k požáru. Karty mívají bez adekvátní cirkulace vzduchu během letních dnů těžení i 80 stupňů celsia, a to nepřetržitě.

Obrázek 14 - Mezery mezi grafickými kartami 2 cm, vlastní zpracování

Pokud jsou výše uvedené věci vykonány, zbývá nastavit výsledky taktování do programu Claymore. Stačí přidat své výsledky do textového konfiguračního souboru (viz. 4.3.2 Volba software) -cclock 1411 -mclock 2000 -cvddc 1000 -mvddc 1000

- Cclock je core clock
- Mclock je memory lock
- Cvddc je core voltáž
- Mvddc je memory voltáž

Voltáže pro jádro i paměť jsou většinou stejné.

4.3 Analýza kryptoměn a ekonomické hodnocení

V následující analýze budou postupně rozebrány 3 měny, které jsou vhodné pro těžbu. Tržní data budou vycházet z veřejných dat z web http://www.coinmarketcap.co. Porovnání cen bude vůči dolaru (USD). Ceny se velice dynamicky mění každým dnem. Uvedené ceny jsou aktuální k časovému intervalu od 25.4.2017 do 20.3.2019. V době psaní této práce využívají všechny tyto kryptoměny koncept Proof of Work.

Monero (XMR)

Tabulka 4 - Základní údaje o Moneru, vlastní zpracování

Tržní kapitalizace:	$ 942 482 083
Cena:	$ 56,74
Celkové množství:	16 876 847
Objem obchodu za 24h:	$ 102 750 635

Obrázek 15 - Graf vývoje ceny Monera [43]

Monero má sloužit jako digitální platidlo v moderním světě. K posílaní transakcí není třeba prostředníka. Ze všeho nejvíc klade Monero důraz na anonymitu a není údajně možné vystopovat transakce [32].

Zcash (ZEC)

Tabulka 5 - Základní údaje o Zcash, vlastní zpracování

Tržní kapitalizace:	$ 363 276 368
Cena:	$ 61,67
Celkové množství:	6 175 219
Objem obchodu za 24h:	$ 254 732 439

Obrázek 16 - Graf vývoje ceny Zcash [44]

Zcash je velice podobné nejvýznamnější digitální kryptoměně Bitcoin. Jeho blockchain vznikl právě na Bitcoinu. Zcash údajně kryje částku asociovanou k určité adrese se speciální funkcí, která dovolí určitým stranám transakční detaily vidět [33].

Ethereum (ETH)

Tabulka 6 - Základní údaje o Ethereum, vlastní zpracování

Tržní kapitalizace:	$ 14 817 151 375
Cena:	$ 140,95
Celkové množství:	105 389 015
Objem obchodu za 24h:	$ 4 664 134 462

Obrázek 17 - Graf vývoje ceny Ethereum [45]

Ethereum je decentralizovaná platforma pro vytváření smart kontraktů. Smart kontrakt může emitovat nové tokeny podle svých vlastních pravidel. Tyto tokeny je možné používat jako novou kryptoměnu, která bude zaznamenána v ETH blockchainu [34].

S ohledem na tržní kapitalizaci, emitované množství a novému přístupu k využití kryptoměn byla vybrána jako vhodná digitální měna pro těžbu Ethereum.

5. Výsledky a diskuse

S ohledem na vybrané komponenty ve vlastní části byly sestaveny 2 stejné těžební sestavy. Každá z nich osazena 3 grafickými kartami. Celkově investovaná částka včetně DPH bez práce a ocelové konstrukce včetně kabelů, zdrojů napájení, síťového kabelu a riserů je zobrazena v následující tabulce.

Tabulka 7 - Celková investice do těžební soustavy, vlastní zpracování

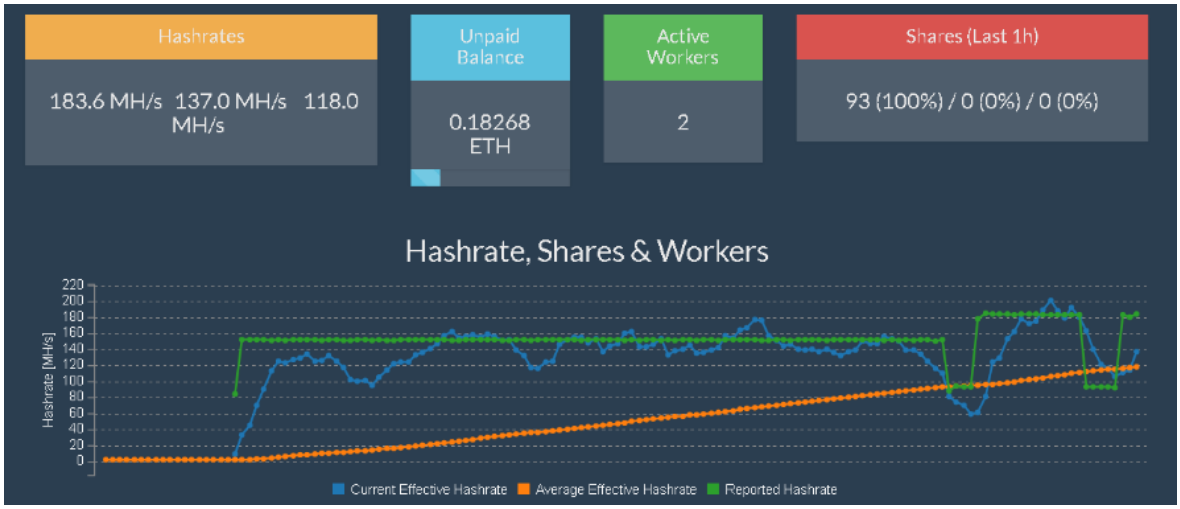
6x	580 nitro+ 8GB	7,490
2x	sempron	660
2x	AM1M-A	900
2x	EVGA GQ	2,470.00
2x	Crucial 4GB DDR3L 1600MHz	720
Suma		54,440

- Cenový tarif za elektřinu je 2,5 Kč včetně DPH
- Těžená kryptoměna Ethereum
- Celková doba těžby 1-2 roky
- Pooly: Ethermine a Dwarfpool

Dále je řešena optimalizace vlastního řešení včetně testování. V závěru výsledků dojde na ekonomické zhodnocení investice.

