**Česká zemědělská univerzita v Praze**

**Provozně ekonomická fakulta**

**Katedra Informačních technologií**


**Diplomová práce**

# Virtuální měna, její těžba a výnosnost

**Bc. David Mička**

# ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

# ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. David Mička

Informatika

Název práce

**Virtuální měna, její těžba a výnosnost**

Název anglicky

**Virtual currency, mining and profitability**

---

**Cíle práce**

Hlavním cílem práce je otestovat těžbu virtuální měny a její výnosnost a výhodnost
Dílčími cíly práce jsou:
Představit koncept kryptografické měny a její historii
Ukázat situaci na trhu s virtuálními měnami
Poskytnout podrobný přehled o používaném hardwaru a jeho vývoji
Předložit očekávané směry vývoje virtuální měny do budoucnosti
Porovnat výkon specializovaného hardwaru se spotřebitelským
Formulovat závěry a doporučení

**Metodika**

Teoretická část představí koncept virtuální měny, její historii, vývoj možností získávání měny a složitost šifrování. Ukázána bude situace na trhu s virtuálními měnami a také porovnání jednotlivých měn vůči sobě, ale i jiným komoditám. Bude rozebrán způsob těžení. Praktická část se zaměří na testování výnosnosti a výhodnosti těžení také s ohledem na reálnou měnu, spotřebu energie, ale také možnosti směny se získanou virtuální měnou. Bude zmíněn používaný hardware na těžení virtuálních měn a jeho srovnání se spotřebitelským. Také budou předloženy očekávané směry vývoje virtuálních měn, jejich získávání a používaného hardwaru do budoucnosti. Na základě poznatků budou formulovány závěry a doporučení práce.

**Doporučený rozsah práce**

50 – 60 stran

**Klíčová slova**

virtuální měna, těžba virtuální měny, hardware, kryptografie, kryptografická měna

---

**Doporučené zdroje informací**

Bitcoin Wiki [online]. San Francisco, CA: Wikimedia foundation, 2014 [cit. 2017-04-24]. Dostupné z: https://en.bitcoin.it/wiki/Main_Page

CryptoCompare [online]. Londýn: Crypto Compare, 2015 [cit. 2017-04-24]. Dostupné z: https://www.cryptocompare.com/

Ethereum Project [online]. Zug, Švýcarsko: Ethereum Foundation, 2014 [cit. 2017-04-24]. Dostupné z: https://www.ethereum.org/

Franco, Pedro. Understanding bitcoin: cryptography, engineering and economics. Chichester, West Sussex: John Wiley & Sons Ltd., 2015. Print.

Root.cz [online]. Praha: Internet Info, 2008 [cit. 2017-04-24]. Dostupné z: http://www.root.cz/

---

**Předběžný termín obhajoby**

2017/18 LS – PEF

**Vedoucí práce**

Ing. Jiří Vaněk, Ph.D.

**Garantující pracoviště**

Katedra informačních technologií

Elektronicky schváleno dne 25. 4. 2017

**Ing. Jiří Vaněk, Ph.D.**

Vedoucí katedry

Elektronicky schváleno dne 27. 4. 2017

**Ing. Martin Pelikán, Ph.D.**

Děkan

V Praze dne 11. 03. 2018

**Čestné prohlášení**

Prohlašuji, že svou diplomovou práci " Virtuální měna, její těžba a výnosnost " 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 27.3.2018 _____

**Poděkování**

Rád bych touto cestou poděkoval Ing. Jiřímu Vaňkovi, PhD. za vedení a cenné rady poskytnuté při zpracování práce. Také bych rád poděkoval Patrikovi Mičkovi a anonymnímu zdroji za poskytnutí výsledků do praktické části této práce.

# Virtuální měna, její těžba a výnosnost

**Abstrakt**

Práce se zabývá problematikou virtuálních měn jejich těžbou a měřením výnosnosti těžby různým hardwarem. Nejdříve je vysvětlen koncept kryptografických virtuálních měn, kde jsou představeny jednotlivé pojmy z této oblasti nutné k pochopení problematiky a představena jejich stručná historie a možný vývoj měn do budoucna.

Praktická část je věnována samotné těžbě vybrané kryptoměny na běžném hardwaru, tedy osobním počítači a dvou specializovaných řešeních. Těžba je analyzována vzhledem ke spotřebě elektrické energie a získaným peněžním prostředkům z této těžby. Výsledky těžby a materiály ke specializovanému hardwaru byly získány od anonymního zdroje a těžba na osobním počítači je prováděna s pomocí vlastního hardwaru.

**Klíčová slova:** virtuální měna, peníze, hash, hashrate, těžba, grafická karta, ASIC, výnosnost, kryptografická měna, hardware

# Virtual currency, mining and profitability

**Abstract**

Thesis deals with the issue of virtual currency, its mining and measuring profitability of this mining with various hardware. First, the base concept of cryptocurrencies is explained, where there are introduced individual ideas of how the currencies work, which is crucial to understand the problematics. The history and mining hardware are dealt with as well.

Practical part is focused mainly on mining of chosen cryptocurrency on both ordinary hardware, which is represented by personal computer, and on two solutions of specialized hardware. Mining is analysed from perspective of energy consumption and earnings. Results of specialized hardware mining were obtained from anonymous source. Mining on personal computer was executed with own hardware.

**Keywords**: virtual currency, money, hash, hashrate, mining, graphics card, ASIC, profitability, cryptocurrency, hardware

# Obsah

# Seznam obrázků

## Seznam tabulek



## Seznam grafů

# 1 Úvod

Peníze fungují jako prostředek směny už od dob starověku, kdy lidé začali měnit jednu komoditu za jinou, posléze se vyvinuly do formy platidla jako například drobné cenné předměty (mušle, plátno – odtud vzniklo právě slovo platidlo, a další). Vždy to byla ale komodita mající funkci peněz. V průběhu historie se jako nejvhodnější komodity ukázaly drahé kovy (zlato, stříbro). Dále z těchto kovů vznikaly mince pak pro neefektivnost nakládání s mincemi vznikly bankovky.

Dalším krokem s rozvojem internetu byly digitální peníze, tedy peníze jako číslo na obrazovce, (částka na bankovním účtu) které ale defacto reálně jako oběživo neexistují, přesto nimi fyzická osoba disponuje.

Podmnožinou digitálních peněz jsou virtuální peníze či virtuální měna, která je vyměňována pouze online a nespravuje ji žádná centrální banka, ovšem tato hranice je pomalu smazávána díky narůstajícím možnostem platit virtuální měnou i služby. Pokud je takováto měna, či komodita zabezpečena říká se jí kryptografická měna a každá z těchto měn, z nichž největším se na tato práce věnuje, má své zakladatele a šifrovací algoritmy pro zabezpečení. Tyto peníze jsou vyměňovány pouze pomocí 1 a 0. Měny pak fungují velmi podobně, a proto můžeme říci, že máme 25 korun českých (Kč) stejně jako že máme například 25 bitcoinů (BTC), kde obojí je směnitelné.

Práce se také věnuje získávání těchto měn, které se děje pomocí řešení těchto algoritmů s využitím výpočetní síly specializovaného hardwaru či právě směnou za reálnou měnu a pak se uchovává ve speciálních databázích uživatelů nazvaných vhodně „peněženka“.

Prozatím je využití kryptoměn pro platbu služeb malé, ale do budoucna by se tento způsob měl rozšířit, i když jednou z charakteristik těchto měn je, že jich může být v oběhu vždy konečné množství.

# 2 Cíl práce a metodika

## 2.1 Cíl práce

Hlavním cílem práce je otestovat těžbu virtuální měny a její výnosnost a výhodnost hlavně vůči spotřebě elektrické energie. Dále je představen koncept fungování kryptografické měny, historie, ukázána situace na trhu s měnami a předloženy nejpravděpodobnější směry vývoje měn do budoucnosti. Zmíněn bude používaný hardware při těžbě a jeho vývoj napříč historií. Po otestování výnosnosti těžby jsou výsledky porovnány na všech řešeních. Na základě výsledků jsou formulovány závěry a doporučení práce.

## 2.2 Metodika

Teoretická část představí koncept virtuální měny, její historii, vývoj možností získávání měny a složitost šifrování. Ukázána bude situace na trhu s virtuálními měnami a také porovnání jednotlivých měn vůči sobě, ale i jiným komoditám. Bude rozebrán způsob těžení. Praktická část se zaměří na testování výnosnosti a výhodnosti těžení také s ohledem na reálnou měnu, spotřebu energie, ale také možnosti směny se získanou virtuální měnou. Bude zmíněn používaný hardware na těžení virtuálních měn a jeho srovnání se spotřebitelským. Také budou předloženy očekávané směry vývoje virtuálních měn, jejich získávání a používaného hardwaru do budoucnosti. Na základě poznatků budou formulovány závěry a doporučení práce.

# 3 Teoretická východiska

Tato část práce se věnuje konceptu kryptografické měny, její historii vývoje složitosti a získávání měny. Ukazuje také situaci na trhu s měnami a jejich použití ve veřejném životě. Také jsou zmíněny měny se zatím největším množstvím v oběhu.
Následující kapitola představí přehled řešené problematiky.

## 3.1 Pojmy

Pro orientaci v problematice kryptografických měn je v této kapitole uvedeno několik nejdůležitějších pojmů z této oblasti.

### 3.1.1 Peněženky

Uživatelé kryptografických měn mají své vlastní databáze, či úložiště měny s unikátní informací potvrzující jejich vlastnictví. Zatímco klíče potvrzují správnost transakce, peněženky snižují riziko krádeže jednotek, které nejsou používány.

Tyto peněženky mohou být uloženy v podstatě na jakémkoli médiu od cloudového úložiště po USB flash disk, přičemž je doporučena alespoň jedna záloha, která neukládá samotné jednotky, ale pouze informaci o jejich vlastníkovi a existenci.

### 3.1.2 Transakce

Přenos jednotek měny mezi dvěma peněženkami se nazývá transakcí, která je pak zapsána do *block chainu* a čeká na potvrzení. Při provedení transakce používají *peněženky* zašifrovaný podpis pro důkaz, že peněženka patří původci transakce. Potvrzování těchto transakcí se nazývá *těžba*.

### 3.1.3 Blockchain (Public ledger)

Hlavní databáze všech uskutečněných transakcí a aktivit, ověřující vlastníky všech vlastněných jednotek v jakémkoli bodě v čase. Jelikož je to záznam transakcí, jeho délka je konečná, obsahující konečné množství těchto transakcí, které s časem roste. Jeden blok v tomto řetězci obsahuje potvrzené a nepotvrzené (čekající transakce).
V každém uzlu sítě určité měny (decentralizované sítě serverových farem spravovaných těžaři) jsou uloženy identické kopie tohoto řetězce transakcí.

### 3.1.4 Těžba a těžaři

Těžaři slouží jako držitelé záznamů pro komunity měn a nepřímí rozhodčí o hodnotě měny. Pomocí velkého výpočetního výkonu, kterým je věnována kapitola v této části práce, těžaři ověřují úplnost, přesnost a bezpečnost block chainu. Těžba samotná pak probíhá počítáním matematických výpočtů a tím potvrzování transakcí v síti měny a přidáváním do block chainu. Těžba je podrobněji rozebrána v dalších kapitolách práce. Kapitola Pojmy čerpá z [49].

## 3.2 Historie kryptografických měn

První měna vznikla 9. ledna 2009, kdy byl vydán *Bitcoin 0.1*. Vytvořena byla vývojářem s pseudonymem Satoshi Nakamoto (dodnes se přesně neví, kdo tento vývojář je) a do verze 0.1.5 byla podporována pouze ve Windows 2000, NT a XP. Po vydání první verze Nakamoto okamžitě opravil některé malé chyby v komunikaci sítě a uzlů a pracoval na celkové použitelnosti klienta. [48]

Další verze se objevila v prosinci 2009, tedy rok po vydání první a podporovala Linux. Díky podpoře Linuxu se komunita stále více zapojovala do vývoje. Tato verze byla schopna použít více procesorů (jader procesoru) ke generování bloků transakcí, tedy v případě čtyřjádrových procesorů mohla mít těžba až čtyřnásobnou produkci.
V této době byl Bitcoin znám jen malé skupině prvních uživatelů, ale to se změnilo s vývojem JSON RPC API, které umožnilo službám třetích stran komunikovat s blockchainem a sítí. Díky narůstající popularitě na fórech (zejména bitcoin.org) bylo objeveno několik chyb v protokolu. [48]

S verzí 0.3 v létě roku 2010 vyrostl počet uživatelů, ale také složitost výpočtů při těžení. V této době se také začala používat k těžení grafická karta (grafický procesor) a uživatel „*ArtForz*“ postavil první farmu založenou na grafických kartách, API OpenGL a tím vygeneroval první blok transakcí v síti Bitcoin. V srpnu toho roku byla objevena první velká zranitelnost protokolu Bitcoinu, kdy transakce nebyly řádně prověřeny před přidáním do blockchainu, což povolilo uživatelům vytvořit nekonečné množství jednotek. O několik dní později byla tato chyba zneužita a jednou transakcí bylo vygenerováno 184 miliard

bitcoinů a posláno dvěma uživatelům. Tato transakce byla samozřejmě následně vymazána z blockchainu hned po zpravení této chyby v protokolu.

Do těžení se přidávalo více uživatelů, ale pro jednotlivce bylo těžké najít bloky a díky tomu také dostat odměnu za těžení. Díky této nerovnoměrnosti příjmů tito uživatelé zorganizovali skupiny, kterým se říká pool, pro rovnoměrné rozdělení odměn. První skupina Bitcoin Pooled Minig (BPM) vznikla na podzim roku 2010, existuje dodnes a nazývá se Slush's Pool. [48]

### 3.2.1 První experimenty

Na konci roku 2010 opustil s verzí 0.3.9 projekt bitcoinu Satoshi. Jeho odchod neznamenal konec měny, ale naopak komunita převzala vývoj a byl představen návrh pro zlepšení bitcoinu (BIP – bitcoin improvement proposal). Objevilo se v něm mnoho návrhů pro zlepšení, prvním z nich bylo propojit bitcoin se systémem překladu internetových adres (DNS) a tím vznikla měna *Namecoin.* Dále vývojáři experimentovali s bloky a dalšími parametry. Díky těmto experimentům vznikly GeistGled, iXcoin, SolidCoin a další.

Jelikož složitost šifrování bitcoinu rostla, uživatelé se přeorientovali na FPGA a GPU farmy pro těžení. Veřejnost se začala obávat chyb algoritmu SHA256, což otevřelo dveře dalším experimentům, kdy první měna, která tento algoritmus nepoužívala byla *Tenebrix*, měna těžená pomocí procesoru. [48]

Další z měn těžených s pomocí procesoru byl *Litecoin*, který byl komunitou přijat s větším nadšením, než Tenebrix.

### 3.2.2 Proof-of-stake

Princip proof-of-stake se na fórech objevil jako reakce na nerovné rozdělení síly (váha podílu na vývoji BIP). Tento princip zavedl sílu volby na základě množství vlastněných jednotek, prokázaných soukromými klíči (stake - podíl) oproti množství výpočetní síly dodávané do sítě, který se nazývá *proof-of-work* (work – práce, odvedená těžením).

Polovina roku 2011 znamenala také start vývoje pro mobilní zařízení a vznikl první decentralizovaný pool, P2Pool, založený na Peer-to-peer transakcích společně s prvním výzkumem ohledně anonymity v bitcoin síti. [48]

### 3.2.3 ASIC

Těžební jednotky ASIC, kterým se věnuje část s hardwarem, přišly na konci roku 2011 a destabilizovaly těžební proces. Problém těchto jednotek spočívá v konsolidaci výpočetní síly do rukou jednotlivců, což je proti samotné filozofii bitcoinu. [48]

### 3.2.4 Ripple

Na Ripple pracoval už v roce 2004 Ryan Fugger, webový vývojář z Vancouveru. Představil Ripplepay jako možnost pro bezpečné platby členům komunity přes celosvětovou síť. Uživatelé zjistili, že Ripple jako řetězec směnek, může použít nejlepší vlastnosti kryptoměn a vyřešit některé problémy jako závislost na centralizované výměně, velká spotřeba elektrické energie a pomalé transakce, což vedlo k vývoji nového systému Ripple v roce 2011. [48]

### 3.2.5 Multi-sig transakce

Více-podpisové transakce jsou součástí BIP 0010 vydané Alanem Reinerem. Taková transakce posílá prostředky z více-podpisové adresy, což je adresa spojena s více než jedním soukromým klíčem. Nejjednodušší je adresa typu m:n, která je spojena s n soukromými klíči s m podpisy, přičemž podpisů k poslání je třeba od m klíčů. [48]

### 3.2.6 Vývoj infrastruktury

V roce 2012 se velikost blockchainu stala problémem a vyvolala další náměty k řešení, jako byl například BIP 0016, který definoval Pay-to-script-hash (P2SH). P2SH řeší přesun odpovědnosti za poskytování podmínek, které je nutné splnit pro provedení transakce, z poskytovatele prostředků na jejich příjemce. Výhoda spočívá v povolení libovolně složitých transakcí od poskytovatele, které používají 20 bytový hash, jež je možné snadno převést například do QR kódu. [48]

S dalším růstem komunity se o bitcoin začali zajímat také specialisté z ekonomie, práv a přírodních věd. Mezi další odborníky, o které se komunita bitcoinu rozšířila patřili také programátoři jiných programovacích jazyků, například Javy. Propojení Javy a bitcoinu přineslo *BitcoinJ,* který byl startovním bodem pro vývoj aplikací v Javě, které spolupracují se sítí bitcoinu. [48]

Následující vývoj objevil další principiální nevýhody bitcoinu, tak vývojáři pracovali na měnách, které by tyto problémy vyřešily. Jednou z takových technologií, ne měnou, je CryptoNote, která používá kruhové podpisy, patřící do skupiny skupinových podpisů

a zaručují anonymitu odesílatele [mff tuma podpis]. Technologie je takzvaně ASIC-resistant, tedy těžení měn s technologií CryptoNote ASIC jednotkami je velmi nevýhodné, až nemožné. První měna založena na této technologii je Bytecoin, který si získal hlavně akademickou pozornost díky jeho pokročilé kryptografii. [48]

### 3.2.7 Vývoj peněženek

Na konci roku 2012 se velká část komunity soustředila na vývoj a zlepšení technologie peněženek, kdy myšlenka deterministické peněženky, jenž vytváří klíče z jednoho startovního bodu, nazvaného *seed* (semínko). Tento seed dovoluje uživateli snadno zálohovat a obnovit peněženku bez nutnosti jakýchkoli jiných informací [btwiki]. Cílem komunity bylo vytvořit intuitivní a bezpečnou peněženku. Tato snaha vedla jak k použití webových peněženek, tak například papírových, kde klíče byly napsány nebo k peněženkám na offline externím úložišti. [48]

### 3.2.8 Nové měny

Tento vývoj připravil základ pro vývoj mnoha alternativních měn vytvořených z bitcoinu. Patří mezi ně Primecoin, založený na hledání prvočísel, Dogecoin, jenž se rozšířil hlavně díky popularitě na internetu a Peercoin společně s NXT, což byly první měny s proof-of-stake technologií. CryptoNode byla přepsána do jazyka C++. V roce 2013 byly kompletně změněny principy bitcoinu a přibily další nové měny. [48]

## 3.3 Koncept kryptografické měny

Následující kapitola představí výhody a nevýhody kryptografických měn, jejich základní přehled a fungování transakcí a těžby.

### 3.3.1 Šifrování

**Kryptografická hash funkce**

Hash funkce je jednosměrný algoritmus, který lze spustit nad určitými daty (heslo, soubor) a jeho výstupem je kontrolní součet pevné délky, přičemž malá změna dat vstupu vede k velké změně dat na výstupu. Takový kontrolní součet pak slouží k ověření autenticity těchto dat. Například stejná data mají při použití stejné funkce vždy stejný výstup (kontrolní součet) a nikdy by neměl být výstup stejný u jiných dat. Tyto kolize se stávají, ale pouze u velkého množství dat, kde doba k nalezení takovéto kolize je prakticky nekonečně velká.

V síti kryptografických měn se hash funkce používají k ověření správnosti transakcí nejen, protože je snadné takovou funkci spočítat, ale také rozšifrovat výstup na vstup je energeticky a výpočetně náročnější než případný zisk, a to samé platí i o nalezení stejného výstupu pro jiná data. [46]

Při těžení měn jsou vstupy těchto funkcí nepotvrzené transakce s dalšími vstupy (čas a reference na předchozí blok). Vlastnost malé změny vstupu, která způsobí velkou změnu dat na výstupu je důležitá pro algoritmus proof-of-work při těžení: pro nalezení bloku se těžaři snaží najít hash začínající určitým počtem nul (cíl, vysvětleno v kapitole představení měn/bitcoin) s pomocí vlastních dat, kterým se říká *nonce*. Nonce je 32 bitové pole, jehož hodnota je nastavena tak, aby hash bloku obsahoval několik nul na začátku a zbytek je neměnný. Jakákoliv změna v *nonci* znamená i změnu v hashi bloku. Je nevýhodné předpovědět jaká kombinace bitů bude mít za výsledek správný hash (odpovídající hashi bloku). Je vypočítáno mnoho hodnot *nonce* a pro každou z nich je přepočítán hash dokud není nalezen takový, který má požadovaný počet nul na začátku. Tento počet nul je určen složitostí (kvůli podobnosti měn, které používají proof-of-work je rozebráno v kapitole představení Bitcoinu). [45]

**SHA-256**

Tento algoritmus je členem SHA-2 hash funkcí vyvinutých NSA a je to zkratka pro *Secure Hash Alghoritm*. Tyto algoritmy jsou následovníky rodiny SHA-1 a jsou to jedny z nesilnějších hash funkcí. Kód SHA-256 se příliš od SHA-1 neliší. Algoritmus ještě nebyl prolomen a 256 bitový klíč také dobře slouží pro použití do AES algoritmu. [43] Tento algoritmus je použit jako *proof-of-work* při těžení, přičemž u bitcoinu se stará u vytváření adres kvůli zlepšení bezpečnosti a soukromí. [44]

**Scrypt**

Algoritmus scrypt je paměťově náročná funkce pro odvozování klíčů, tudíž vyžaduje velké množství paměti. Proto je třeba na ASIC jednotkách používaných pro těžení bitcoinu třeba vyhradit místo pro RAM paměť a z tohoto důvodu jsou grafické karty pro těžení měn založených na tomto algoritmu vhodnější, protože je na nich přítomno poměrně velké množství rychlé paměti.

Scrypt vytváří mnoho náhodných čísel, které je třeba uložit v paměti. Algoritmus potom k těmto číslům přistupuje předtím, než vrátí výsledek. Výhoda tohoto algoritmu spočívá ve snížení výhod ASIC jednotek a tím zpřístupnění měn více uživatelům a těžařům. [42]

### 3.3.2 Blok

Blok je soubor, kde jsou uložena transakční data. Tyto bloky transakcí jsou seřazeny do lineární sekvence, jak jsou generovány. Této sekvenci se říká *blockchain.* Nové transakce jsou stále potvrzovány těžaři do nových bloků, které jsou posléze přidány do blockchainu. Po přidání už jsou transakce nevratné. Blockchain pak slouží jako potvrzení pro všechny uzly v síti, že transakce jsou platné a ověřené. [50]

**Struktura**

Každý blok obsahuje, mimo jiné, záznam některých, nebo všech nedávných transakcí a odkaz na blok, který byl zařazen před ním. Obsahuje také řešení složitého matematického problému, které je pro každý blok unikátní. Vše je zapsáno v hlavičce tohoto bloku.

Také je třeba zmínit *Merkle tree,* což je binární strom obsahující všechny transakce, které mají být do bloku přidány a má z nich být spočítán hash. [51]

Nové bloky nemohou být přijaty, pokud není problém vyřešen. Tento problém řeší *těžba,* kde je řešen složitý matematický problém s pomocí algoritmu hash funkce (kapitola šifrování). Tento proces je vlastně soutěž o nalezení správného řešení tohoto problému mezi těžaři. Pokud je řešení nalezeno, je snadné jej pro ostatní uživatele potvrdit, tedy je nutné řešení nalézt pouze jednou. Za nalezení tohoto řešení náleží řešiteli odměna – více v kapitole o těžbě.

Složitost tohoto problému je automaticky přizpůsobena podle toho kolik bloků je v síti měny vyřešeno za určitý časový úsek.

Každý blok obsahuje referenci na přechozí a tím tvoří řetězec. Je také možné řetězec rozdělit, například, když dva těžaři vyřeší problém dvěma různými platnými způsoby ve stejný čas, aniž by o tom věděli. Síť kryptoměny toto rozdělení řeší během chvíle, tudíž zůstane jen jedna větev tohoto rozdělení.

Klienti přijímají jako platný „nejdelší“ řetězec bloků. Nejdelší je takový řetězec (blockchain), který má největší kombinovanou složitost (ne nejvíce bloků), což znemožňuje někomu rozdělení řetězce vytvořením velkého množství bloků s malou složitostí a tím jeho akceptaci do sítě jako nejdelšího. [50]

### 3.3.3 Těžba

Jelikož kryptoměny nemají centrální autoritu pro řízení sítě, nějaké subjekty v ní musí ověřit a potvrdit transakce a tím je seskupit do bloku a zařadit do řetězce (*blockchain,* vysvětleno v kapitole Blok).

Uzly v síti, která tuto činnost vykonávají se nazývají „těžaři“. Pokaždé, když jsou transakce přidány do bloku a následně zařazeny do blockchainu, je odměněn ten uzel, který vyřešil matematický problém. Tento problém musí být vyřešen proto, aby měna nebyla znehodnocena přidáváním velkého množství bloků a tím generování velkých sum jednotek měny a také pro udržení stabilního množství vygenerovaných bloků za určitý časový úsek.[41]

Hlavní účel těžby je udržet síť měny bezpečnou a aktuální pro každý uzel v síti a tím dosáhnout společného konsenzu (souhlasu všech uzlů, že blockchain je ve správném a platném stavu). Těžba je také mechanismus vytváření nových jednotek do sítě. Těžaři dostávají transakční poplatky a nově vytvořené jednotky za potvrzení bloku, což slouží pro rovnoměrné rozšíření jednotek a zároveň motivace pro udržení sítě v chodu a zlepšení její bezpečnosti.

**Složitost těžby**

Nalezení nového bloku je složitý počítačový problém, jelikož je třeba nalézt hash (kapitola šifrování) hlavičky bloku a ten musí být nižší než udávaný cíl (cíl je řešen v kapitole představení Bitcoinu, jelikož je pro proof-of-work algoritmy použit stejně), aby byl přijat. Hash bloku musí začínat určitým počtem nul a pravděpodobnost spočítání takového hashe je velmi nízká, tudíž musí být podle algoritmu měny (SHA-256, Scrypt, EthHash a další) provedeno mnoho pokusů o spočítání (jak funguje tzv. hashování je podrobněji vysvětleno v kapitole Proof-of-Work).

**Měření složitosti**

Složitost se měří podle složitosti nalezení bloku s nejjednodušším cílem. Čím více uzlů těží, tím více bloků je vytvořeno. S rostoucím počtem těžařů roste také složitost pro nalezení bloku pro kompenzaci, což vyrovnává tvorbu bloků a tím také jednotek. Jakékoli bloky s hash hodnotou nevyhovující cíli budou odmítnuty ostatními uzly v síti. [40]

### 3.3.4 Transakce

Transakce je přenos jednotek měny mezi dvěma subjekty, přesněji mezi peněženkami dvou subjektů. Tyto peněženky fyzicky žádnou měnu nenesou, ale obsahují její adresu v síti, která drží záznam všech provedených transakcí a tím zůstatek.

Šifrování kryptoměn je asymetrické a adresa pak slouží jako veřejný klíč. U bitcoinu se pro větší anonymitu používá pro každou transakci jiná adresa, není to ovšem podmínka. Každá adresa má odpovídající soukromý klíč. Není možnost zjistit soukromý klíč z veřejného. [38] Tento klíč pak slouží k digitálnímu podpisu transakce. Podpis vznikne po průběhu funkce:

$$šifrovacíFunkce(TransakčníDetaily, soukromýKlíč) = DigitálníPodpis$$

U bitcoinu slouží pro vytvoření podpisu funkce *ECDSA, Elliptic Curve Digital Signature Algorithm* a soukromý klíč má délku 256 bitů. [38]

Transakční detaily se pak pro každou měnu mohou lišit, ale obsahují vždy položky:

- Adresa uživatele od
- Adresa uživatele pro
- Počet jednotek k odeslání

Digitální podpis je pak validován v síti a s pomocí adresy (veřejného klíče), je ověřeno, že transakce je důvěryhodná a jednotky náleží správnému vlastníkovi. Validace probíhá pomocí podpisu a veřejného klíče. Takováto transakce pak mohla být zkopírována (je podepsána) a může být se stejným podpisem přidána vícekrát. Tomuto brání přidání informace o ID transakce, kde přidání vytvoří pokaždé unikátní podpis.

Po validaci je transakce přidána do bloku, kde čeká na potvrzení těžaři, kteří za tuto práci dostávají poplatky. [37]

Rychlost transakcí je počet potvrzených transakcí za vteřinu. Nejrychlejší v tomto ohledu je síť měn Ripple (podrobnosti v kapitole Ripple), kde je potvrzeno 1500 transakcí/s oproti tomu v bitcoin síti je potvrzeno pouze 7 transakcí/s. [36]

### 3.3.5 Hardware

**Hashrate**

Hashrate je měrná jednotka síly v síti měny, tedy jak je silný hardware uzlu, který těží.
Těžení kryptoměny je potvrzování transakcí do bloku a získávání odměny za potvrzení daného bloku. K tomuto musí hardware počítat deterministickou hash funkci (jeden vstup produkuje vždy stejný výstup). Více informací o hash funkcích je uvedeno v kapitole šifrování.
Těžaři musí najít vstup, který obsahuje seznam všech nedávných transakcí, které potřebují potvrdit a jejichž hash hodnota je menší než cíl (podrobnosti o cíli v kapitole Bitcoin a podkapitole Složitost).

Nalezení hashe menšího, než cíl je možné pouze pomocí hledáním hrubou silou. Hashrate je tedy počet vypočítaných hash funkcí za jednu vteřinu. Některý specializovaný hardware dnes dokáže provést biliony těchto funkcí (jednotka TH/s – terahash za sekundu).

**CPU**

Centrální procesorová jednotka byla používána jako prostředek k těžění první měny bitcoin pouze v jejích začátcích,

CPU je hardwarový komponent vykonávající strojový kód uložený v paměti, který nazýváme programem. Procesor tedy vykonává několik, maximálně stovek, podobných činností, pro které je určen, pomocí logických hradel, ze kterých jsou složeny aritmeticko-logické jednotky, které vykonávající instrukce uložené právě v programu. Tedy procesor je spíše řídící element.

Pro těžení se procesor velmi rychle stal nedostatečným, protože dokáže, sice velmi rychle, spočítat hash, ale jeho jádra, kterých je nyní v běžném procesoru 6 a většinou je každé jadro tzv. „hyperthreaded“, tedy dokáže zpracovat více instrukcí naráz a chová se jako další jádro, dokáží zpracovat maximálně desítku instrukcí za jeden takt. Tudíž je možno procesor

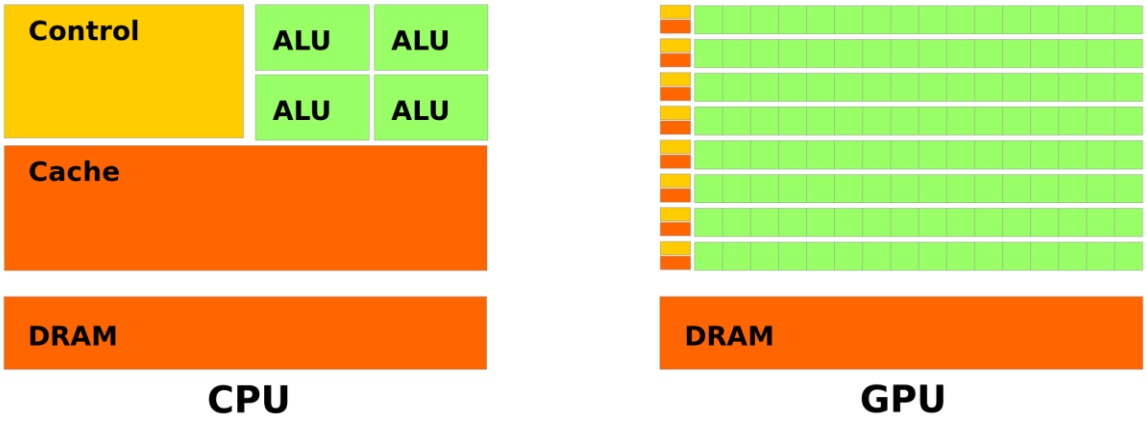
používat, ale výhodnost tohoto řešení zaručuje jedině výdělky v červených číslech vzhledem ke spotřebě energie, kde typický procesor vyšší třídy spotřebuje průměrně kolem 90 W.

**GPU**

Grafická karta a její jádro slouží primárně pro vykreslování UI systému, dekódování videa a renderování trojrozměrného prostředí (hry, 3D modely). Pro tyto účely obsahují dnešní grafické karty mnoho malých procesorů pro jednoduché výpočty, které, stejně jako CPU, dokáží provádět stejné výpočty, ale jsou určeny spíše pro opakující se práci – vykreslování mnoha snímků za sekundu ve 3D prostředí znamená neustále za sebou provádět výpočty pixelů.

Grafické karty se s příchodem DirectX 10 v roce 2006 začaly vyrábět s unifikovanými shadery, zvanými stream procesory. Tyto procesory jsou vlastně ALU určené jak na vertex, pixel shading, tesselaci atd. Díky unifikaci procesorů je možné na nich provádět i jiné výpočty, než na které jsou primárně určeny a jelikož počítání hash funkcí je jedna z činností, které grafická jádra provádějí velmi rychle, a navíc je to právě ta repetitivní činnost, při které se zpracovává velké množství dat, staly se grafické karty náhradou za CPU.

Toto provádění se navíc děje paralelně po všech stream procesorech, a tudíž typická grafická karta provede až o 800x více instrukcí než procesor. Jedna z nejvíce používaných grafických karet na těžení je AMD Radeon RX580 s 2304 stream procesory [52], což znamená 2304 jader, která vykonávají výpočty na síti měny.




*Obrázek 1 - rozdíl mezi architekturou CPU a GPU [35]*

*AMD a nVidia*

Rozdíly neexistují pouze mezi procesory a grafickými kartami, ale podstatné rozdíly ve výkonu jsou zaznamenány i mezi produkty dvou největších konkurenčních firem. Tento rozdíl je hlavně ve výkonu těžby.

Rozdíl je dán nejen jiným softwarem grafických karet (OpenCL u AMD a CUDA u nVidia), ale architekturálními rozídly v samotném jádře.

AMD vyrábí svá GPU na GCN architektuře, která obsahuje jednodušší procesory obvykle na nižší frekvenci (1200 - 1700MHz), a protože jsou menší, vejde se jich na stejnou plochu čipu více a operace mohou díky své jednoduchosti vykonat efektivněji.

NVidia používá CUDA jádra, která běží na firmou vyvinutém softwaru. Tato jádra jsou architekturálně složitější s vyšší frekvencí (až 2100MHz) a v jednom taktu vykonají méně operací, i když výkon v plovoucí řadové čárce je ve stejných kategoriích karet podobný.

Například u Bitcoinu je AMD zvýhodněno také použitím algoritmu SHA-256, který používá rotaci 32 bitového celého čísla (integeru). AMD má pro tuto operaci jednu instrukci (BIT_ALIGN_INT), ale nVidia karty musí provést 3 intrukce (2 posuny a 1 sčítání). Jen tento rozdíl dává AMD náskok 70 % ve výkonu. [34]

**ASIC**

ASIC znamená *appliaction-specific integrated circuit,* tedy integrovaný obvod určený pro určitou činnost, oproti například grafickým kartám, které mohou být využity obecněji.