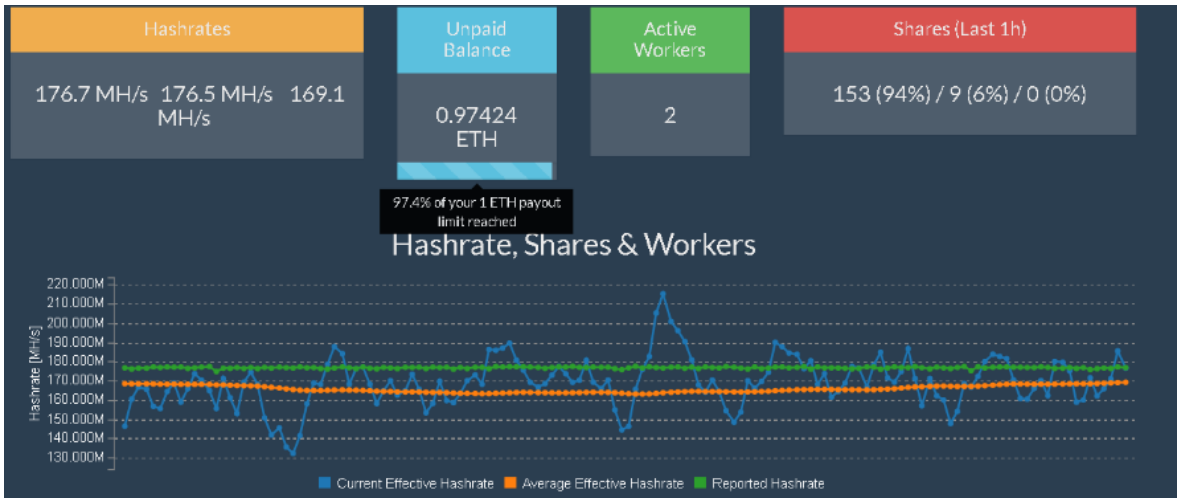
5.1 Optimalizace, testování

Na úvod je vhodné uvést, že to nejsou 2 roky nepřetržité těžby. Během těžení docházelo k častým výpadkům. Těžební soustava byla z počátku dost nestabilní. Výhodou bylo, že testování bylo urychleno možností testovat těžbu na dvojici těžebních soustav zároveň. Rigy pracovaly na Windows, kde byly testovány vhodné parametry (core clock, memory clock a voltáže).



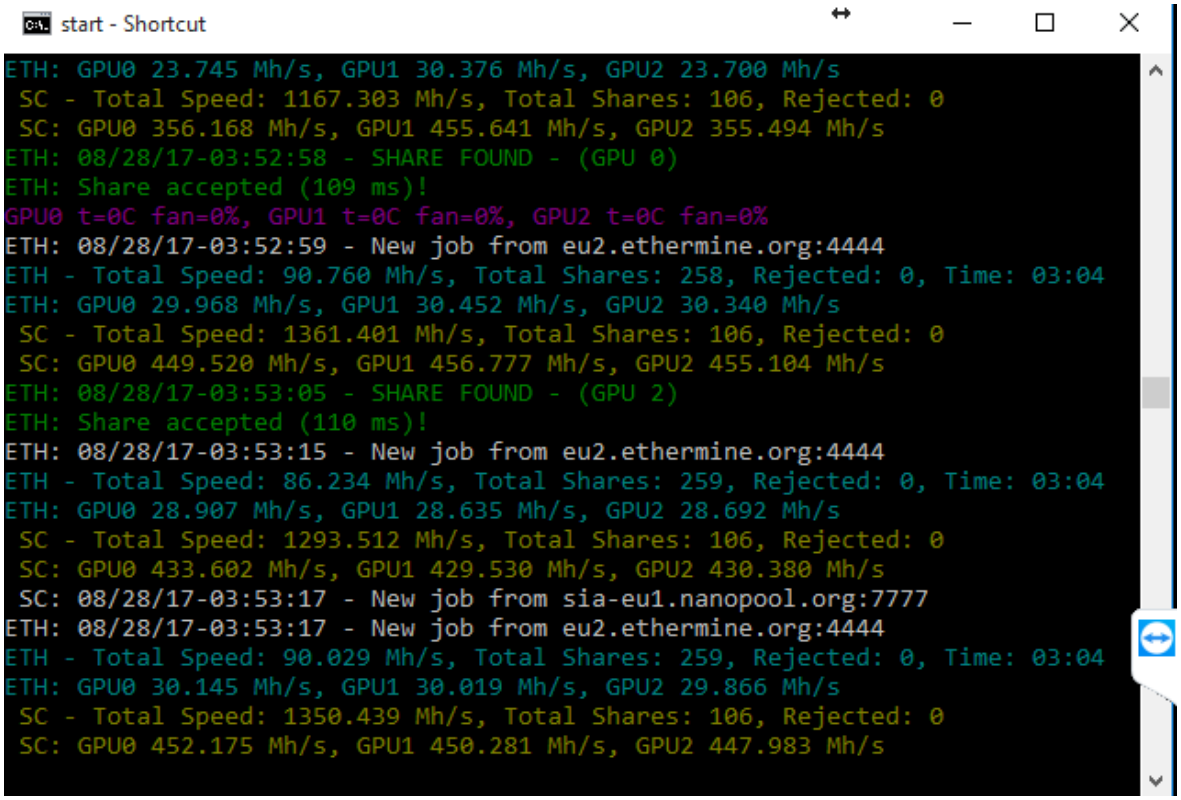
Obrázek 18 - Nestabilní těžba na poolu Ethermine, vlastní zpracování

Na obrázku na poolu Ehtermine jsou vidět výpadky a také, že soustava byla nestabilní. Důvodem výpadků byla snaha o dosažení co možná nejlepšího výkonu .