První ASIC jednotky byly použity pro těžení v bitcoin síti, kde složitost vzrostla na míru, při které ani desítky grafických karet neměly požadovaný příjem. ASIC jednotky jsou určené pro jednu specifickou činnost, tedy v tomto případě počítání hash funkcí jednotlivých měn. Bitcoin ASIC jsou přímo určeny pro počítání SHA-256, který nevyžaduje velké množství paměti.

ASIC chipy prošly překotným vývojem a za zmínku stojí založení firmy CoinTerra v létě roku 2013 a její první produkt o 8 měsíců později. Tedy mezi specifikací problému a vydáním produktu neuběhl ani rok.

*Specifikace*

Mezi hlavní vlastnosti ASIC patří vysoká hashrate (typicky desítky TH/s) při nějaké účinnosti (J/GH – joulů na jeden GigaHash). Pořizovací cena je spíše vedlejší faktor.

Dalším faktorem jsou velikosti čipu (Giga hash na $mm^2$ – tedy kolik výpočtů připadá na obsah čipu) a η-factor (bere v úvahu velikost tranzistorů na čipu). Nejdůležitějším prostředkem pro těžení s pomocí ASIC je stabilní zdroj elektrické energie. Dále je také třeba brát v potaz vnitřní strukturu, tedy počet jader (*hashing engines*) na čipu ASIC jednotky a výpočetní sílu jednotlivých jader. [32]

Nejznámější firmou pro distribuci jednotek je čínská společnost Bitmain Ltd. a prodává jednotky AntMiner, jenž jsou rozšířeny více než ve 100 zemích na světě. Jejich nejnovější BM1387 čip je první 16nm FinFET pro těžbu. Hashrate dosahuje až 14TH/s podle softwaru, přičemž spotřeba je do 1327 W, což dává účinnost 0,098 J/GH, kde je třeba počítat s účinností zdroje. [24]

**Náklady na energie**

Jelikož většina sítí pracuje s proof-of-work algoritmem, je třeba používat velké množství výpočetní síly a ta spotřebovává energii.

Pro největší měnu Bitcoin není problémem jen spotřebovávaná energie, která se složitostí, a tudíž i potřebou větší výpočetní síly roste, ale také fakt, že většina této energie je produkována z uhelných elektráren. Například za jednu transakci je vyprodukováno 142 kg $CO_2$ a energie by mohla napájet skoro 10 průměrných amerických domácností po celý den.

Celková elektrická energie spotřebována bitcoinem je přiblžně 55 % spotřeby energie České republiky, což znamená přibližně 0,16% z celého světa. V absolutních číslech je spotřeba bitcoin sítě přibližně 37TWh. Všechny uvedené údaje jsou za jeden kalendářní rok.
Pro úsporu energie je třeba přejít na proof-of-stake algoritmus, kde spotřeba energie není tak velká. [31]

**Nedostatek grafických karet v roce 2017 a 2018**

Nástup nových měn s šifrovacími protokoly, které jsou odolné vůči ASIC jednotkám (hlavně Ethereum) způsobilo nedostatek grafických karet na trhu a raketový vzrůst jejich cen.

Výrobci nestíhali dodávat poptávané množství a poptávka překonala nabídku tak, že i ceny bazarových kusů vyrostly mnohdy i nad ceny nově prodávaných. Ke konci roku se situace začala stabilizovat, ale stále jsou ceny mnohem vyšší, jak ukazuje tato tabulka vybraných karet. Ceny jsou v dolarech na americkém trhu.

| Grafická karta | Cena před | Cena nyní |
|---|---|---|
| AMD Radeon RX570 | $170 (3620Kč) | $460 (9500Kč) |
| AMD Radeon RX580 | $230 (4900Kč) | $460 (9500Kč) |
| AMD VEGA 64 | $500 (10700Kč) | $1100 (22700Kč) |
| nVidia GeForce GTX1060 | $250 (5300Kč) | $400 (8250Kč) |
| nVidia GeForce GTX1070 | $380 (8100Kč) | $800 (16500Kč) |
| nVidia GeForce GTX1080 | $500 (10700Kč) | $1100 (22700Kč) |

*Tabulka 1 - navýšení cen grafických karet k 19.3.2018, server newegg.com*

[30]

### 3.3.6 Proof-of-work a Proof-of-stake

**Charakteristika**

Následující kapitoly představí 2 hlavní přístupy k těžení v sítích kryptografických měn.

**Proof-of-work**

Proof-of-work je protokol, který má za úkol odrazit útoky jako je například DDoS (distributed denial of service – posílání falešných požadavků, například na spojení). Protokol existoval ještě před bitcoinem, Nakamoto jej pouze na bitcoin aplikoval. Umožňuje důvěryhodný a distribuovaný vzájemný souhlas komunity. To znamená, že pokud chcete přijmou/poslat prostředky nemusíte vložit důvěru ve služby třetích stran, jako například při placení na internetu, kde je třetí stranou společnost provozující platební bránu.

V síti má každý k dispozici kopii blockchainu a tím pádem se nemusí o transakce starat třetí strana, protože každý si může informace ověřit.

- Existuje požadavek na náročný počítačový výpočet, kterému se říká těžba (proto název se slovíčkem work-pracovat)
- Odměna náleží prvnímu řešiteli tohoto počítačového problému
- Soutěž mezi těžaři o nalezení řešení tohoto problému
- Ve skupinovém těžení (pool) se těžaři při nalezení řešení odmění podle výpočetní síly

Protokol proof-of-work vyžaduje těžení pro vytvoření řetězce důvěryhodných transakcí (bloku) do blockchainu. (odkaz na související kapitoly – těžení, blok, transakce)[27]

Příklad proof-of-work algoritmu vypadá následovně:
Text, na kterém je prováděna práce (proof-of-work) je „Hello World!“. Cílem je najít takovou variantu, tak aby hash začínal třemi nulami (jedná se o SHA-256) a tedy bude nižší než hledaný cíl (řešeno v kapitolách Bitcoin a Těžba). Text se mění přidáním čísla na jeho konci (nonce) a toto číslo je po každém pokusu inkrementováno.

```
"Hello, world!0" =>
1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64
"Hello, world!1" =>
e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8
"Hello, world!2" =>
ae37343a357a8297591625e7134cbea22f5928be8ca2a32aa475cf05fd4266b7
...
"Hello, world!4248" =>
6e110d98b388e77e9c6f042ac6b497cec46660deef75a55ebc7cfdf65cc0b965
"Hello, world!4249" =>
c004190b822f1669cac8dc37e761cb73652e7832fb814565702245cf26ebb9e6
"Hello, world!4250" =>
0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9
```

Nalezení takového hashe trvalo 4520 pokusů, což pro moderní počítač není závratné číslo (grafické karty dokáží hash spočítat až 20 milionkrát za vteřinu). Výsledek funkce má na konci více nul, než bylo původně vyžadováno. [29]

**Proof-of-stake**

Proof-of-stake je jiný způsob ověřování transakcí, stále je algoritmem a cíl je stejný jako u předchozího protokolu, cesta k jeho dosažení je ovšem jiná. Problém může spočívat v centralizaci, jelikož nejvíce jednotek budou mít ti, kteří už jich nejvíce vlastní.

- Uživatel, který najde blok je vybrán deterministicky, podle jeho počtu jednotek, tedy podílu (stake)
- Těžaři jako odměnu dostávají poplatky za transakce
- PoS měny mohou být i tisíckrát nákladově efektivnější

Například Ethereum přejde na proof-of-stake algoritmus hlavně z důvodu šetření elektrické energie (jedna transakce s BTC vyžaduje energii, která dokáže napájet přibližně dvě průměrné americké domácnosti po jeden den). PoS nevyžaduje takové množství energie, jelikož těžení vlastně „neexistuje“.

Těžaři v PoS síti se nazývají kováři, jelikož netěží, ale jen získávají transakční poplatky. Kováři jsou vybíráni v pomocí nového protokolu Casper, kde funguje jistina, kterou uživatel musí složit, aby mohl hledat nové bloky. Do tohoto protokolu se mohou tedy připojit všichni, kdo jistinu složí. Počet validátorů (uživatelů potvrzujících transakce - kovář) není limitován, ale je hlídán ekonomicky snížením odměny, pokud je validátorů mnoho, či naopak zvýšením, pokud je počet malý.

Bezpečnost je zajištěna právě složenou jistinou, o kterou může útočník, či nevhodný validátor přijít.
U PoS tedy není třeba na rozdíl od PoW používat k získání odměny výpočetní sílu, protože získání odměny je určeno vlastněnými prostředky a momentální složitostí sítě, výhodou tedy je menší náročnost na energii.
Bezpečnost u PoW je zajištěna, pasivně, složitostí, kde nabourání do algoritmu je dražší než případný zisk při prolomení. [28] [27]

### 3.3.7 Přehled nejdůležitějších kryptoměn

**Bitcoin**

Distribuovaná peer-to-peer (transakce uživatel s uživatelem) měna, vytvořená Satoshi Nakamotem (nejmenší jednotka 1 Satoshi = $1 * 10^{-8}$BTC) s okamžitým a bezpečným převodem mezi dvěma uživateli kdekoli na světě.
Nejznámější a nejpoužívanější měna s největší tržní kapitalizací (největší hodnotou), která momentálně čítá 16,4 milionu BTC (označení pro jednotku bitcoinu) s neustále se měnící cenou za jednotku. V lednu byla cena za jeden BTC až 20 000 USD, v březnu je to okolo 8500USD. Celková hodnota všech Bitcoinů v síti je 142,2mld USD.

*Tvorba bitcoinů*

Tvorba měny probíhá v síti v procesu *těžení,* kterému se podrobně věnuje kapitola *Těžba*. Těžení je zjednodušeně proces řešení složitých matematických problémů hardwarem a tím nalezení nového bloku (odkaz na text vysvětlující blok). Vytvoření nového bloku je *proof-of-work (odkaz na text)* systém, jehož složitost se odvíjí od síly sítě. Odměna za vyřešení bloku se automaticky upravuje tak, aby za každé 4 roky se množství vytvořených bitcoinů zmenšilo na polovinu. Tedy přibližně 10,5 milionu jednotek bylo vytvořeno první 4 roky (odměna 50BTC) a v dalším čtyřletém období se tato suma zmenší o polovinu na 5,25 milionu (odměna 25BTC) a tak dále. Tento trend zaručuje, že nikdy nebude vytěženo více než přibližně 21 milionu BTC.

*Získání bitcoinů*

Je mnoho různých cest k získání bitcoinů:

- Přijmout jako platbu za zboží nebo služby
- Nakoupit za fiat měnu
- Nakoupit v bitcoinových bankomatech
- Směnit za hotovost osobně
- Těžením
- Vytvořit nový blok samostatným těžením (nyní odměna 12,5BTC)

*Uživatelé*

Uživatelé mohou být pouze vlastníci nebo vlastníci a zároveň těžaři. Každý uživatel má svou *adresu* v síti a *peněženku.*

*Adresa*

Identifikátor obsahující 26-35 alfanumerických znaků začínající číslem 1 nebo 3, což určuje možný cíl platby. Adresy mohou být generovány pro uživatele zdarma.

Dva možné formáty adres používaných uživateli bitcoinu:

1. Běžná P2PKH začínající číslem 1 – například: 1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2
2. Novější P2SH začínající číslem 3 – například: 3J98t1WpEZ73CNmQviecrnyiWrnqRhWNLy

Tato adresa je pak na jedno použití (single-use token), tedy pro každou transakci je vytvořena nová adresa. Takováto tvorba může probíhat v režii uživatele i offline, bez registrace do Bitcoin sítě. Například stačí použít volně dostupný sofware pro generování adres.
Adresy jsou case-sensitive, tudíž musí být při jakékoli manipulaci kopírovány přesně. Pokud je taková adresa nepřesná, bude sítí odmítnuta, přičemž pravděpodobnost přijetí špatné adresy je $1:2^{32}$.

Ověření transakce mezi adresami ještě, než proběhne, se pak provádí přes elektronický podpis, kterým disponují peněženky. Některé služby mají například adresy používané pouze k ověření, ale v takovém případě by tato adresa nikdy neměla být použita k transakcím.

**Více podpisové adresy**

Mohou být vytvořeny adresy, které vyžadují kombinaci několika soukromých klíčů. Protože takové adresy využívají nové prvky, začínají číslem 3. Takové adresy si můžeme představit jako šek posílaný více stranám, kde všechny zmíněné strany musí takový šek podepsat. Počet klíčů k vytvoření takovéto adresy je rozhodnut ještě před jejím vytvořením, uživatelem generujícím tuto adresu.

**Znovu použití adresy**

Znamená použití jedné adresy k více transakcím, což není jejich smýšlené užití. Takovéto použití adresy ohrožuje soukromí a bezpečnost účastníků transakcí a zároveň vlastníků jejich výsledku.

*Peněženka*

Bitcoinová peněženka je kolekcí soukromých klíčů, ale může to být také software k jejich správě a provádění transakcí.
Jedna z nejpoužívanějších peněženek je *Bitcoin Core,* která ukládá informace do souboru **wallet.dat** ve formátu „bitkeys“ (formát pro informace v peněžence, například csv).

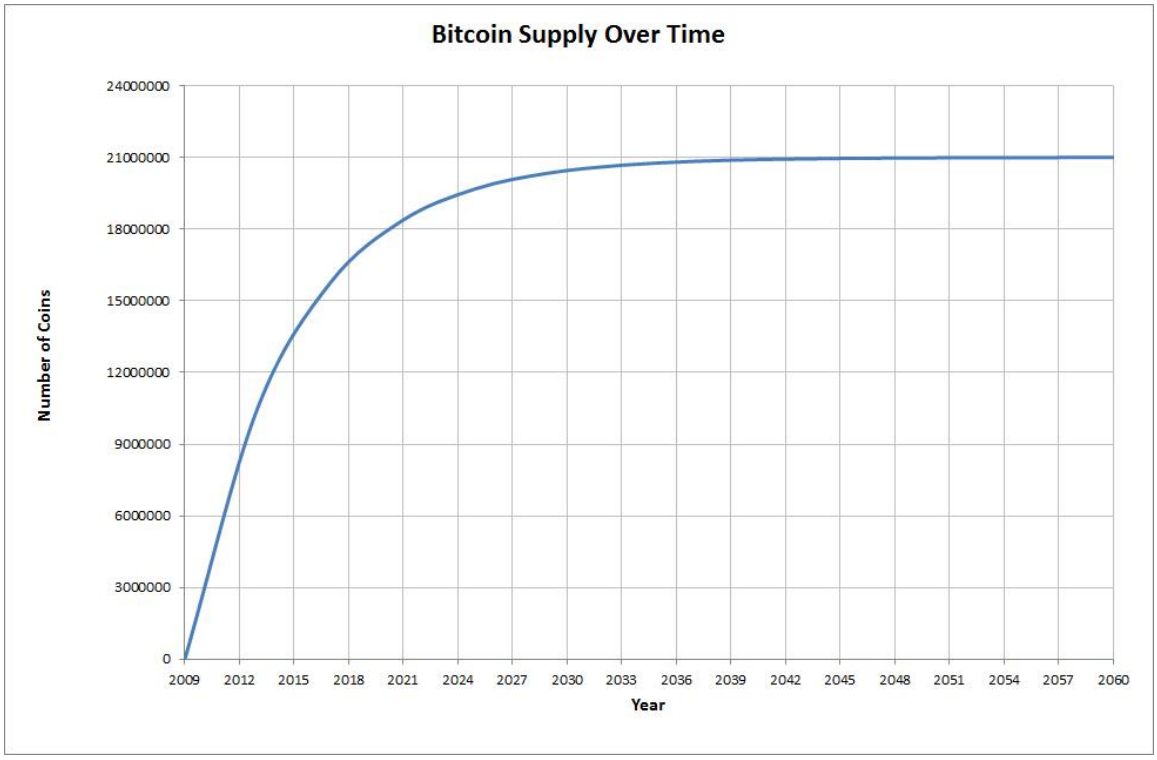
Taková peněženka pak obsahuje:

- Klíče pro každou z adres
- Transakce provedené z/do adres
- Preference uživatele
- Implicitní klíč
- Náhradní klíče

- Účty
- Číslo verze
- Key pool (úložiště pro předgenerované klíče, zatím nepoužité)

*Omezení*

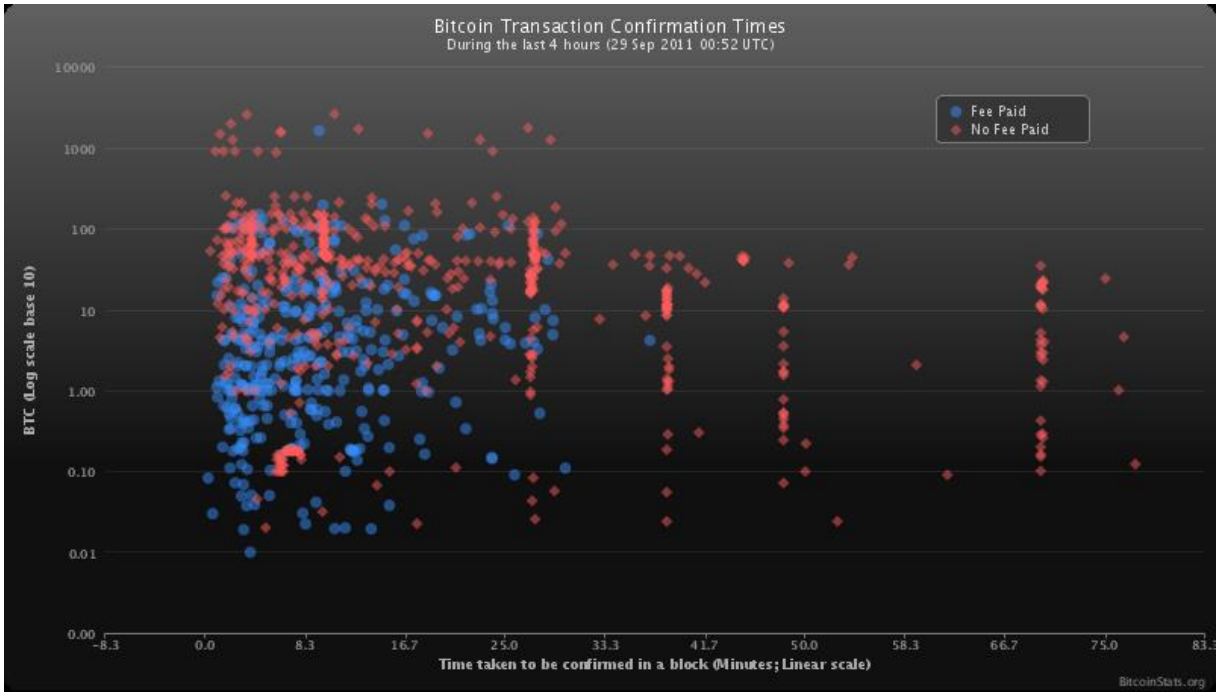
Počet bitcoinů v síti je omezen na 20 999 999, 9679 BTC, od této sumy bude počet bitcoinů v síti statický, což se stane přibližně v roce 2140. Ovšem použití transakčních poplatků bude vytvářet stále nové bloky.