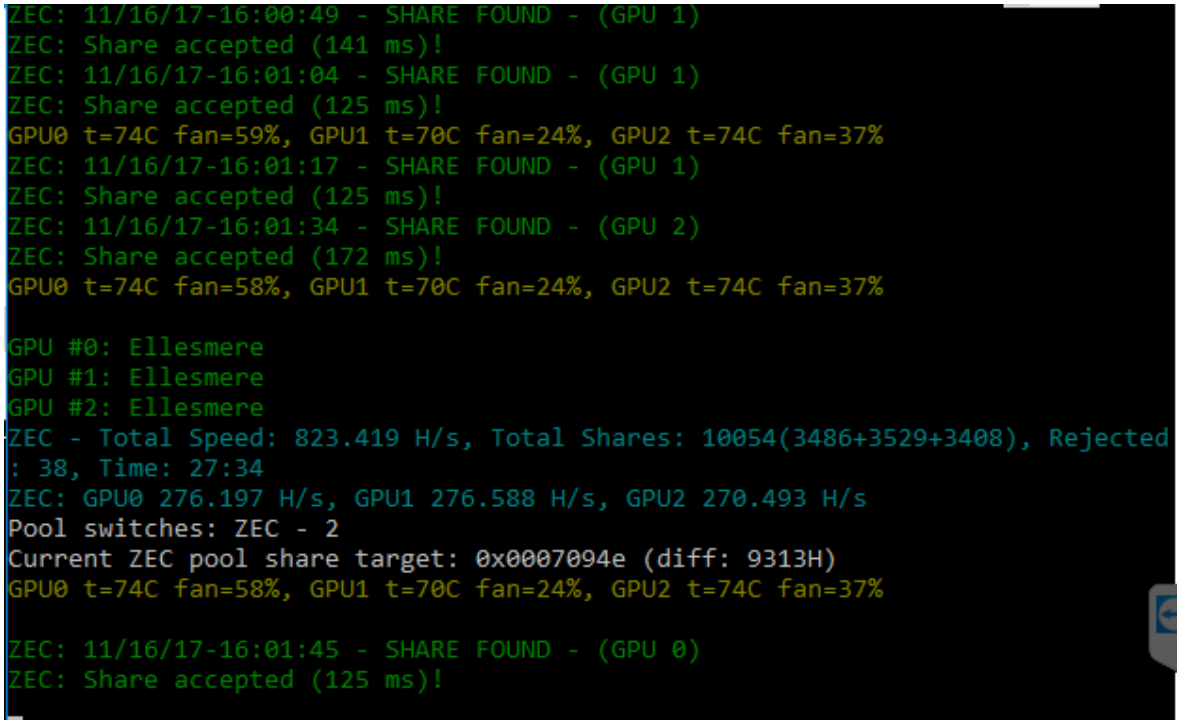
Obrázek 19 - Stabilní těžba na poolu Ethermine, vlastní zpracování

Na obrázku je vidět, že snížení parametrů mělo za následek vyšší stabilitu za cenu nižší odměny.



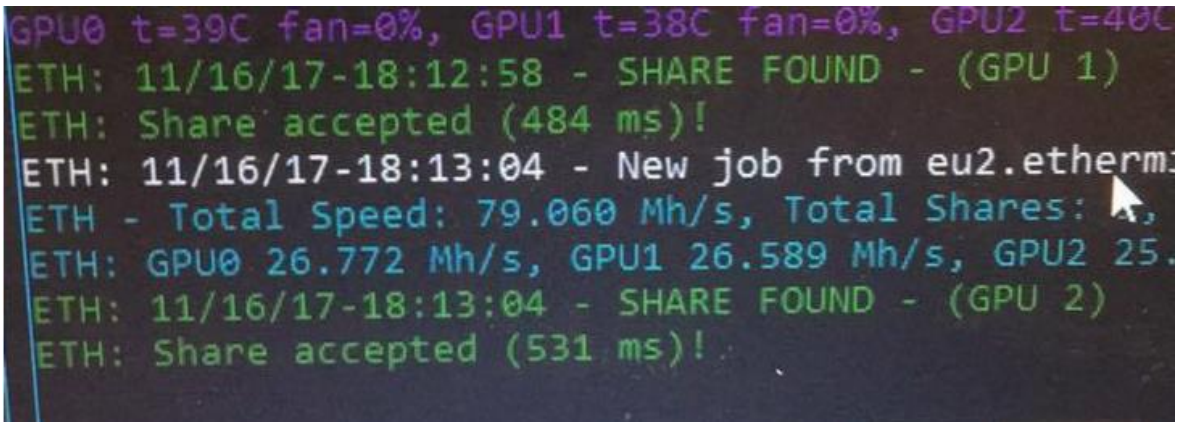
Obrázek 20 - Duální těžba ETH a SIA, vlastní zpracování

Dualní těžba byla dost nestabilní a spotřebovala dost energie. Rig se většinou po pár hodinách zasekl. Navíc většinu kryptoměn, které nabízely možnost duálně těžit drtivě ovládly specializované ASIC.



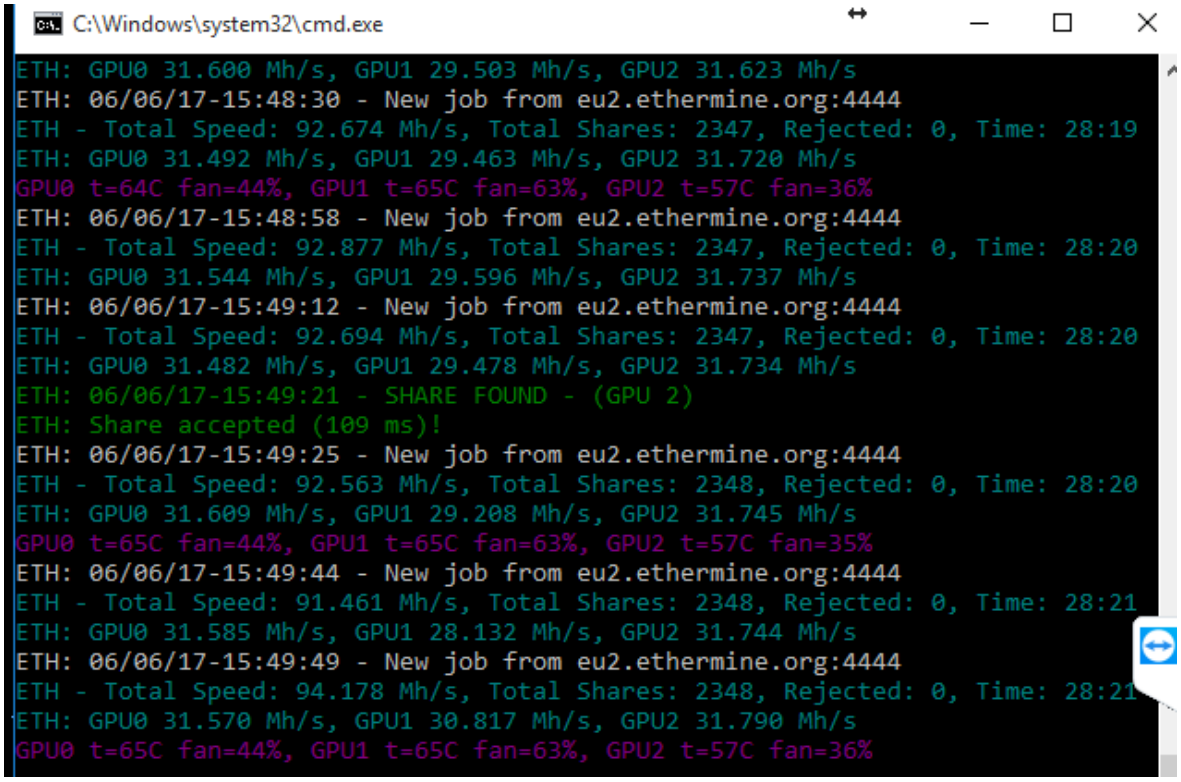
Obrázek 21 - Těžba ZEC, vlastní zpracování

Dále byla na těžební soustavě vyzkoušena těžba kryptoměny Zcash. Výsledky těžby potvrdily fakt, že je výhodnější těžit Ethereum. Těžba Zcash je možná i na méně výkonných grafických kartách.



Obrázek 22 - Těžba ETH bez taktování, vlastní zpracování

Původně karty bez nastavených parametrů taktů a voltáží dodávaly výkon okolo 26 MH/z s velmi vysokou spotřebou okolo 200 W. Taktování AMD karet se ukázalo jako nezbytné.

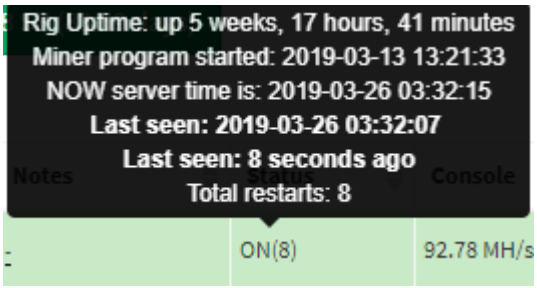


Obrázek 23 - Těžba ETH s taktováním, vlastní zpracování

Se správnými parametry grafické karty dokázaly předvést vyšší výkon až o 20 %.

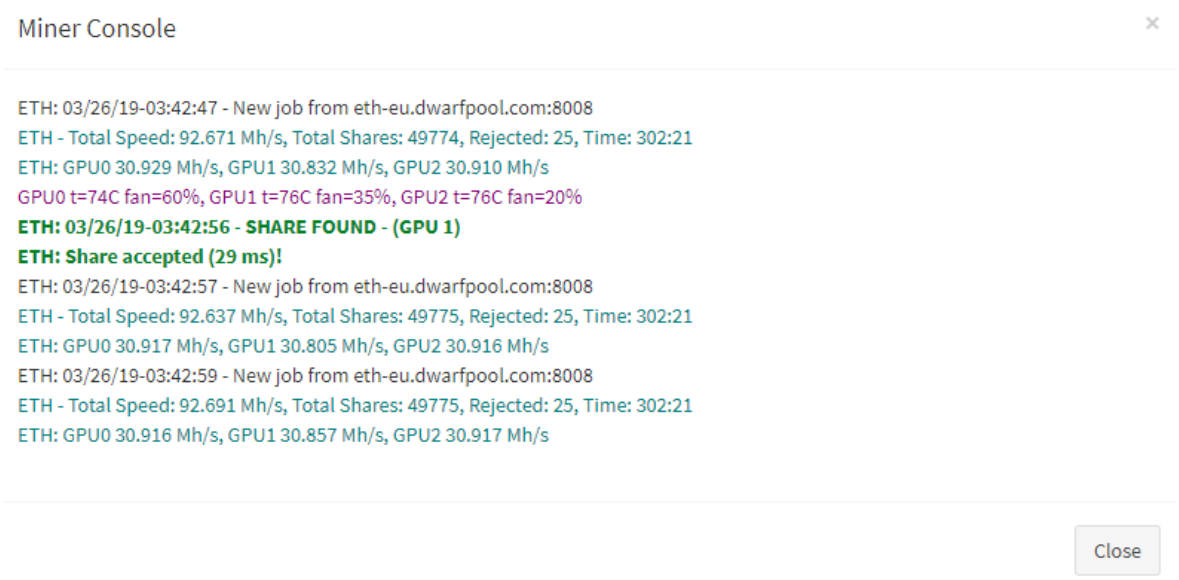
Bez duální těžby přestaly rigy padat a začaly těžit stabilně.

Poté začaly dělat problémy samotné Windows. Příkladem jsou různé systémové aktualizace a neustálá potřeba těžbu občas zastavovat kvůli promazání log souboru. Během expirace licence Windows bylo rozhodnuto přejít na službu Simplemining, která slibovala bezstarostnou obsluhu.



Obrázek 24 - Ukázka stabilní 5týdenní těžby přes službu SimpleMining, vlastní zpracování

Výsledkem je stabilní těžba, která vydrží běžet bez problémů klidně i 5 týdnů.