*Graf 1 - vývoj počtu bitcoinů v čase*

Se zmenšujícím se počtem jednotek roste jejich cena (zákon nabídky a poptávky). S větší hodnotou bitcoinu jich bude potřeba méně k nákupu služeb.

Každý uživatel musí počkat 10 minut předtím, než může své peníze použít. Toto omezení je dáno průměrným časem, za který je nalezen nový blok. Pak lze potvrdit, že uživatel skutečně jednotky vlastní a může je použít k dalším transakcím.




*Obrázek 2- průměrný čas k potvrzení transakce (rok 2011) červeně: bez poplatku, modře: s poplatkem*

*Složitost*

Aby byla pochopena složitost těžení bitcoinu, je nutné nejdříve zmínit *cíl*. Cíl je 256 bitové číslo, které je sdíleno mezi všemi Bitcoinovými klienty. Hash SHA-256 hlavičky bloku musí být nižší nebo stejný jako současný cíl pro přijetí bloku do sítě. Čím nižší je cíl, tím je složitější potvrdit blok.

Maximální cíl (tedy nejjednopdušší) používaný zařízeními SHA-256:
0x00000000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
Tedy jak složité je najít hash pod daný cíl. Bitcoinová síť má souhrnnou složitost bloku a platné bloky musí mít hash menší nebo roven tomuto cíli. Tato složitost se mění s každými 2016 bloky.

Rovnice pro výpočet složitosti:

$slozitost = \frac{slozitost\_1\_cil}{soucasny\_cil}$, kde $slozitost\_1\_cil$ tradičně reprezentuje hash, ve kterém prvních 32 bitů jsou 0 a zbytek 1 (tomuto se říká *pool difficulty*, jednotka *pdiff*). Protokol Bitocinu představuje cíle jako vlastní typ s plovoucí desetinnou čárkou a jako výsledek klienti odhadují složitost na tomto typu. (*bdiff*)

Každý blok v sobě má uloženou složitost jako cíl. Tento cíl je zabalený a dá se získat s pomocí předdefinované rovnice. Tedy pokud je zabalený cíl 0x1B0404CB, pak jeho hexadecimální reprezentace vypadá následovně:

$$0\text{x}0404\text{CB} * 2^{(8*(0x1B-3))}$$

$$= 0\text{x}00000000000404\text{CB}000000000000000000000000000000000000000000000000$$

Vypočtení složitosti nalezení tohoto bloku:

Nejvyšší možný cíl (složitost 1) je definován jako 0x1D00FFFF, z čehož plyne hexadecimální reprezentace:

$$0x00FFFF * 2^{(8*(0x1D-3))}$$

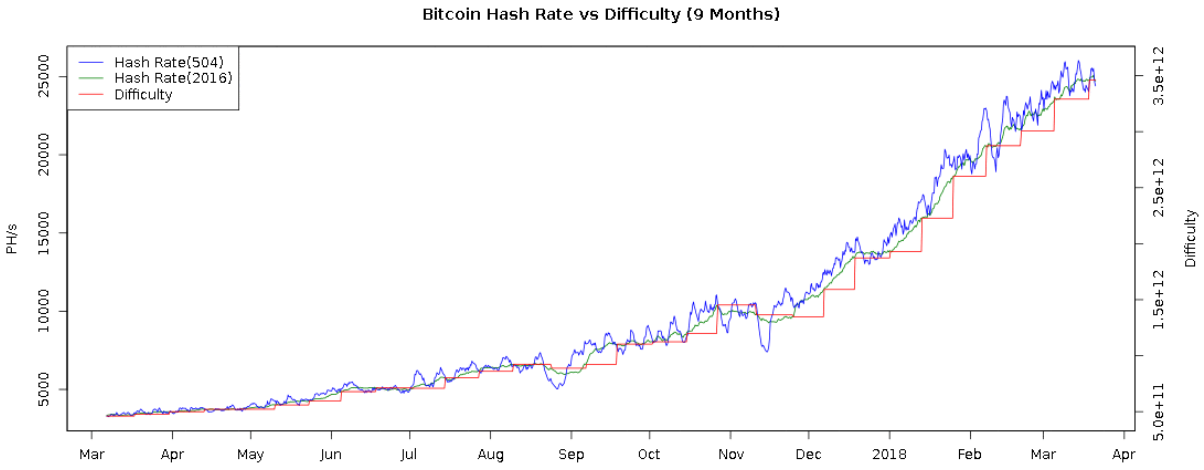
$$= 0x00000000FFFF0000000000000000000000000000000000000000000000000000$$

Tedy stejný cíl jako výše zmíněný, pouze zkrácený.

Výpočet pak probíhá podle vzorce uvedeného výše:

0x00000000FFFF0000000000000000000000000000000000000000000000000000 /
0x00000000000404CB000000000000000000000000000000000000000000000000
= 16307.420938523983 *(bdiff)*

0x00000000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF /
0x00000000000404CB000000000000000000000000000000000000000000000000
= 16307.669773817162 *(pdiff)*




*Graf 2- vývoj složitosti bitcoinu v posledním roce [26]*

Celá kapitola o Bitcoinu je čerpána z [25].

*Použití*

Jelikož v České republice je jedna z nejaktivnějších komunit, dá se touto měnou platit na mnoha místech, a nejen ve velkých městech. Díky rozšíření přijímá měnu kolem 200 restaurací, taxislužby, fotografové nebo daňoví poradci. Celosvětově přijímají platby bitcoinem hlavně firmy, jejichž zaměření je hlavně v IT sféře.

Minulý rok byla v ČR zavedena elektronická evidence tržeb, a s tím přichází pro podniky nutnost vlastnit pokladnu, která tuto měnu podporuje.

Ve výhodách jsou zmíněny malé poplatky za transakce, kde se tato skutečnost promítá i do veřejné sféry, kde jsou poplatky třikrát menší než například za stravenky. [53]

**Litecoin**

*Stručné představení*

Litecoin je, po Bitcoinu, druhá nejoblíbenější kryptoměna a čtvrtá ve velikosti tržní kapitalizace. Je založena na protokolu Bitcoinu, tudíž je také peer-to-peer, transakce jsou s velmi malým, nebo žádným poplatkem a měna je open source.

Litecoin navrhl společně se členy Bitcoin komunity Charles Lee a spustil jej 13. října 2011. V porovnání s bitcoinem přináší několik vylepšení.

Hlavní charakteristikou je použití scrypt jako šifrovacího a proof-of-work algoritmu. Algoritmus potlačuje hardwarovou škálovatelnost tím, že požaduje velké množství paměti při provádění výpočtů. Tato změna oproti SHA-256, který používá Bitcoin, snižuje nárůst efektivity a iniciativy vyvíjet specializovaný hardware na těžení, například jednotky ASIC, které je možno připravit k mnoha účelům a k jejich použití na těžení Litecoinu dojde dříve, nebo později.

Druhá charakteristika spočívá v čase mezi potvrzením transakcí, který je stanoven na 2:30min, což znamená rychlejší přístup uživatelů k jejich financím.
Použití Litecoinu roste a potvrzuje to prohlášení MtGox, největší směnárna Bitcoinu na světě, že přijímá Litecoin do svého portfolia. Tyto zprávy pomohly měně zvýšit cenu a ten dosáhl v roce 2017 tržní kapitalizace přes dvě miliardy dolarů a nyní se obchoduje za 43 dolarů.

*Porovnání s bitcoinem*

- SHA256 (Bitcoin) a Scrypt (Litecoin)
  SHA256 je velmi dobře paralelizovatelný algoritmus, tedy není nutno vynaložit prakticky žádný výpočetní výkon na rozdělení problému do menších částí.
  (stackoverflow/emabras) Scrypt sice používá SHA256 jako podprogram, ale spoléhá na rychlý přístup do velkého množství paměti. SHA256 počítá pouze aritmetické operace, a proto je jednoduché ho spustit na více ALU (Aritmeticko Logická Jednotka), kdežto spustit více instancí Scryptu je složité kvůli paměťovému omezení. Proto se Litecoin těží lépe na grafických kartách, kde je přítomno velké množství paměti.
    - Charakteristika
      - Levné pořizovací náklady pro těžení – začít těžit bitcoin dnes vyžaduje velkou vstupní investici v podobě ASIC jednotek, v případě Litecoinu je potřeba buď počítač nebo grafické karty
      - Nedojde k centralizaci těžení díky použití většího množství paměti – v případě bitcoinové sítě mohou někteří uživatelé jednorázově investovat velké množství peněz do jednotek ASIC a tak z části centralizovat síť. U Litecoin k něčemu

takovému nemůže dojít, protože u jednotek ASIC je velmi drahé duplikovat použití paměti, tudíž investice do ASIC by byla v případě Litecoinu velmi drahá.

- Použití webových stránek na těžení – uživatelé na internetu mohou podpořit stránku těžením, jenom tím, že ji navštíví. Mohou těžit nejen přes CPU, ale i s GPU s použitím OpenCL API.
- Vývojáři mohou získat výhodu na uživateli lepšími implementacemi na určitý hardware, což prohloubí nejen znalosti o měně, ale také kryptografii

Všechny informace o měně Litecoin byly čerpány z [21]

**Ethereum**

Ethereum se jako měna snaží v podstatě nahradit existující client-server model decentralizovanou sítí uzlů složenou z počítačů dobrovolníků, což by vytvořilo jakýsi „světový počítač“, který by mohl tuto možnost připojit se, nabízel všem na světě a dovolil jim nabízet služby ostatním. Služby nabízejí třetí strany (aplikace v AppStore například), tento systém se snaží působnost třetích stran eliminovat.

Pokud jsou uloženy dokumenty například na Google Docs, nebo fotky na Facebooku, jsou všechna tato data vlastněná právě těmito třetími stranami. Tento model by všechny třetí strany eliminoval a vrátil vlastnictví jejich tvůrcům.

*Fungování Ethereum*

Měna používá hodně z bitcoinového protokolu, ale mění ho tak, aby byla schopna podpořit její využití dál než jen jako peníze.

Měnit protokol tak, že vývojáři jsou schopni vytvořit aplikace nebo dohody, jenž mají další kroky, nová pravidla vlastnictví, jiné typy transakcí nebo jiný způsob přenosu stavu.

K tomuto měna používá turingovsky úplný programovací jazyk, což vývojářům umožnuje napsat více programů, pomocí nichž se mohou dít transakce a měnit určité výstupy.

Používá *smart contracts,* což jsou programy, které jsou vykonávány přesně, jak zamýšleli jejich tvůrci, právě zmíněným jazykem.

Může být také chápáno jako smlouva mezi dvěma subjekty, jehož pravost je vynucena kryptografickým kódem. Například dva uživatelé si mohou poslat prostředky k určitému datu, použitím právě smart contractu. [20] [19]

**Porovnání s měnou Bitcoin**

Na následujícím obrázku porovnání s bitcoinem je na řádku *transaction* vidět u ethereum takový smart contract. Skript pro transakci může být pro transakci libovolně upraven. [54]

| | bitcoin | ethereum |
|---|---|---|
| **concept** | digital money | smart contracts |
| **transaction** | send from alice to bob | send from alice to bob if..<br>• date = jan 1, 2018<br>• bob's balance < 10 eth |
| **market cap** | ~$18 billion | ~$1 billion |
| **founder** | satoshi nakamoto (unknown) | vitalik buterin and team |
| **release date** | jan 2009 | july 2015 |
| **release method** | early mining | presale raised $18M in bitcoin |

*Tabulka 2 - porovnání ethereum a bitcoin [20]*

Smart contracty:

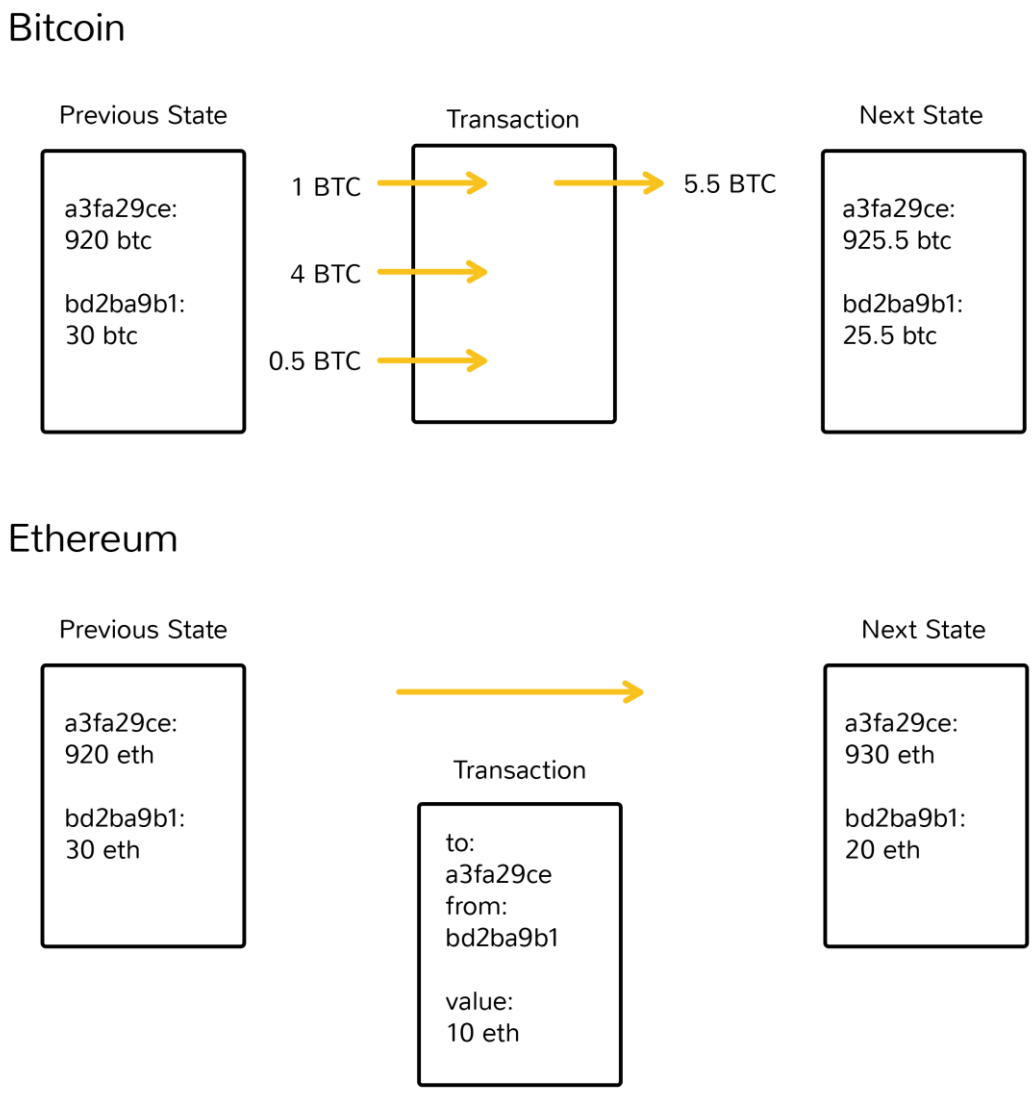
- Mohou sloužit jako „multi-signature“ (vícepodpisové) účty, a tak jsou prostředky použity, pouze pokud souhlasí určité procento uživatelů
- Spravují dohody mezi uživateli
- Ukládat informace například o aplikaci, přihlašovací údaje atd.

**Blockchain**

Struktura blockchainu je velmi podobná tomu z bitcoinu, tedy je to řetězec všech transakcí, který má každý uzel uložen.

Na rozdíl od bitconu, si ale uzly v ehtereum síti ukládají nejaktuálnější stav každého *smart contractu*. Pro každé použití si síť musí udržovat informace o stavu, nebo informace o aplikacích, zůstatku uživatelů, kód *smart contractu* a kde je tento kód uložen.

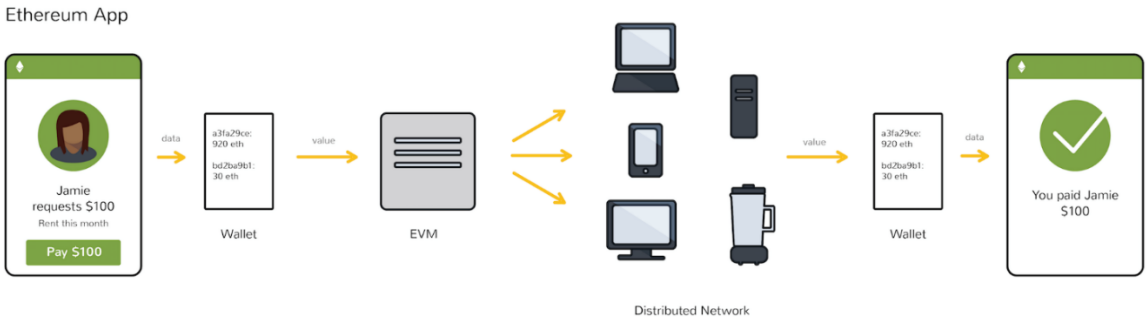
Bitcoin při transakcích zachází se svými jednotkami při transakcích jako s obyčejnými penězi. Naproti tomu ehtereum používá účty, jako v bance, kde jsou pro přenos využity poukázky (tokeny), které jsou uloženy v peněžence a mohou být přesunuty na jiný účet (jako platba). Tento rozdíl v transakcích a posouvání sítě do dalšího stavu dobře popisuje následující obrázek:




*Obrázek 3 - bitcoin transakce a ethereum token*

**Virtuální stroj ethereum**

Jelikož ethereum využívá *smart contractů,* je třeba takový kód přeložit do bytekódu, který může být spuštěn EVM (Ethereum Virtual Machine). Všechny uzly provádějí kontrakty pomocí svých EVM, jako na obrázku.




*Obrázek 4- EVM*

Každý uzel v síti má tedy uloženou kopii transakcí a historii *smart contractů* a k tomu drží inforamce o aktuálním stavu. Pokaždé když je vykonána nějaká operace, všechny tyto uzly se musí dohodnout, že se tato operace odehrála a byla důvěryhodná.

Cílem u EVM je zodpovědnost za tyto změny sítě v rukou těžařů a uzlů, tedy decentralizovaná síť bez jakékoli centrální kontrolní autority. EVM může provádět *smart contract* s jakýmikoli pravidly, která jsou programátorem napsána. Jako Javu je možné taky kontrakty psát ve vyšších programovacích jazycích jako *Solidity* nebo *Serpent*.

Informace pro podkapitoly Blockchain a Virtuální stroj Ethereum byly včetně obrázků čerpány z [20]

### Ripple

Ripple je stejně jako bitcoin a ostatní měny, peer-to-peer decentralizovaná měna s nízkými, či žádnými poplatky za transakce.

Na rozdíl od ostatních měn se v Ripple síti dají posílat jakékoli měny, a to i měny běžné (fiat), přičemž funguje i výměna těchto měn. Transakce jsou potvrzeny v několika sekundách, protože neexistuje těžení a klienti jsou připraveni hned.

Ripple síť je určena uživatelům, kteří spíše chtějí decentralizovaný systém pro výměnu fiat měn a k tomu přidat výhody kryptoměn. [17] Tedy:

- Levné transakce – třetí strany při transakci neexistují, není třeba transakčních poplatků (transakce stojí maximálně $0.01)
- Soukromě – není třeba nikomu posílat osobní informace
- Bezpečně – po transakci si příjemce nemůže účtovat poplatky, ani chtít žádné další informace
- Spolehlivě – transakce jsou nevratné

Na ripple síti lze také samozřejmě používat bitcoin na vstupu transakce a na jejím výstupu může být jakákoli jiná měna, což znamená například zaplatit bitcoinem a příjemce dostane platbu v dolarech. [14] [15]

Ripple síť má také svou vlastní měnu XRP (*ripples*) a primárně slouží k ochraně sítě. Uživatel musí mít určitou jistinu XRP pro možnost vlastnictví účtu a možnosti provádět transakce. V XRP jsou účtovány také transakční poplatky, při kterých jsou jednotky zničeny. Zvláštností XRP je skutečnost, že všechna měna byla vypuštěna do oběhu na jejím začátku. Autoři vytvořili počáteční *ledger* (viz pojmy) se 100 miliardami XRP a více těchto jednotek už nebude, a proto, jak již bylo zmíněno výše, není třeba těžení. [15]

#### Unique Node List

V síti měny XRP každý uzel, při změně ledgeru, elektronicky podepisuje jeho prohlášení svého názoru o správnosti ledgeru. Každý v síti může ověřovat správnost sběrem těchto prohlášení a pokud takovýchto prohlášení nasbírá dost na svůj *Unique Node List (UNL),* může být ledger prohlášen za důvěryhodný.

#### Další funkce Ripple

- Žádná těžba
  - Bez útoků s 51 % pravděpodobností (zastavení procesů v blockchainu díky centralizaci výpočetní síly) [16]

        - Bez bloků obsahujících jednu nebo žádnou transakci
        - Bez těžby, tudíž není třeba investic do vybavení
    - Rychlost ověření
        - Ripple ověří účet, či transakci pomocí několika bytů, tudíž není třeba stahovat celý blockchain
    - Deterministické peněženky
        - Účty mají dvojitá (hlavní a vedlejší) hesla
        - Data peněženek jsou uložena zašifrovaná na Ripple síti
        - Není potřeba třetích stran pro provoz peněženek [14] [15]

### 3.3.8 Výhody kryptografických měn

1. Podpora hodnoty vestavěním umělého nedostatku

Většina měn má zabudován jejich nedostatek, tedy ve zdrojovém kódu je napsáno kolik jednotek této měny může existovat. Podobně jako drahé kovy jsou tak chráněny proti inflaci.

2. Uvolnění vládního monopolu měn

Kryptoměny umožňují spolehlivou výměnu vně přímé kontroly nadnárodních bank. Tento systém je atraktivní pro ty, kteří se bojí kvantitativního uvolňování (expanzivní monetární politika centrální banky pro stimulaci ekonomiky, například nákup státních dluhopisů). Z dlouhodobého hlediska odborníci očekávají, že světové vlády začnou alespoň okrajově začleňovat aspekty kryptoměn jako vestavěný nedostatek nebo ověřovací protokoly do státních měn.

3. Komunity starající se o sebe

Těžba je vestavěná kontrola kvality a mechanismus zařizování politiky pro kryptoměny. Jelikož jsou těžaři za svou práci placeni, mají svůj finanční podíl na udržování přesných a aktuálních záznamů o transakcích a tím zajišťují integritu systému a hodnotu měny.

4. Ochrana soukromí

Soukromí a anonymita byly už od začátku největšími obavami po zastánce kryptoměny. Mnoho uživatelů používá pseudonymy, jenž nejsou spojeny s žádnou informací, podle které by bylo možné uživatele identifikovat. Bitcoin používá adresy v jeho síti, které zaručují

anonymitu. Sice je možné v komunitě vyhledat identitu uživatele, ale ne u nových kryptoměn odvozených z Bitcoinu.

5. Cena transakcí

Díky použití klíčů a peněženek se vyřešil problém s dvojitými výdaji, čímž se zajistí, že nové kryptoměny nebudou zneužívány technicky zdatnými podvodníky schopnými replikovat digitální prostředky. Bezpečnostní prostředky kryptoměn také umožňují vyřadit poskytovatele plateb třetí strany (Visa, PayPal), který platbu ověřuje, což okamžitě ruší velké poplatky za tyto platby. Roli tohoto prostředníka pak zastávají těžaři, kteří za každou potvrzenou transakci mohou, ale také nemusí dostat poplatek, který je ale ve srovnání s klasickými službami velmi malý (méně než 1 %).

6. Vlády nemohou kontrolovat účty

Jelikož kryptoměny mají decentralizovaný systém, nelze odstavit vlastníka od jeho účtu, protože uživatelé mají kopie blockchainu, kde je uložena každá transakce tohoto vlastníka.

7. Cena mezinádrodní směny

Transakce kryptoměn jsou stejné jak v domácím, tak v celosvětovém měřítku. Nezáleží kde se nachází poskytovatel nebo příjemce, transakce jsou buď zdarma nebo s malým poplatkem. Mezinárodní transakce bank oproti tomu mohou účtovat někdy i 15 % za tuto platbu, či výběr z bankomatu v zahraničí.

### 3.3.9 Nevýhody kryptoměn

1. Nedostatek kontroly a regulace podněcuje černý trh

Největší nevýhodou kryptoměn je její schopnost podněcovat nelegální činnost, jelikož není kontrolována žádnou institucí. Mnoho transakcí na černém trhu je uskutečněno pomocí kryptoměn. Například nechvalně známý web na prodej drog „Silk road“ používal pro nákupy pouze Bitcoin, předtím, než byl v roce 2014 vypnut.
Kryptoměny jsou také oblíbeným nástrojem pro praní špinavých peněz. Protože vládní složky složitě hledají původce transakcí, je vlastně výhoda anonymity také nevýhodou.

2. Potenciál ke krácení daní

Kryptoměny, jak už bylo zmíněno, nejsou kontrolovány centrální bankou ani vládou a fungují vně jejich pravomocí, což přitahuje daňové útočníky. Zaměstnavatelé mohou zaměstnance platit v Bitcoinech a tím osvobodit od daní jak sebe, tak zaměstnance. Podobně pak mohou fungovat některé online obchody, které přijímají platbu v Bitcoinech a mohou se tak vyhnout placení daně z příjmu.
Ve Spojených státech platí daňové zatížení na všechny platby kryptoměnou, avšak mnoho států takovou politiku nemá, protože původci a příjemci transakcí jsou těžko dohledatelní.

3. Možnost ztráty financí díky ztrátě dat

Protože jsou všechny jednotky měn data na síti či na úložišti, může snadno dojít k jejich ztrátě, či odcizení. Zdrojový kód nebo šifrovací protokol je prolomitelný vždy.
Nejvíce však záleží na uživateli, jak si svá data ochrání, zejména kam si uloží své soukromé klíče (cloud, USB disk – u obojího je možnost odcizení nebo selhání).

4. Manipulace

Mnoho měn má velké množství svých jednotek ve vlastnictví několika málo lidí (tvůrců a jejich nejbližších společníků). Tito vlastníci mají kontrolu nad zásobami jednotek měny a mohou tak manipulovat s cenou.

5. Složitá směna za měnu s nuceným oběhem

Obecně mají ty největší měny, tedy takové s největším tržním podílem v dolarech, vyhrazené online směnárny za fiat měnu (měnu s nuceným oběhem). Méně oblíbené měny tuto možnost přímé směny nemají. Před směnou za peníze je třeba je vyměnit za měny největší, které přímou směnu mají vyhrazenou na internetu. Tím je potlačena poptávka po těchto menších měnách.

6. Omezená, či žádná možnost vrácení prostředků

Kryptoměny nemají žádnou kontrolu stran transakcí, pouze jejich správnosti, k čemuž slouží těžaři jako prostředníci. Takováto kontrola by porušovala decentralizovanou povahu. V praxi to znamená, že pokud je zaplaceno (transakce je nevratná) a její odesílatel byl podveden, není možnost obrany.

Některé měny se snaží adresovat tento problém, ale jeho řešení je stále nekompletní a neověřené praxí.

Informace pro obě předchozí kapitoly byly čerpány z [49].

### 3.3.10 Vývoj do budoucna

Kryptoměny byly vytvořeny, aby fungovaly vně kontroly státu a tato skutečnost přitahuje zájem subjektů nevěřících centrálním bankám.

Například v zemích s hyperinflací je bitcoin používán jako hlavní prostředek směny, díky jednoduchosti transakcí a stabilitě sítě na rozdíl od měn s nuceným oběhem v těchto zemích.

Na druhou stranu jsou kryptoměny stále zmítány problémy. Nemohou být použity v národním měřítku, protože podporují málo transakcí za určitý časový úsek (bitcoin podporuje 7 transakcí za vteřinu) naopak síť VISA dokáže zpracovat 65000 transakcí za vteřinu. Dalším důvodem, proč nemohou být kryptoměny do budoucna použity je právě absence jejich regulace a tím způsobená velká fluktuace ceny za jednotku. Bitcoin v tomto roce dosáhl až k 19000USD za jednotku a během týdne klesl až k 15000USD. [11]

Následující graf ukazuje vývoj ceny bitcoinu, kde maxima dosáhl v prosinci. Měna není regulována, a tudíž například větší emise znamenají velký pokles ceny.


*Graf 3-cena bitcoinu v roce 2017 [13]*

I přes všechny tyto problémy budou kryptoměny stále více přijímány jako běžné platidlo. Také například nadnárodní společnosti vytvořily své vlastní kryptoměny (Kodak a Telegram) a roste počet bank, které uvažují o zavedení technologie blokchain, na které by mohla běžná měna fungovat.

V budoucnu je tedy možné, že nynější vliv kryptoměny bude mít za následek transformaci měn ve virtuální a zmizí například papírové peníze. Tato změna podpoří bezpečnost transakcí. [12]

Například v Estonsku už vzniká takováto národní kryptoměna jako součást nového programu *e-Obyvatel*. Při zavedení centralizované kryptoměny by pak klesly poplatky u bank a převody peněz se zrychlily.

Jak je zmíněno v kapitole nevýhod, kryptoměna má za následek zvýšení kriminální aktivity (díky anonymitě). Tento problém u národních měn odpadá díky možnosti sledovat uživatele, protože by měna byla centralizovaná a blockchain pod kontrolou centrální banky (proti filozofii kryptoměn). [11]

# 4 Vlastní práce

V této části práce bude řešena těžba měny, její výhodnost vůči spotřebě elektrické energie a vloženým finančním prostředkům. Také bude vysvětleno, jak měnu získat jiným způsobem a jak s ní nakládat. Těžba bude testována z pohledu běžného uživatele vlastnícího domácí počítač, tak z pohledu cíleného využití specializovaného hardwaru. Těžba měny pomocí domácího počítače je realizována pomocí vlastního hardwaru a těžba pomocí specializovaného hardwaru je zprostředkována pomocí získaných informací z praxe od anonymního zdroje.

Pro těžbu byla vybrána měna představená v teoretické části a tou je Ethereum. Důvod upřednostnění před jinými měnami je menší složitost těžení na grafických kartách, a tudíž možnost lepší demonstrace na spotřebitelském hardwaru. Také těžba na specializovaném hardwaru je prováděna v síti měny Ethereum.

## 4.1 Ethereum

Měna je nyní ve verzi 1.0 a předpokládá se, že ve verzi 1.1 přejde na Proof-of-Stake model a tím zanikne těžba v její síti. Než se tak stane, je možné v síti těžit například pomocí proof-of-work algoritmu Ethash.

### 4.1.1 Ethash

Tento algoritmus je modifikovaný *Dagger-Hashimoto* a cílí na splnění dvou úkolů:

1. **ASIC-vzdorný:** výhoda specializovaného obvodu pro Ethash by měla být co nejmenší, aby právě uživatelé se spotřebitelským hardwarem měli možnost přispět do sítě.
2. **Ověřitelnost klientem:** blok by měl být relativně efektivně ověřitelný jednoduchým klientským programem.

S další změnou můžeme specifikovat také třetí úkol, pokud je třeba, ale s nárůstem složitosti výpočtů.

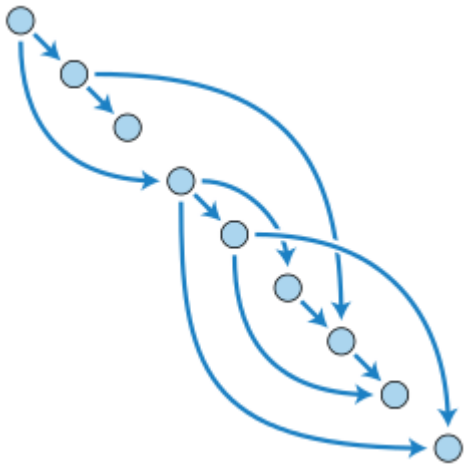
3. **Uložení celého blockchainu:** těžba by měla vyžadovat uložení stavu celého blockchainu

Dagger-Hashimoto je složen ze dvou algoritmů:

- Hashimoto algoritmus vytvořený Thaddeem Dryjou, který se snaží docílit ASIC-vzdornost díky tomu, že je orientovaný na V/V, tedy činí zápisy a čtení z/do paměti limitujícím faktorem těžení. Takto splňuje úkoly 1 a 3 uvedené výše, jelikož používá paměť pro uložení stavu blockchainu a je tím také do jisté míry zmenšena výhoda ASIC jednotek.
- Dagger byl vyvinut Vitalikem Buterinem a používá acyklický orientovaný graf (Directed Acyclic Graph) pro docílení paměťově náročných výpočtů, ale zároveň paměťově jednoduché validace. [7]

**DAG**

DAG je přibližně 1GB velký, náhodně generovaný dataset, který tvoří acyklický orientovaný graf (z algortimu Dagger). Takovýto graf je konečný, orientovaný a neobsahující žádné cykly. Příklad takového grafu je vidět na obrázku:



*Obrázek 5 - acyklický orientovaný graf [10]*

Tento graf je generován každou *epochu* (30 000 bloků nebo 100 hodin). Ethash očekává DAG jako dvou-rozměrné pole celých čísel s rozměry [n x 16], kde n začíná na 16777186 a odtud se zvětšuje. Posléze je vše zapsáno do souboru uloženém u klienta.