Obrázek 25 - Ukázka stabilní těžby ETH po přechodu na SimpleMining, vlastní zpracování

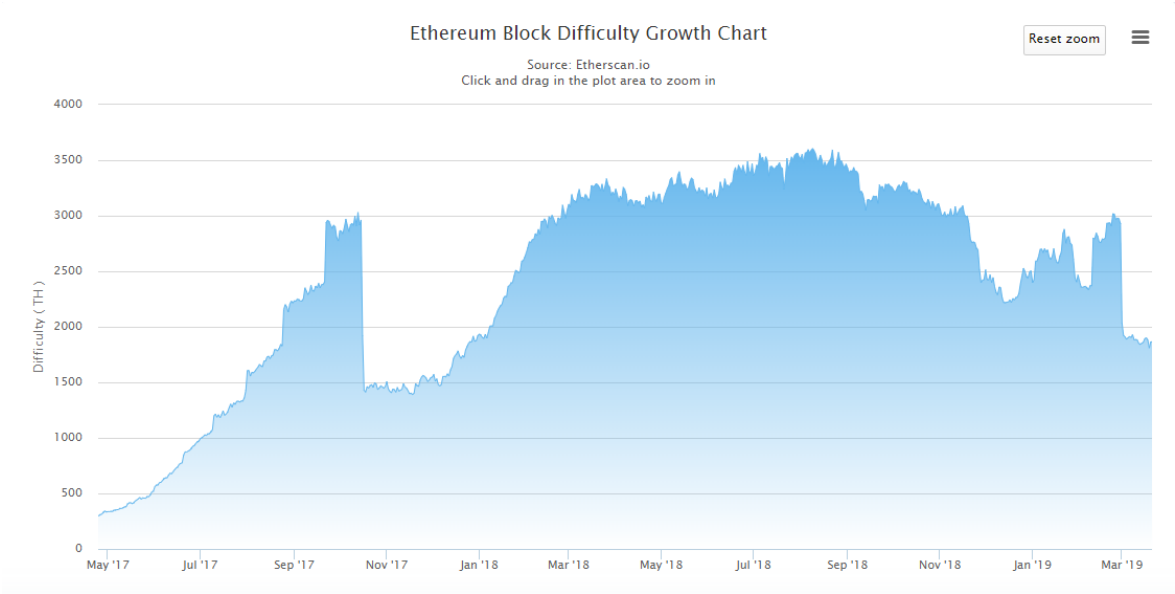
S příchodem na Simplemining proběhla i změna poolu na Dwarfpool. Poplatky jsou stejné. Závěrečné optimalizované nastavení je tedy:

- Core MHz: 1200
- Memory MHz: 2200
- Undervolt: 950

Toto nastavení běží stabilně na 6 kartách sapphire nitro+ rx 580 8GB limited edition s upraveným BIOS od společnosti AMD.

5.2 Návratnost investice

Ethereum v průběhy těžby snižovalo odměny za vytěžený blok. Zvyšovala se i obtížnost těžby s přibývajícím počtem minerů. V roce 2017 přišla „Ice Age“, kdy byla snížena odměna z 5 ETH za blok na 3 ETH. V roce 2018 nastalo další snížení odměny z 3 ETH na 2 ETH za jeden blok, které je aktuální v době psaní diplomové práce. Snižování odměn je příprava na změnu konceptu Proof of Work na Proof of Stake (viz. kapitola 3.6 Těžba kryptoměn).



Obrázek 26 - Reakce minerů na snížení odměny [46]

5.2.1 Zhodnocení těžby

Uvedená číselná data a statistiky pocházejí z reálných dat z těžby kryptoměny Ehereum.

- Průměrný hashrate dosahuje až 210 MH/z
- Jedna karta spotřebuje zhruba 170 W/h
- Přímý odběr ze zásuvky činní 1100 W/h
- Cenový tarif je 2,5 Kč za Kw/h včetně DPH
- Těžba trvala přibližně 650 dnů (včetně dnů mimo provoz)
- Celkově se vytěžilo 14.48217146 Ethereum s odečtenými poplatky poolu a těžebního programu.

Ve výsledných nákladech nejsou započítány výpadky těžby.

1100 W = 1,1 KW

Rigy běží nonstop tudíž:

1,1 * 24 * 2,5 = 66 Kč za den

Náklady na elektřinu činní

66 * 365 = 24 090 Kč za jeden rok.

Celkové náklady na elektřinu činí:

66 * 650 = 42 900 Kč

Návratnost investice s taktikou Holding.

Miner kryptoměnu shromažďuje a čeká na lepší cenu. Návratnost je vypočítaná jako celková hodnota vytěžených kryptoměn.

Cena Ehereum ke dni 20.3.2018 činí 3172 Kč. Hodnota držené kryptoměny je tedy:

14,5 * 3172 = 45 994 Kč.

Po odečtení nákladů z těžby:

45 994 - 42 900 = 3094 Kč

Z uvedené částky je patrné, že těžba ztrátová nebyla za předpokladu, že je kryptoměna stále držena.

Výpočet ROI (návratnost investice):

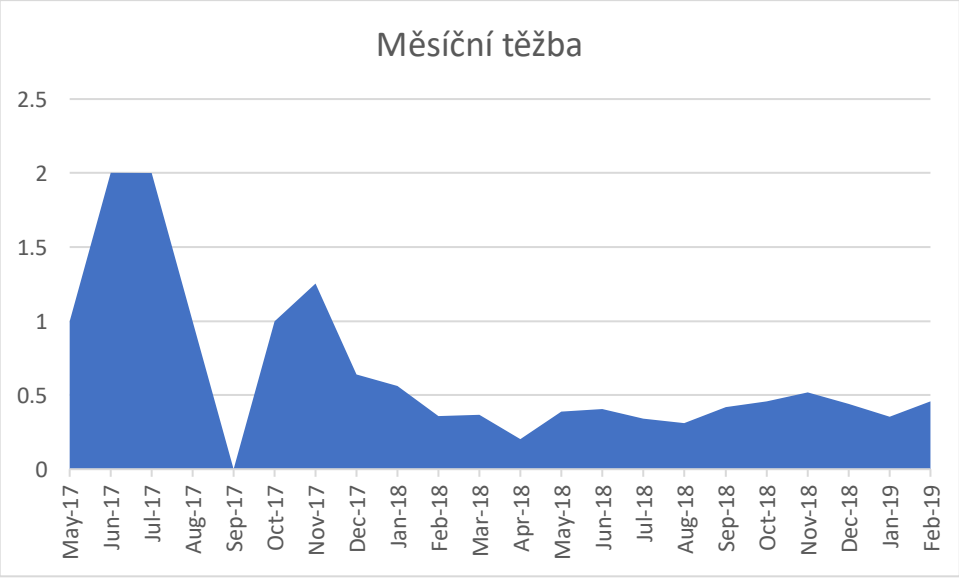
ROI = (výnosy – celková investice) /investice * 100

ROI = 3009/54440 * 100

ROI = -94,3 %

Výsledek znamená, že se investice splatila pouze z necelých 6 % za necelé dva roky.