Na tomto vygenerovaném datasetu pak klient řeší výpočetní problém, z části odvozený z hashe hlavičky bloku. [9]

Algoritmus pak probíhá následovně:

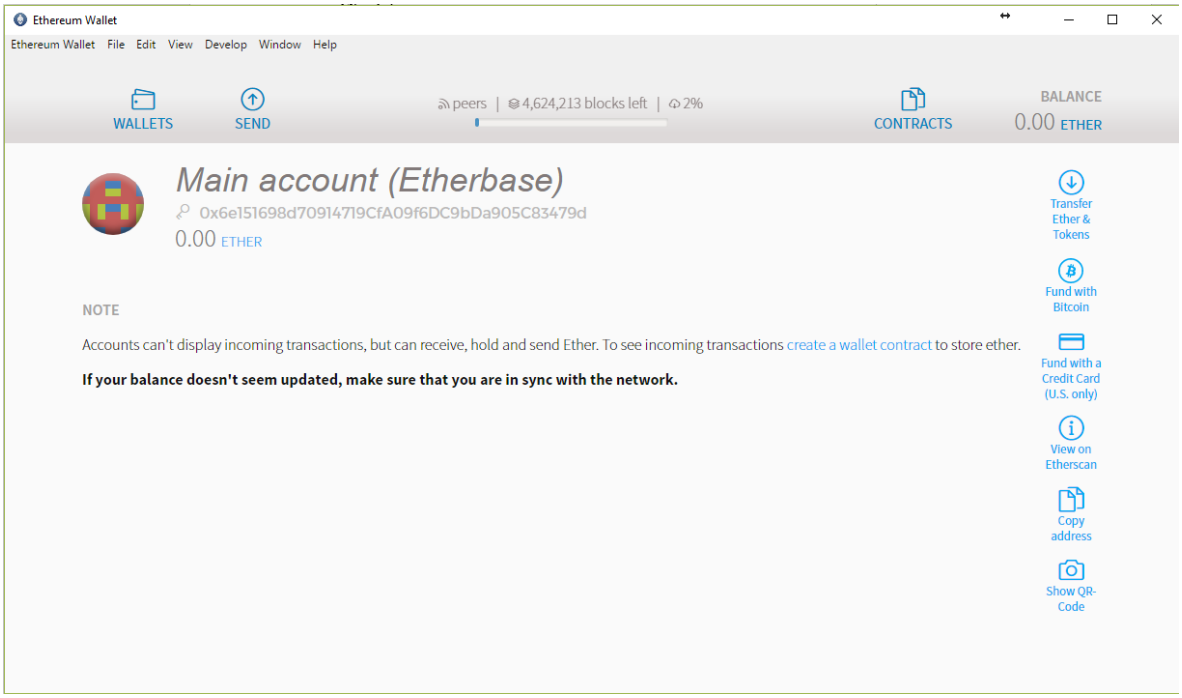
1. Existuje **počáteční hodnota (seed)**, která může být spočítána skenováním hlaviček bloku
2. Z této hodnoty je možné vygenerovat **16MB pseudonáhodnou vyrovnávací paměť(cache)**
3. Z této hodnoty je vygenerován **1GB dataset**, kde každá položka závisí na malém počtu položek z paměti vygenerované v bodu 2
4. Těžba pak probíhá s náhodnými částmi datasetu a vytvořením hashe z nich. Ověření není paměťově náročné, jelikož je použita cache pro znovu nalezení konkrétních částí datasetu a tudíž je třeba uložit jen cache z bodu 2 [8]

## 4.2 Těžba na spotřebitelském hardwaru

Těžbu lze provádět na jakémkoli počítačovém hardwaru, který je schopen provádět aritmetické operace výpočtu hash funkcí, tedy takový, který obsahuje alespoň jednu aritmeticko-logickou jednotku,

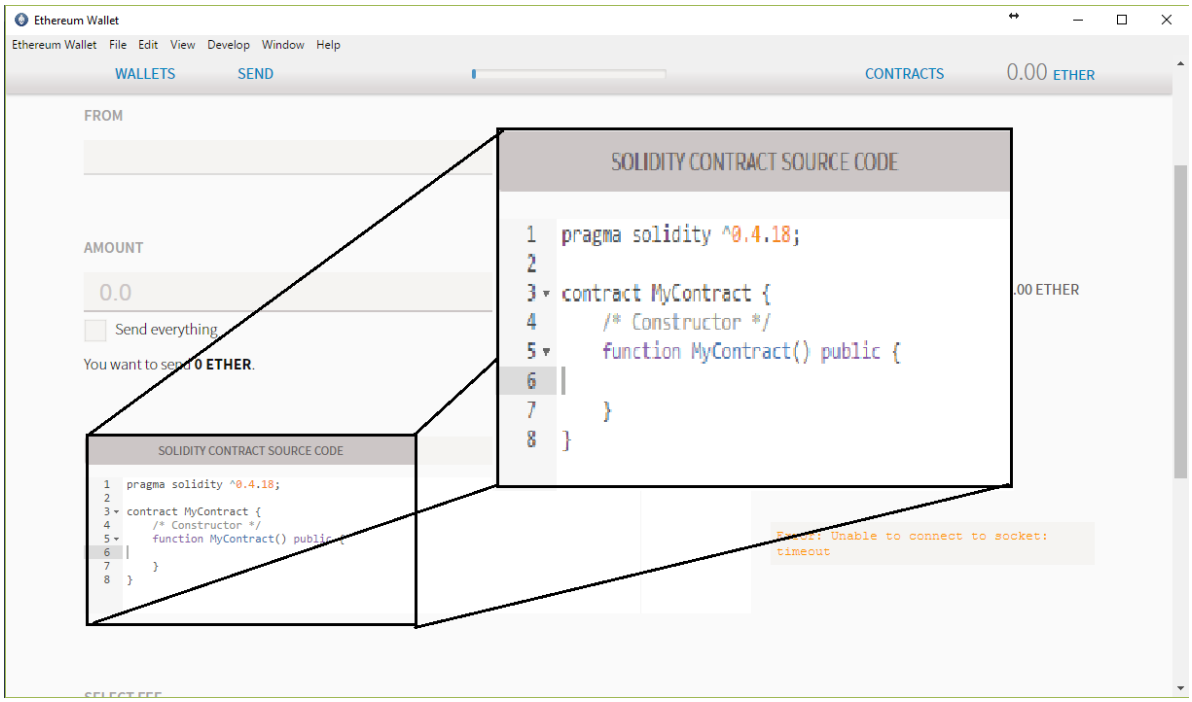
Pro těžbu v síti měny ethereum je nejdříve potřeba založit si peněženku, která je dostupná jako volně stažitelný software na stránce www.ethereum.org a nainstalovat jej.

Po instalaci a spuštění dojde k synchronizaci sítě a založení adresy peněženky na kterou lze převést prostředky jak vytěžené, tak získané pomocí transakcí, respektive smart contractů.




*Obrázek 6 - úvodní obrazovka programu Ethereum wallet (autor)*

Peněženek je pak možno vytvořit více a také je možné programovat rovnou v aplikaci vlastní smart contracty.




*Obrázek 7 - možnost naprogramování vlastního smart contractu (autor)*

### 4.2.1 Pooled a solo mining

*Solo mining* znamená, že uzel provádí výpočty v síti sám, bez připojení do poolu. Všechna odměna za nalezené bloky je připsána uzlu samotnému.

Výhody solo miningu:

- Nezávisí na provozovateli poolu, tudíž není zatíženo případnými výpadky
- Neúčtují se poplatky, uzlu připadne celá odměna za nalezený blok

Nevýhody solo miningu:

- Energeticky nevýhodné
- Nestálý příjem

Oproti solo, *pool mining* je těžba ve skupině uzlů (*poolu*), který sdružuje jejich sílu. Tyto uzly pak společně řeší výpočty a pokud je nalezeno řešení bloku, je odměna za něj rozdělena po zúčastněných uzlech.

Jako důkaz, že je uzel zúčastněn těžby slouží tzv. *share*, což je řešení bloku, který má nastavenou menší složitost, než je takový blok, který lze v určitou chvíli připojit do blockchainu. Uzel tyto *shares* posílá do poolu (pool musí být příjemce). Samozřejmě při takovém těžení může dojít k nalezení takového share, který může být řešením a ten je poolem vložen do blockchainu a odměna za něj je rozdělena. [55]

Výhody pool miningu:

- Stálý příjem
- Možný vyšší příjem díky *long pollingu* (zprávy od poolu, že blok byl vyřešen a tím se na něm dále nepracuje)

Nevýhody pool miningu:

- Výpadky postkytovatele poolu
- Při účtování poplatků může být příjem nižší
- Možnost útoku na pool

Kapitola o pool a solo miningu byla čerpána z [6].

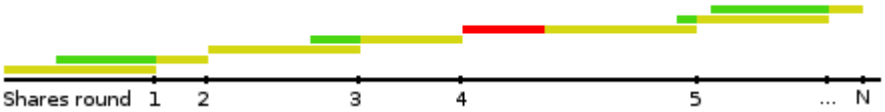
### 4.2.2 Použitý software a pool

Po nastavení peněženky je třeba stáhnout speciální program a dávkový soubor pro jeho spuštění a tím připojení stroje do sítě. Jelikož jde o těžení na spotřebitelském hardwaru (jedna grafická karta), použijeme program pro připojení do poolu. Pokud by těžení probíhalo

jako solo uzel, jedna grafická karta by v řešení hashe soupeřila se všemi uzly, což není výhodné. Nevznikají také skoro žádné čitelné statistiky o těžení a tudíž nelze příliš měřit výhodnost a výnosnost těžby.

Pool, na kterém probíhá těžba se nazývá ethermine.org. Tento pool používá PPLNS (Pay Per Last Number of Shares) systém výplat, což znamená, že odměna je vyplácena ne podle odevzdaných podílů (shares) v kole (doba mezi dvěma nalezenými bloky), ale podle posledních N podílů, kde N je číslo stanoveno různými metodami (fixní, či dvojnásobek složitosti atd.). [5]

Následující obrázek použití PPLNS popisuje:




*Obrázek 8 - započítané podíly podle PPLNS [5]*

Čísla znamenají jednotlivá kola a N na konci osy znamená stanovený počet kol. Zelené úseky jsou započítány do dalšího kola (tedy dvakrát, protože podíly z předchozích kol se vejdou do N podílů toho kola – kolo 1 a 3). Oproti tomu kolo 5 bylo dlouhé a počet podílů byl vyšší, tudíž nejsou započítány starší podíly (červená barva). Stanovený počet shares je na obrázku žlutou barvou.

Dále poskytuje informace o přesné výši hashratu (aktuální, průměrnou), výplaty jsou okamžité, je možné nastavení prahu výplat (min 0.05ETH, max 10ETH), poplatky jsou jednoprocentní a jsou zaznamenávány detailní statistiky. [5]

Pro těžbu byl použit program ethminer dostupný z www.github.com/ethereum-mining/ethminer/releases a pro spuštění musel být nastaven dávkový soubor, který obsahuje hlavní spouštěcí kód:

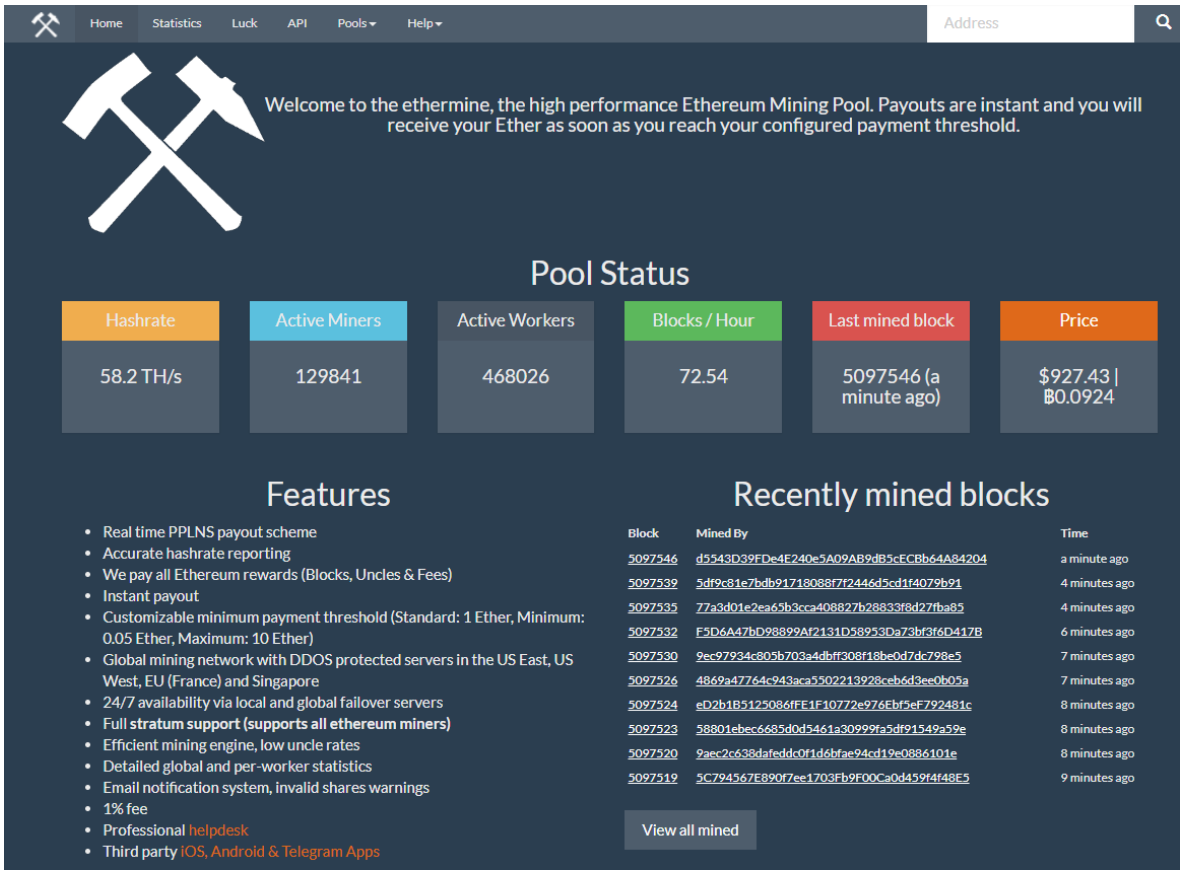
```
1) ethminer.exe –farm-recheck 200 -G -S

2) eu1.ethermine.org:4444 -FS

3) us1.ethermine.org:4444 -O

4) <Your_Ethereum_Address>.<RigName>
```

1. Spuštění programu ethminer
2. Hlavní server na kterém běží pool
3. Záložní server
4. adresa uzlu . název stroje

Předtím je také vhodné nastavit program, aby grafickou kartu využil na plný výkon:

```
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
```

Na následujícím obrázku je hlavní stránka poolu ethermine.org, kde jsou zobrazeny informace o kombinované hashrate, aktivních těžařích (uzlech), celkový počet jejich strojů, kolik je vytěženo bloků za hodinu a číslo posledního vytěženého bloku, před jakou dobou byl vytěžen a jaký je aktuální kurz vůči dolaru a bitcoinu.




*Obrázek 9 - stav ethermine poolu*

### 4.2.3 Hardware

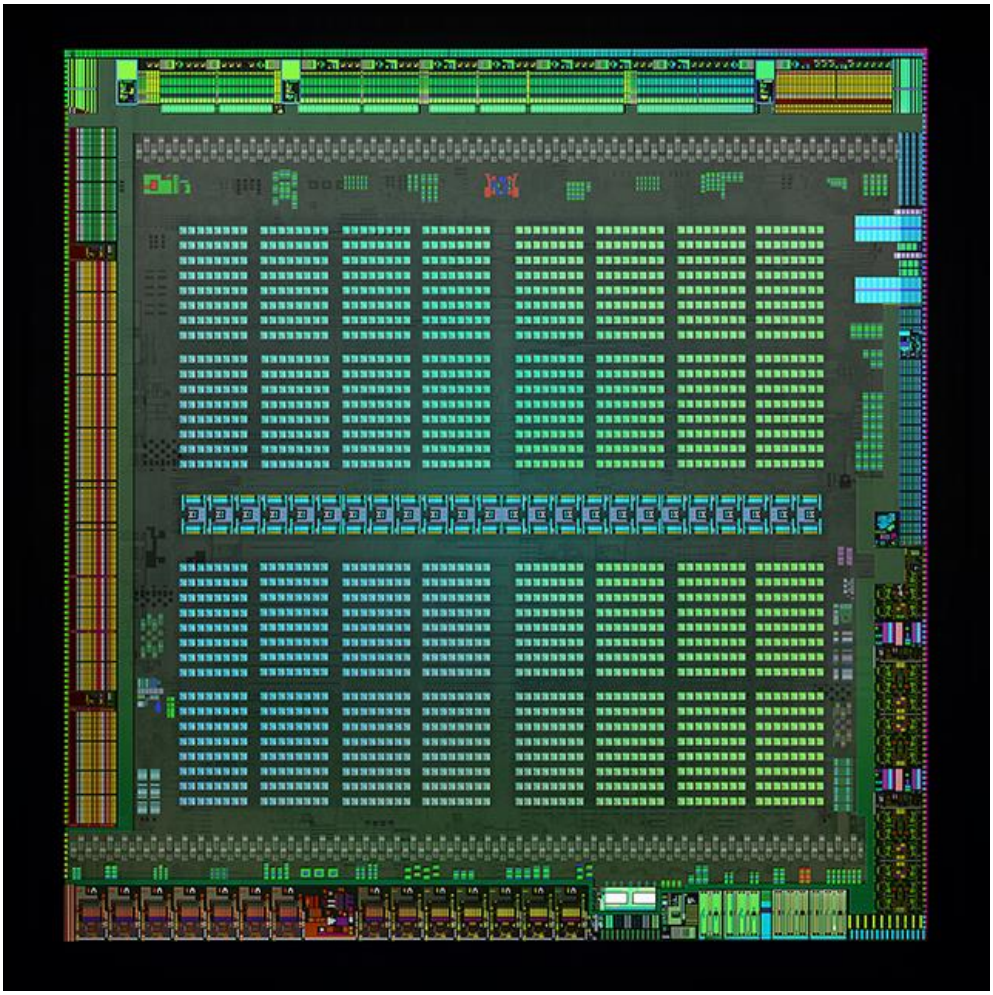
Použitý hardware je součástí domácích počítačů a je to vše co je k těžení ve smyslu hardwaru potřeba. Těžit se dá i na CPU, ale hashrate není vysoká, a tudíž se těžba nevyplatí vůbec, vzhledem ke spotřebě elektřiny. Existuje ale měna optimalizována přímo na CPU výpočty, Monero.

Konfigurace PC je následující:

- Procesor: Intel Core i5 6400 @ 2,7GHz s udávanou spotřebou 65W
- RAM: 8GB DDR4 2400MHz
- Základní deska: Asus B150M, socket 1151 Skylake
- Zdroj: Enermax Liberty ELT500AWT, 500W
- Systémový disk: Intel SSD 540s, 120GB, SATAIII

**NVidia GeForce GTX 970**

První grafickou kartou použitou k těžbě na osobním počítači je karta od firmy MSI s čipem nVidia GTX970 na architektuře Maxwell. Karta byla vydána v roce 2014 a čip GM204 je vyroben 28nm procesem s 5,2 mld. tranzistory. Tato grafická karta byla pořízena v roce 2017, prodej byl zprostředkován přes server bazos.cz a pořizovací cena činila 4500kč.

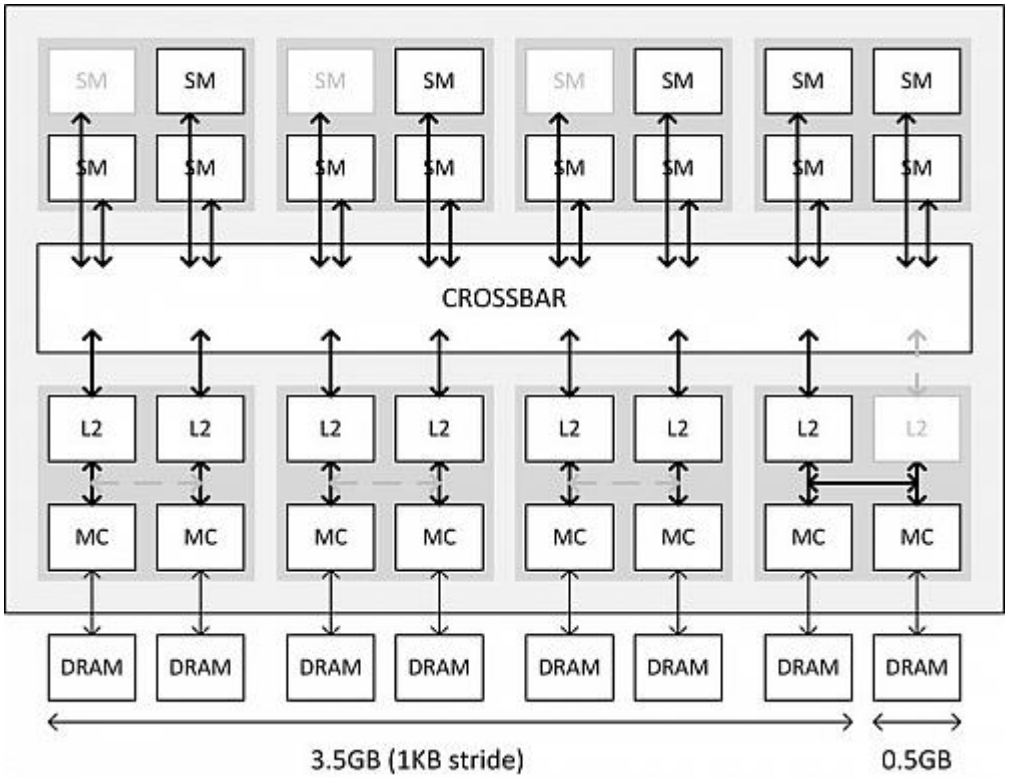


*Obrázek 10 - čip Maxwell*

*Specifikace*

Karta obsahuje 1664 jednotek CUDA (streaming procesory, výpočetní jádra) oproti plným 2048 jádrům z čipu karty GTX980. Dále obsahuje 104 texturovacích jednotek a 56 ROPs (Render Output Unit, renderovací jednotka).

NVidia v oficiálním oznámení karty uvedla rednerovacích jednotek 64, jenže osmina z nich je vypnutá, přestože řadiče pamětí jsou aktivní všechny. Tudíž bloků s ROPs je 7, ale řadičů paměti je 8. Jelikož vypnutí renderovacích jednotek s sebou nese vypnutí paměťového řadiče a tím zmenšení sběrnice na 224 bitů z 256. Následující obrázek situaci popisuje. [22]




*Obrázek 11 - řešení při vypnutí ROP bloku u Maxwellu [22]*

Pokud je blok vypnut, karta by měla obsahovat pouze 3,5 GB paměti, nVidia však osadila celých 4 GB. Posledních 512 MB je napojeno zvláštní cestou a jejich využití výrazně zpomaluje chod grafické karty. Tato paměť je typu GDDR5 a jejich propustnost je 224,4 GB/s při taktu 1753 MHz (7012 MHz efektivně – vynásobeno 4), přičemž jde o takt z výroby. [3]

Rychlost jádra je implicitně nastavena na 1050MHz a při vytížení stoupá na 1178 MHz (tzv. Boost Clock). Výkon v plovoucí řadové čárce je 3,9 TFLOPS. Udávaná spotřeba karty při 100 % vytížení je 145 W. [4]


*Obrázek 12 - MSI GeForce GTX970 Gaming 4G (autor)*

### *Takty, teploty a spotřeba*

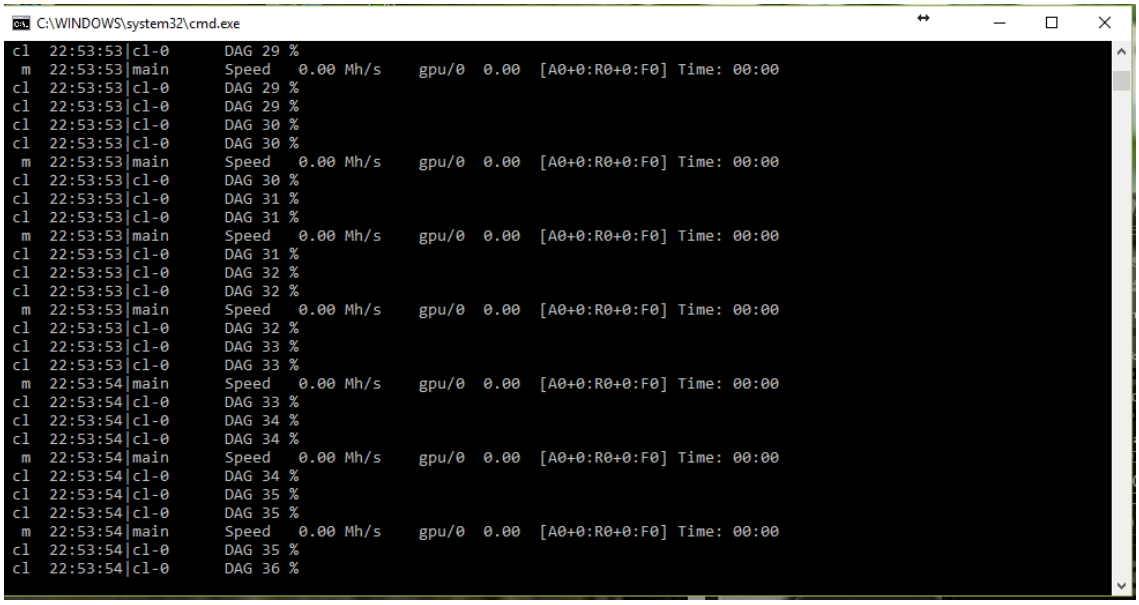
Takty jádra a pamětí uvedené výše nejsou konečné. Výrobce tyto takty, s použitím adekvátního chladiče, může navýšit. Karta od firmy MSI je od výroby nastavena na 1114 MHz na jádře a 1750 MHz na pamětech.

Pro navýšení výkonu a hashrate lze tyto takty ještě zvýšit. Každé jádro dosáhne limitu frekvence na jiné hodnotě. Pro nastavení taktů a přetaktování (zvýšení frekvence nad nastavenou z výroby) byl použit program MSI Afterburner, který dovolí měnit takty i při chodu aplikace závislé na grafické kartě (3D aplikace, výpočetní aplikace).
Program pak ukazuje důležité informace na nastaveném profilu (limity výkonu, teploty, nastavení taktování a rychlost ventilátorů). Na kruhových panelech je pak zobrazena teplota vpravo a takty vlevo. Níže jsou pak uvedeny nastavitelné grafy monitorování stavu grafické karty.


*Obrázek 13 - program MSI afterburner a informace o grafické kartě (2D, klidový režim, zdroj: autor)*

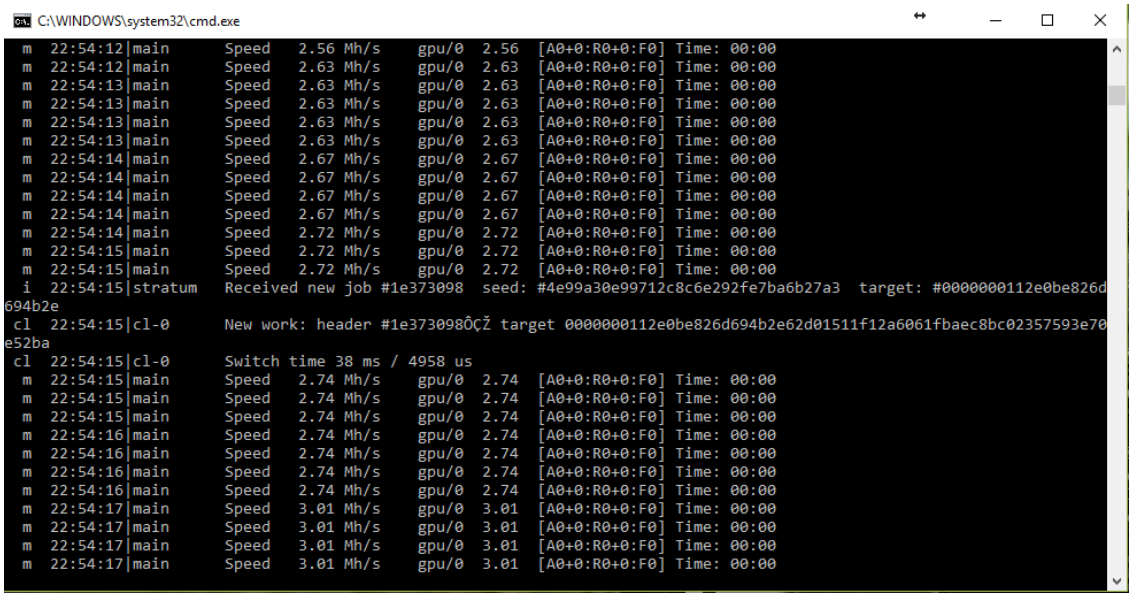
*Těžba a hashrate*

Při spuštění programu v příkazové řádce se nejprve nastaví hodnoty na využití grafické karty (viz hodnoty dávkového souboru v kapitole Software) a je nutné vygenerovat DAG (kapitola DAG).



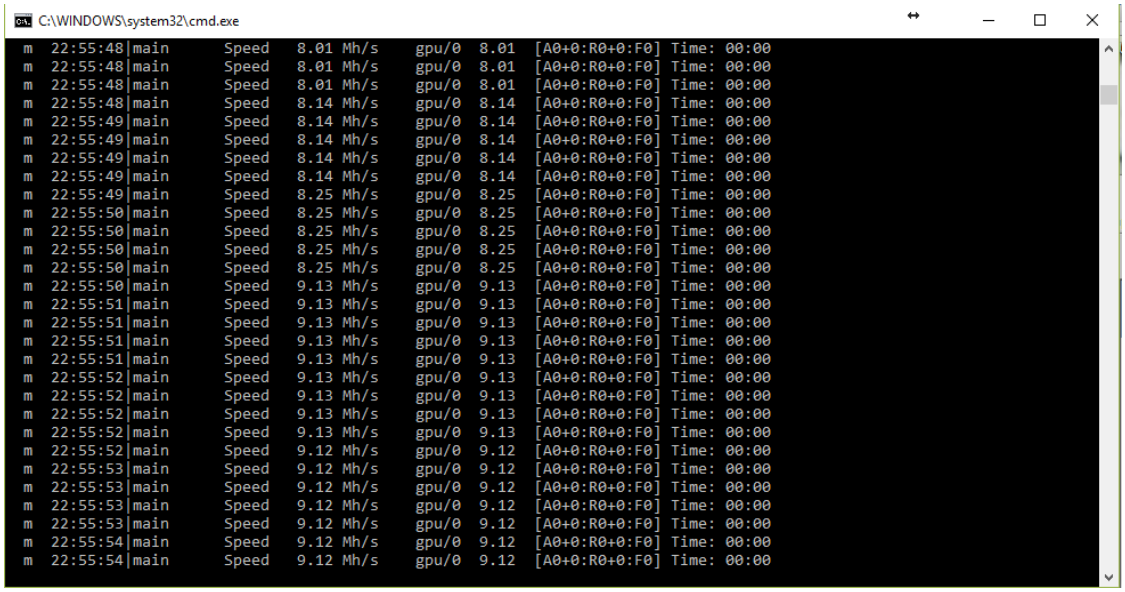

*Obrázek 14 - generování DAG (autor)*

Po prvním, testovacím spuštění se hashrate pohybovala kolem 2-4 MH/s, ale podle ostatních uživatelů s totožnou grafickou kartou by měla být mnohem vyšší. Díky informacím na fórech se problém podařilo opravit.



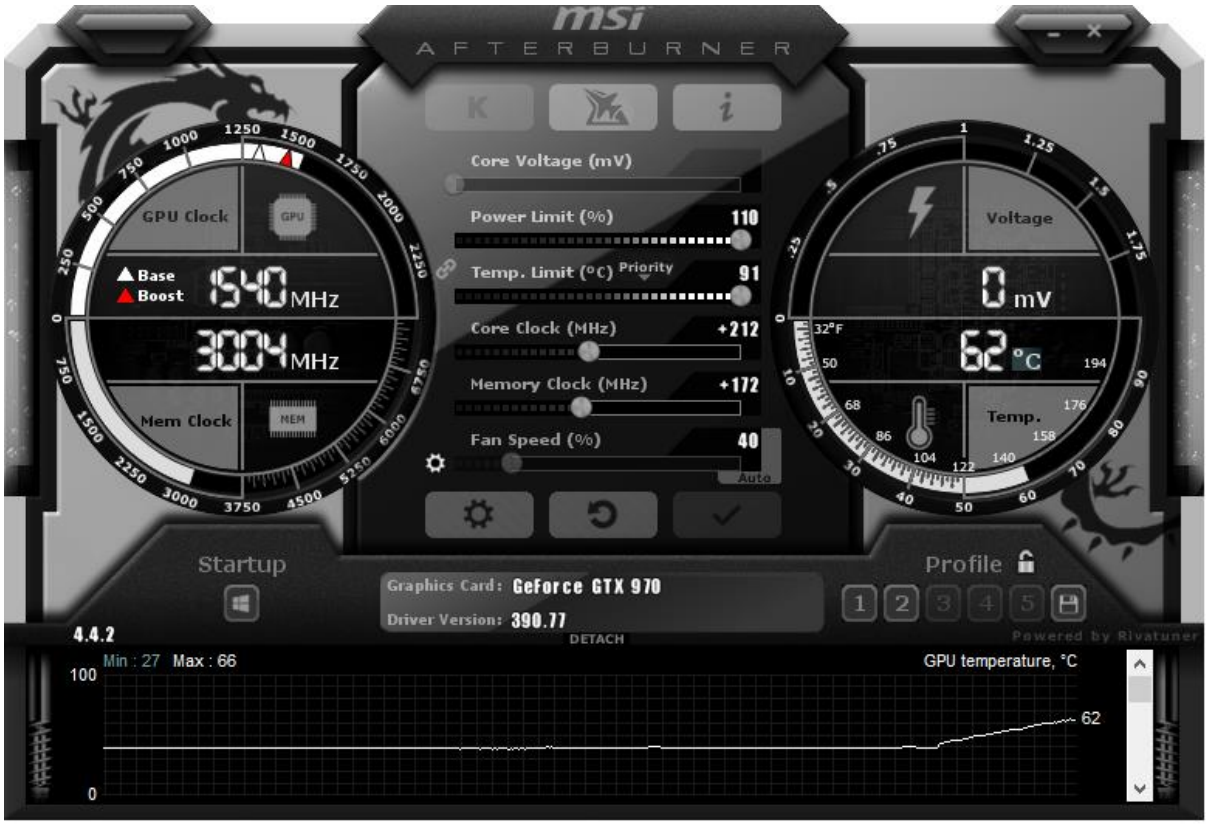

*Obrázek 15 - těžba s nízkou hashrate (uprostřed je přiřazení práce na novém bloku, zdroj: autor)*

V nastavení grafické karty (panel nVidia) postačilo nastavit atribut, který čip optimalizoval pro výpočetní výkon. Po tomto nastavení již hashrate dosahovala hodnot korespondujících s výkonem karty a složitostí, která se průměrně pohybuje okolo 8-12 MH/s




*Obrázek 16 – těžba (autor)*

Na následujícím obrázku lze vidět vytížení grafické karty při provádění těžby.

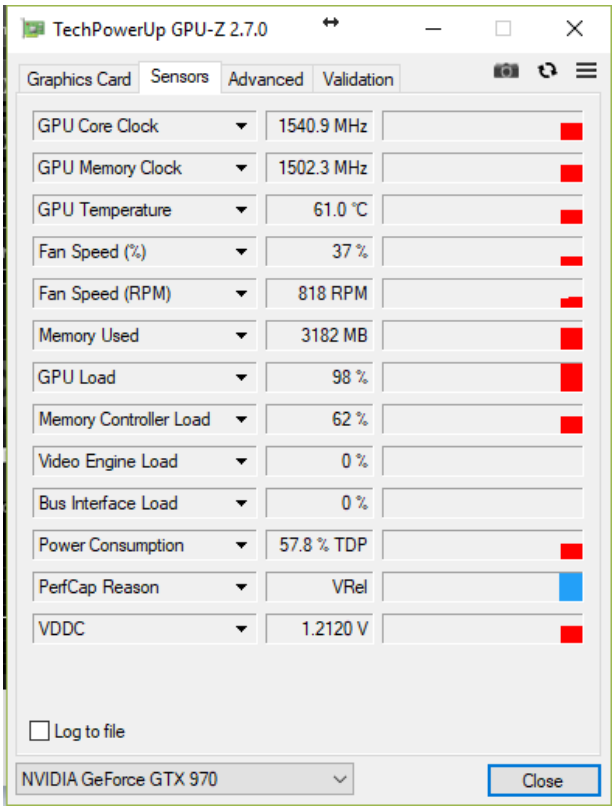



*Obrázek 17- zatížení grafické karty těžbou (autor)*

Takty jsou nastaveny na 1540 MHz (+212 MHz oproti továrnímu nastavení) a paměti na 3004 MHz (+172 MHz, MSI Afterburner ukazuje poloviční rychlost oproti efektivní). Zvláštní je údaj s paměťmi, které by při plném zatížení měly mít frekvenci 1839 MHz, což

je 7356 MHz efektivně, ale pravděpodobně nedojde k jejich plnému vytížení. Program GPU-Z od společnosti TechPowerUp ukazuje hodnoty pamětí na 1502,3MHz (6008MHz efektivně), což je stejný údaj.