Je možné konstatovat, že taktika holdingu během těžby sice není ztrátová, ale z pohledu investice výhodná není.

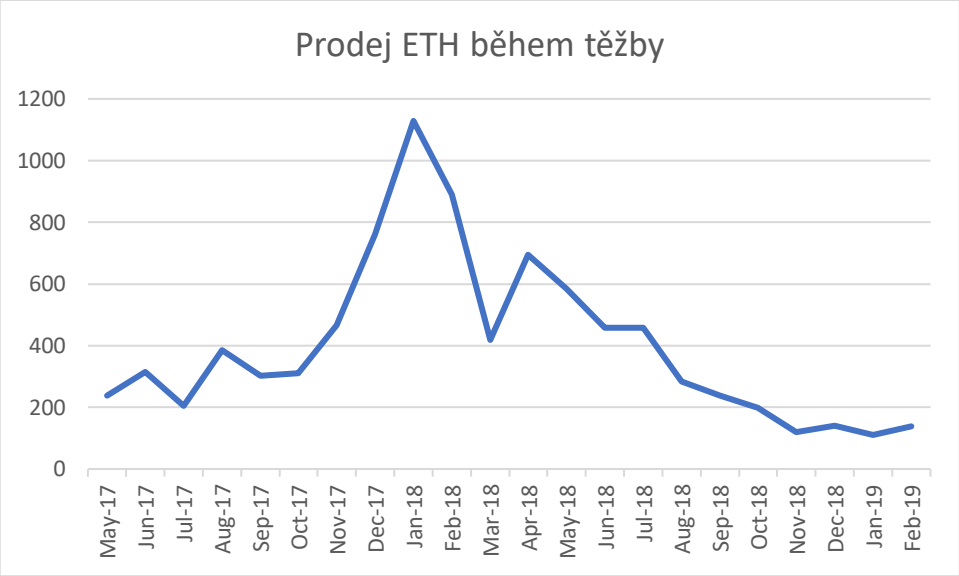


Obrázek 27 - Graf přijatých ETH z těžby, vlastní zpracování (viz. Příloha)

Na obrázku je vidět, že jeden měsíc těžební rigy netěžily ETH. Je zde vidět i snižování odměn. Výkon grafických karet se příliš neměnil.

Návratnost investice s měsíčním prodejem.

Miner prodává vytěženou kryptoměnu na konci měsíce.



Obrázek 28 - Graf měsíčního prodeje ETH z těžby, vlastní zpracování (viz. Příloha)

Celkově bylo uskutečněno 22 prodejů v celkové hodnotě 120 701 Kč.

Po odečtení nákladu z těžby:

120 701 - 42 900 = 77 801 Kč

Z uvedené částky je patrné, že tato strategie pokrývá náklady na těžbu i samotnou investici.

Výpočet ROI (návratnost investice):

ROI = (výnosy – celková investice) /investice * 100

ROI = 23361/54440 * 100

ROI = 42,9 %

Výsledek znamená, že se investice měla zhodnocení 42 % za necelé dva roky.

Je možné konstatovat, že tato taktika byla velice zisková a z pohledu investice výhodná.

Je nutné podoktnout, že těžební soustava je schopná pokračovat v těžbě.

Závěr

Diplomová práce si kladla za hlavní cíl návrh optimalizované sestavy hardwarových komponentů určených pro zpracování výpočetních úloh stanovenými algoritmy pro těžbu kryptoměn. K tomuto účelu byly v teoretické části popsané pojmy a technologické principy nezbytné k pochopení dané tématiky. V části vlastní práce byla po analýze komponent vytvořena vlastní sestava. Na tuto sestavu byl implementován software s potřebným nastavením, aby daná těžební sestava byla schopna těžby. Tato sestava se prokázala jako funkční a efektivní nástroj k těžbě. V části výsledků a diskuze je možné vidět výsledky z optimalizace hardwaru a následné těžby.

Jedním z dílčích cílů bylo řešení ekonomicky zhodnotit s ohledem na návratnost investice. Z výsledku tohoto zhodnocení je patrné, že použitím taktiky měsíčního prodeje z příjmů kryptoměn se již investice vrátila a zhodnotila.

Dalším dílčím cílem bylo srovnání blockchainové technologie s již běžně využívanou technologií. Toto srovnání proběhlo formou uvedením těchto technologií do praxe. Výsledkem bylo zjištěno, že technologie mají v některých bodech podobné principy, jako je například Peer-to-peer struktura sítě, ale v zásadě se liší jejich funkčnosti a použití.

Tematicky diplomová práce splnila všechny stanovené cíle. Práce proběhla na reálných datech a s uvedením navržené sestavy do provozu. V souvislosti na toto téma je důležité zmínit, s přihlédnutím k analýze kryptoměn a vzhledem k současným cenám za elektřinu, že se z krátkodobého hlediska těžit nevyplatí. Výhledově je doporučeno investovat do komponent schopných těžby alespoň 5 let s ohledem na budoucí náklady s těžbou spojené.

Seznam použitých zdrojů

[1] Základní komponenty počítače. *Informační systém Masarykovy univerzity* [online]. [cit. 2019-03-14]. Dostupné z: https://is.muni.cz/do/med/el/vt/um/txt/zakladni_komponenty.html

[2] Vše, co jste chtěli vědět o SSD | Svět hardware. *Svět hardware* [online]. [cit. 2019-03-14]. Dostupné z: https://www.svethardware.cz/vse-co-jste-chteli-vedet-o-ssd/26524

[3] ExplainingComputers.com: Hardware. *ExplainingComputers.com by Christopher Barnatt* [online]. [cit. 2019-03-14]. Dostupné z: https://www.explainingcomputers.com/hardware.html

[4] What Is an ASIC miner? | Digital Trends. *Technology News, Product Reviews, Deals & How-To's* [online]. [cit. 2019-03-16]. Dostupné z: https://www.digitaltrends.com/computing/what-is-an-asic-miner/

[5] EthOS Mining OS. *EthOS Mining OS* [online]. [cit. 2019-03-16]. Dostupné z: http://ethosdistro.com/

[6] PŘISPĚVATELÉ FÓRA. Claymore's Dual Ethereum AMD+NVIDIA GPU Miner v12.0 (Windows/Linux). *Bitcoin Forum* [online]. [cit. 2019-03-16]. Dostupné z: https://bitcointalk.org/index.php?topic=1433925.0

[7] WikiLeaks bypasses donations boycott | CBC News. *CBC News* [online]. [cit. 2019-03-16]. Dostupné z: https://www.cbc.ca/news/technology/wikileaks-bypasses-donations-boycott-1.1170719

[8] Silk Road 1: Theory & Practice - Gwern.net. *Essays - Gwern.net* [online]. [cit. 2019-03-16]. Dostupné z: https://www.gwern.net/Silk-Road

[9] What is Cryptocurrency: Cryptocurrency Explained the Easy Way. *Bitdegree* [online]. [cit. 2019-03-16]. Dostupné z: https://www.bitdegree.org/tutorials/what-is-cryptocurrency/#Crypto

[10] PŘISPĚVATELÉ WIKIPEDIE. Cryptography. In: *Wikipedia, the Free Encyclopedia* [online]. [cit. 2019-03-16]. Dostupné z: http://en.wikipedia.org/wiki/Cryptographic_hash_function

[11] Symetrická kryptografie – Wikisofia. *Wikisofia* [online]. [cit. 2019-03-16]. Dostupné z: https://wikisofia.cz/index.php/Symetrick%C3%A1_kryptografie

[12] Asymetrická kryptografie. *Univerzitní informační systém MENDELU* [online]. [cit. 2019-03-16]. Dostupné z: https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=7027

[13] Block chain - Bitcoin Wiki. *Bitcoin Wiki* [online]. [cit. 2019-03-17]. Dostupné z: https://en.bitcoin.it/wiki/Block_chain

[14] Address - Bitcoin Wiki. *Bitcoin Wiki* [online]. [cit. 2019-03-17]. Dostupné z: https://en.bitcoin.it/wiki/Address

[15] NAKAMOTO, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System – Satoshi Nakamoto* [online]. [cit. 2019-03-24]. Dostupné z: http://bitcoins.info/bitcoin.pdf

[16] Block - Bitcoin Wiki. *Bitcoin Wiki* [online]. [cit. 2019-03-17]. Dostupné z: https://en.bitcoin.it/wiki/Block

[17] BLACK, Adam. *Hashcash - A Denial of Service Counter-Measure.* [Online]. [cit. 2019-03-17] http://www.hashcash.org/papers/hashcash.pdf

[18] HURŤÁK, Petr. *Analýza virtuální měny Bitcoin* [online]. [cit. 2019-03-17]. Bakalářská práce. Dostupné z: http://www.vse.cz/vskp/show_file.php?soubor_id=1244711

[19] How to Calculate Bitcoin Transaction Fees When You're in a Hurry - Bitcoin News. *News - Bitcoin News* [online]. [cit. 2019-03-24]. Dostupné z: https://news.bitcoin.com/how-to-calculate-bitcoin-transaction-fees-when-youre-in-a-hurry/

[20] Mining Difficulty and Network Hashrate Explained - Crypto Mining Blog. *2Miners - Altcoin Cryptocurrency Mining Pools PPLNS & SOLO*[online]. [cit. 2019-03-1]. Dostupné z: https://2miners.com/blog/mining-difficulty-and-network-hashrate-explained/

[21] Mining Pools and How They Work | CryptoCompare.com. *CryptoCompare.com - Live cryptocurrency prices, trades, volumes, forums, wallets, mining equipment, and reviews | CryptoCompare.com* [online]. [cit. 2019-03-17]. Dostupné z: https://www.cryptocompare.com/mining/guides/mining-pools-and-how-they-work/

[22] Breakdown: Mining Pools - Mycryptopedia. *Mycryptopedia - Learn About Cryptocurrency & Blockchain Technology* [online]. [cit. 2019-03-17]. Dostupné z: https://www.mycryptopedia.com/breakdown-mining-pools/

[23] White Paper · ethereum/wiki Wiki. *Github* [online]. [cit. 2019-03-18]. Dostupné z: https://github.com/ethereum/wiki/wiki/White-Paper

[24] CryptoNight - Bitcoin Wiki. *Bitcoin Wiki* [online]. [cit. 2019-03-18]. Dostupné z: https://en.bitcoin.it/wiki/CryptoNight

[25] How does the RX 580 compare to the GTX 1070 Ti for mining? - Quora. *Home - Quora* [online]. [cit. 2019-03-18]. Dostupné z: https://www.quora.com/How-does-the-RX-580-compare-to-the-GTX-1070-Ti-for-mining

[26] AMD Sempron X2 2650 - Procesor | Alza.cz. *Alza.cz - největší obchod s počítači a elektronikou | Alza.cz* [online]. [cit. 2019-03-18]. Dostupné z: https://www.alza.cz/amd-sempron-x2-2650-d931611.htm

[27] AM1M-A | Základní desky | ASUS Česká republika. *ASUS Česká republika* [online]. [cit. 2019-03-18]. Dostupné z: https://www.asus.com/cz/Motherboards/AM1MA/

[28] PATRIOT FLARE 60GB, 2,5", SSD, PFL60GS25SSDR alternativy - Heureka.cz. *Heureka.cz* [online]. [cit. 2019-03-18]. Dostupné z: https://pevne-disky.heureka.cz/patriot-flare-60GB-2_5-ssd-pfl60gs25ssdr/

[29] Crucial 4GB DDR3 1600 SO-DIMM CT51264BF160BJ | CZC.cz. *CZC.cz* [online]. [cit. 2019-03-18]. Dostupné z: https://www.czc.cz/crucial-4GB-ddr3-1600-so-dimm_2/120708/produkt?gclid=CjwKCAjw-OHkBRBkEiwAoOZql0zR40MFXbMXLMP1WBT_vXiLj65GsnakquQ_FA7eKhICCYfVx-mhdBoCkGIQAvD_BwE

[30] Jak zkontrolovat specifikace a požadavky na systém počítače s Windows 10 — Microsoft. *Oficiální domovská stránka Microsoft* [online]. [cit. 2019-03-18]. Dostupné z: https://www.microsoft.com/cs-cz/windows/windows-10-specifications

[31] BitTorrent - Technologie. *Root.cz - informace nejen ze světa Linuxu* [online]. [cit. 2019-03-24]. Dostupné z: https://www.root.cz/clanky/bittorrent-technologie/

[32] Home | Monero - secure, private, untraceable. *Monero* [online]. [cit. 2019-03-20]. Dostupné z: https://www.getmonero.org/

[33] Privacy-protecting digital currency | Zcash. *The Basics | Zcash* [online]. [cit. 2019-03-20]. Dostupné z: https://z.cash/the-basics/

[34] What is Ether. *Ethereum Project* [online]. [cit. 2019-03-20]. Dostupné z: https://www.ethereum.org/

[35] Co je to ROI? Jasné vysvětlení, vzorec i příklad - Monetizace. *Internetový marketing jako úspěšný kanál - Monetizace* [online]. [cit. 2019-03-24]. Dostupné z: https://www.monetizace.cz/slovnicek/roi

[36] Bitcoin Blockchain - What is Proof of Work? - Reskilling IT. *Bitcoin Blockchain - What is Proof of Work? - Reskilling IT* [online]. [cit. 2019-03-22]. Dostupné z: https://vitalflux.com/bitcoin-blockchain-proof-work/

[37] Bitcoin mining the hard way: the algorithms, protocols, and bytes. *Ken Shirriff's blog* [online]. [cit. 2019-03-22]. Dostupné z: http://static.righto.com/images/bitcoin/block_diagram_ghash.png

[38] Wikipedia, the free encyclopedia. *Bitcoin network - Wikipedia* [online]. [cit. 2019-03-22]. Dostupné z: https://en.wikipedia.org/wiki/Bitcoin_network#/media/File:Bitcoin_Transaction_Visual.svg

[39] Ethereum Avg. Transaction Fee chart. *Bitcoin, Litecoin, Namecoin, Dogecoin, Peercoin, Ethereum stats* [online]. [cit. 2019-03-23]. Dostupné z: https://bitinfocharts.com/comparison/ethereum-transactionfees.html

[40] Monero Difficulty chart. *Bitcoin, Litecoin, Namecoin, Dogecoin, Peercoin, Ethereum stats* [online]. [cit. 2019-03-23]. Dostupné z: https://bitinfocharts.com/comparison/monero-difficulty.html

[41] Wiring diagram Torrent file The Way Things Work BitTorrent. *KissPNG - HD png images and illustrations. Free unlimited download.*[online]. [cit. 2019-03-23]. Dostupné z: https://www.kisspng.com/png-wiring-diagram-torrent-file-the-way-things-work-bi-6358840/preview.html

[42] Public-Blockchain. *Cloud Technology Partners - Cloud Computing Consulting* [online]. [cit. 2019-03-23]. Dostupné z: https://www.cloudtp.com/wp-content/uploads/2017/04/Public-Blockchain.png

[43] Monero (XMR) price, charts, market cap, and other metrics | CoinMarketCap. *Cryptocurrency Market Capitalizations* | *CoinMarketCap*[online]. [cit. 2019-03-25]. Dostupné z: https://coinmarketcap.com/currencies/monero/#charts

[44] Zcash (ZEC) price, charts, market cap, and other metrics | CoinMarketCap. *Cryptocurrency Market Capitalizations* | *CoinMarketCap*[online]. [cit. 2019-03-25]. Dostupné z: https://coinmarketcap.com/currencies/zcash/

[45] Ethereum (ETH) price, charts, market cap, and other metrics | CoinMarketCap. *Cryptocurrency Market Capitalizations* | *CoinMarketCap*[online]. [cit. 2019-03-25]. Dostupné z: https://coinmarketcap.com/currencies/ethereum/

[46] Ethereum Block Difficulty Growth Chart. *Ethereum (ETH) Blockchain Explorer* [online]. [cit. 2019-03-21]. Dostupné z: https://etherscan.io/chart/difficulty

Přílohy

DATA	Měsíční odměny z těžby	Cena k poslednímu dni měsíce	Prodej
May-17	1.00035456	236.96	237.0440165
Jun-17	2.00043431	315.17	630.4768815
Jul-17	2.00062555	203.87	407.8675309
Aug-17	1.00004492	386.14	386.1573454
Sep-17	0	303.19	0
Oct-17	1.00009768	310.55	310.5803345
Nov-17	1.25475492	465.5	584.0884153
Dec-17	0.64124363	760.35	487.5695941
Jan-18	0.56008026	1128.66	632.1401863
Feb-18	0.35829415	890.11	318.9212059
Mar-18	0.36721119	418.47	153.6668667
Apr-18	0.20240446	694.44	140.5577532
May-18	0.38750438	585.54	226.8993147
Jun-18	0.40617511	458.8	186.3531405
Jul-18	0.34281886	457.25	156.7539237
Aug-18	0.312035	284.55	88.78955925
Sep-18	0.41909587	236.99	99.32153023
Oct-18	0.45905433	198.34	91.04883581
Nov-18	0.51890582	119.41	61.96254397
Dec-18	0.43960445	140.18	61.6237518
Jan-19	0.35296615	110.46	38.98864093
Feb-19	0.45846586	138.85	63.65798466
Celkem	14.48217146		5364.469356