Další hodnoty, které jsou třeba zmínit je Power Consumption, spotřeba energie, která dosahovala přibližně 60 % TDP, což je údaj udávající hodnotu vyzářeného tepla ve wattech, které může podle výrobce daný čip vyzářit a je třeba toto teplo odvést chladičem (Thermal Design Power). Karta GTX970 má hodnotu udávanou výrobcem stanovenou na 145 W, tudíž spotřeba samotné karty byla při těžbě 87 až 100 W. Důležitější je ale spotřeba celé sestavy, která byla také měřena. Teplota nedosahuje při těžení více než 62 °C při napětí 1,210 V na čipu karty. Měnit napětí na čipu karty je nutné jen tehdy, když je systém nestabilní.




*Obrázek 18 - program GPU-Z ukazuje stejné hodnoty pamětí (autor)*

**AMD Radeon RX470**

Na druhém osobním počítači je grafická karta od konkurenční firmy AMD, jejíž pořizovací cena v roce 2016 byla 6100 Kč s DPH.

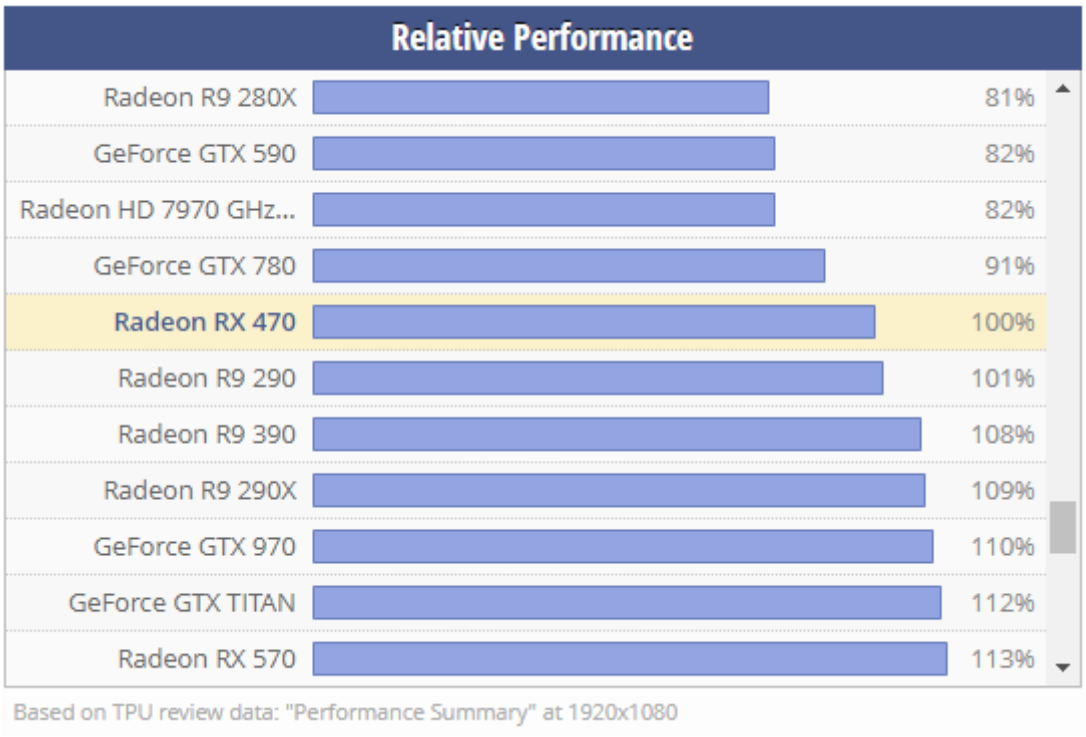
Konfigurace PC:

- Procesor: Intel Core i3-6100 @ 3,7GHz s udávanou spotřebou 51 W
- RAM: 8 GB DDR4 2400MHz
- Základní deska: Asus B150M-A M.2, socket 1151
- Systémový disk: Intel 535 SSD, 240 GB

*Specifikace*

AMD Radeon RX470 je karta středního segmentu vydaná v roce 2016 (o 2 roky novější, než předchozí karta), jejíž jádro Ellesmere s 5,7 miliardami tranzistorů na 14nm výrobním procesu plně podporuje DirectX 12. Oproti nejvýkonnější kartě z řady, RX480, je deaktivováno 256 stream procesorů (2304 a 2048), ale není zde operováno s ROPs (32) jako u předchozí karty, tudíž celá připojená 4 GB GDDR5 paměť běží na rychlé 256 bitové sběrnici. [23]

Z výroby je jádro karty taktováno na 926 MHz a při zátěži je frekvence zvýšena na 1206 MHz. U pamětí je takt nastaven na 1650 MHz (6600 MHz efektivně). Následující obrázek ukazuje porovnání dvou testovaných karet v herním výkonu. Srovnání není sice úplně relevantní s ohledem na zaměření práce, ale v konečném důsledku je velmi zajímavé. [23]




*Obrázek 19 - porovnání relativního herního výkonu karet ze serveru TechPowerUp [23]*

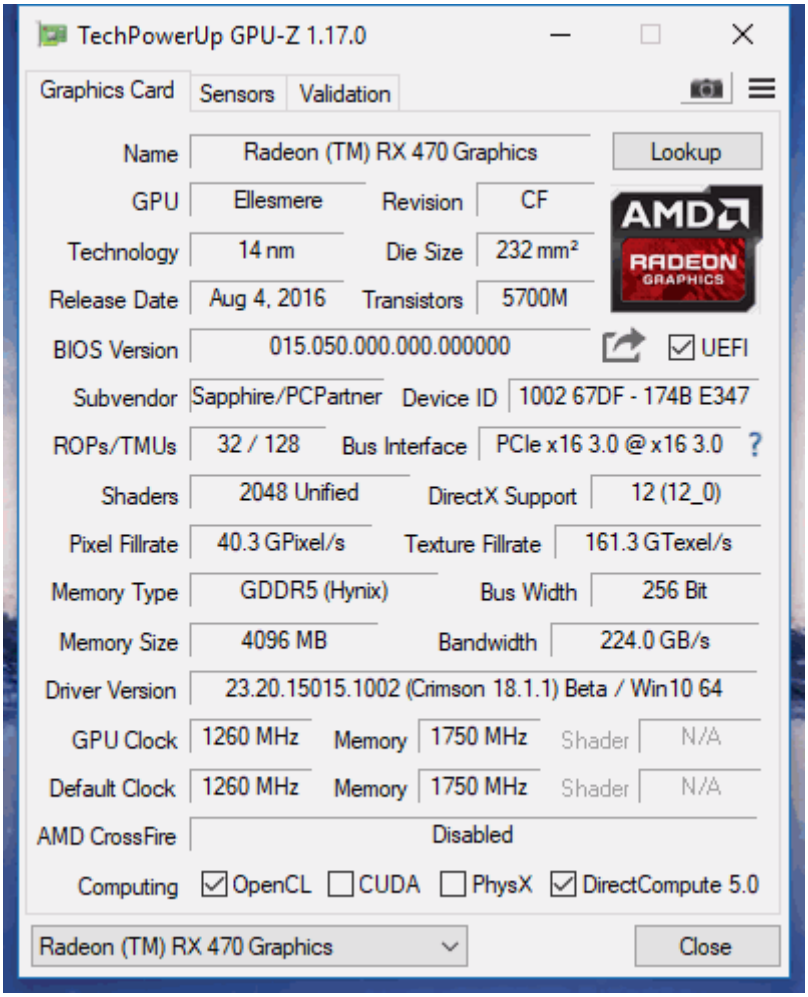
Server uvádí, že předchozí karta je výkonnostně o 10 % lepší, i přesto že její výpočetní výkon v řadové čárce je 4,9 TFLOPS. Těžba ale požaduje jiné výpočty a v těchto jsou AMD karty lepší.

Jelikož je nyní grafických karet velký nedostatek, cena karty se i na bazarech pohybuje velmi vysoko (okolo 7500 Kč s DPH).

Takty teploty spotřeba

Pro těžbu byla využita karta od společnosti Sapphire, Radeon RX470 Nitro 4 GB. Od výrobce byly nastaveny takty na jádře 1260 MHz a na pamětech 1750 MHz (7000 MHz efektivně).


*Obrázek 20 - Sapphire RX470 Nitro (zdroj: Patrik Mička)*




*Obrázek 21 - informace o kartě RX470 z GPU-Z (zdroj: Patrik Mička)*

### 4.2.4 Výsledky

Všechny peněžní částky jsou uvedeny bez DPH, pokud není řečeno jinak.
Příkon sestavy ze sítě byl měřen wattmetrem Solight DT26 s možností nastavit také počet spotřebovaných kWh, což je pro měření výnosnosti těžby nejdůležitější údaj.

**nVidia GTX970**

Následující tabulka ukazuje průměrné hodnoty spotřeby sestavy za určené časové období.

| Karta | příkon (W) | Spotřeba/1 těžba (kWh) | Spotřeba/h (kWh) |
|---|---|---|---|
| nVidia GTX970 | 190,78 | 1,845 | 0,1885 |

*Tabulka 3 - hodnoty spotřeby elektrické energie (autor)*

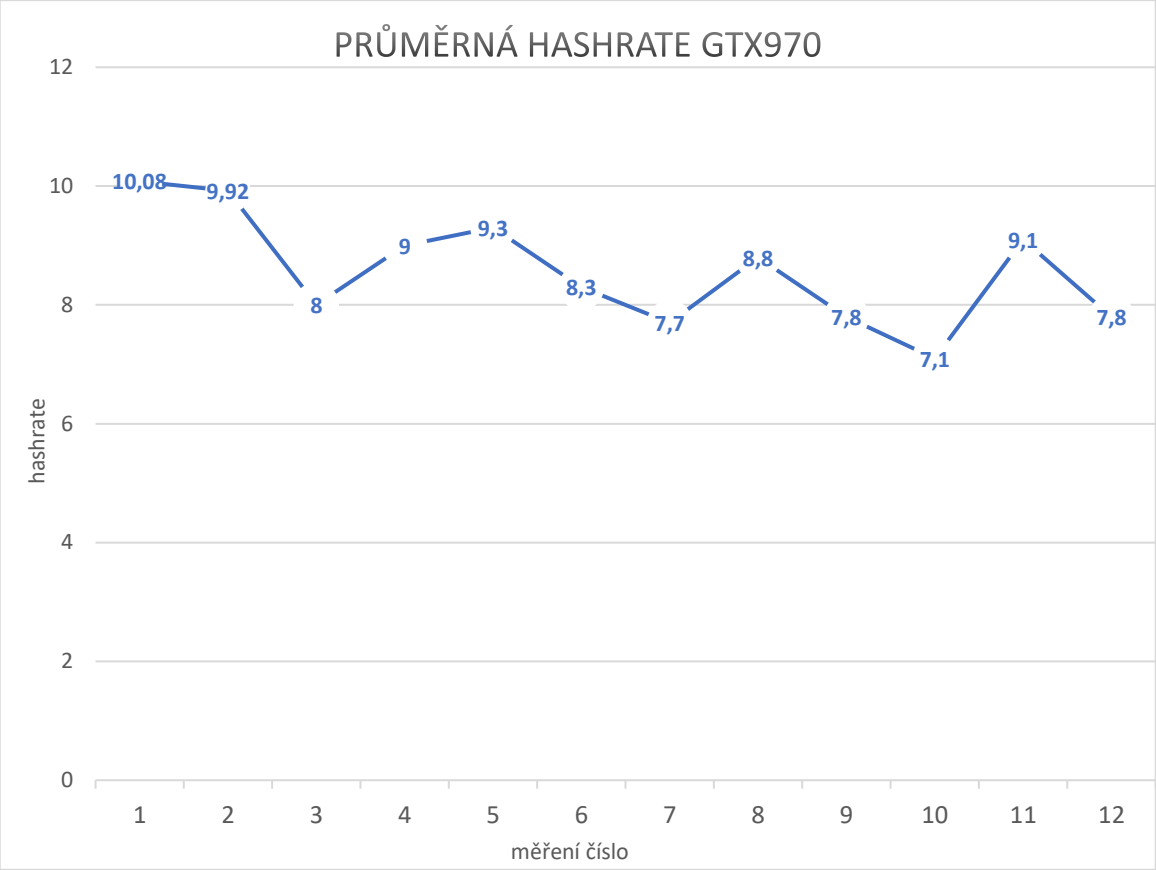
Jedna těžba trvala průměrně 8 hodin a podle spotřeby byla průměrná cena 7,05 Kč s DPH, kde cena za kWh je průměrná cena v České republice, která činí 3,82 Kč/kWh s DPH. [56]

Těžba pak po nastavení grafické karty na výpočetní výkon (zmíněno v kapitole představení hardwaru) vypadala následovně:

| Karta | Vytěženo ETH /1 těžba | Vytěženo ETH / h | Průměrná hashrate | Maximální hashrate |
|---|---|---|---|---|
| nVidia GTX970 | 0,000323 | 0,0000329 | 8,575 MH/s | 18 MH/s |

*Tabulka 4 - výsledky těžby (autor)*

Průběh průměrné hashrate pak znázorňuje následující graf:

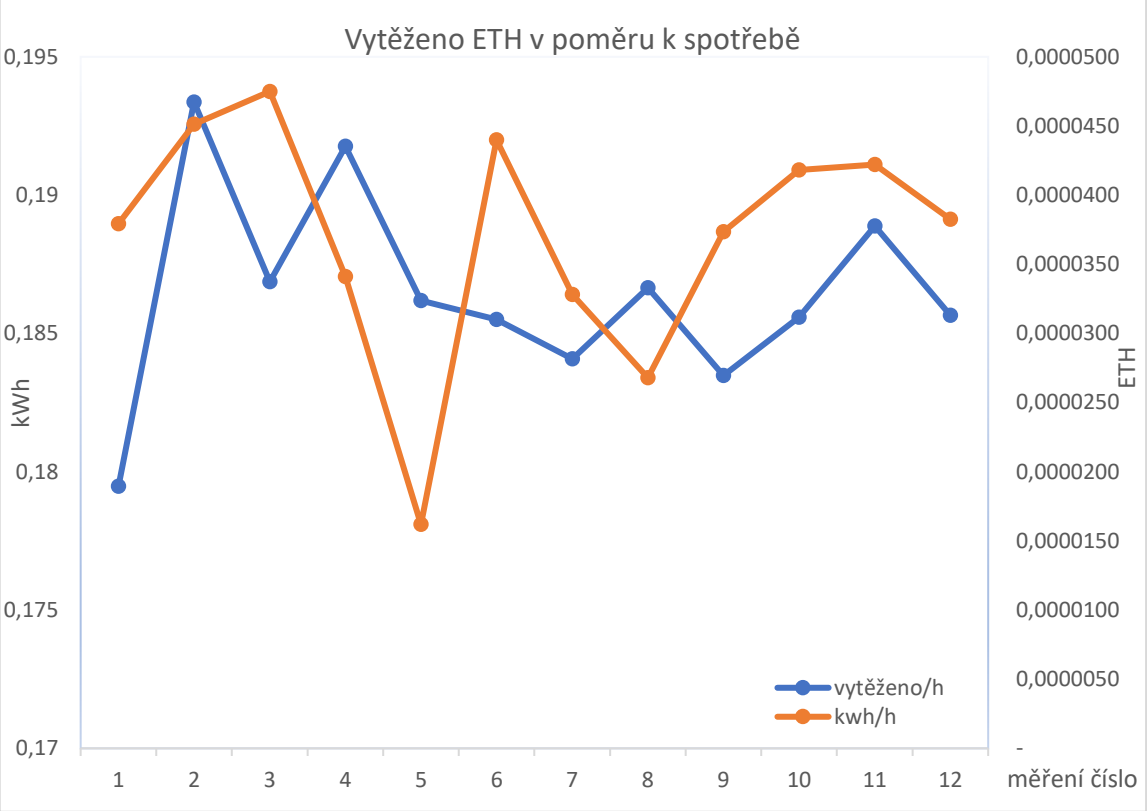



*Graf 4 - průběh průměrné hashrate (autor)*

Při těžbě na spotřebitelském hardwaru je výnosnost velmi závislá na aktuálním kurzu měny, který je díky decentralizované povaze závislý v podstatě pouze na nabídce a poptávce, a tím velmi nestálý. Proto se zisk může proměnit ve ztrátu prakticky v řádech hodin. Důkazem může být propad prakticky všech měn na roční minimum během ledna 2018 (ETH z přibližně 1400 dolarů za jednotku na 600 dolarů za jednotku během jednoho týdne).

Pokud se v poměru porovná spotřeba elektřiny s vytěženou měnou vychází stále spotřeba ve většině případů větší, tedy výnosnost znovu závisí hlavně na momentálním kurzu. Měna za těžbu v poolu je inkasována poměrně stálým tempem, ale může dojít například k zvětšení složitosti. Spotřeba elektřiny osobního počítače může kolísat například v závislosti na procesech běžících na pozadí.

Následující graf tyto skutečnosti zahrnuje:




*Graf 5 - poměr spotřebované elektřiny a vytěžené měny (autor)*

Pokud převedeme skutečnosti na ekonomickou výkonnost, tak při nynějším kurzu je těžba nevýhodná (těžba probíhá při kurzu přibližně 850-870 USD/ETH, což znamená 18000 Kč za jednotku, kurz se rychle mění).

Naopak pokud by byl započítán nejvyšší kurz (1400 USD/ETH, 28500 Kč), je těžba relativně rentabilní. Následující tabulka shrnuje rentabilitu těžby při různých kurzech.

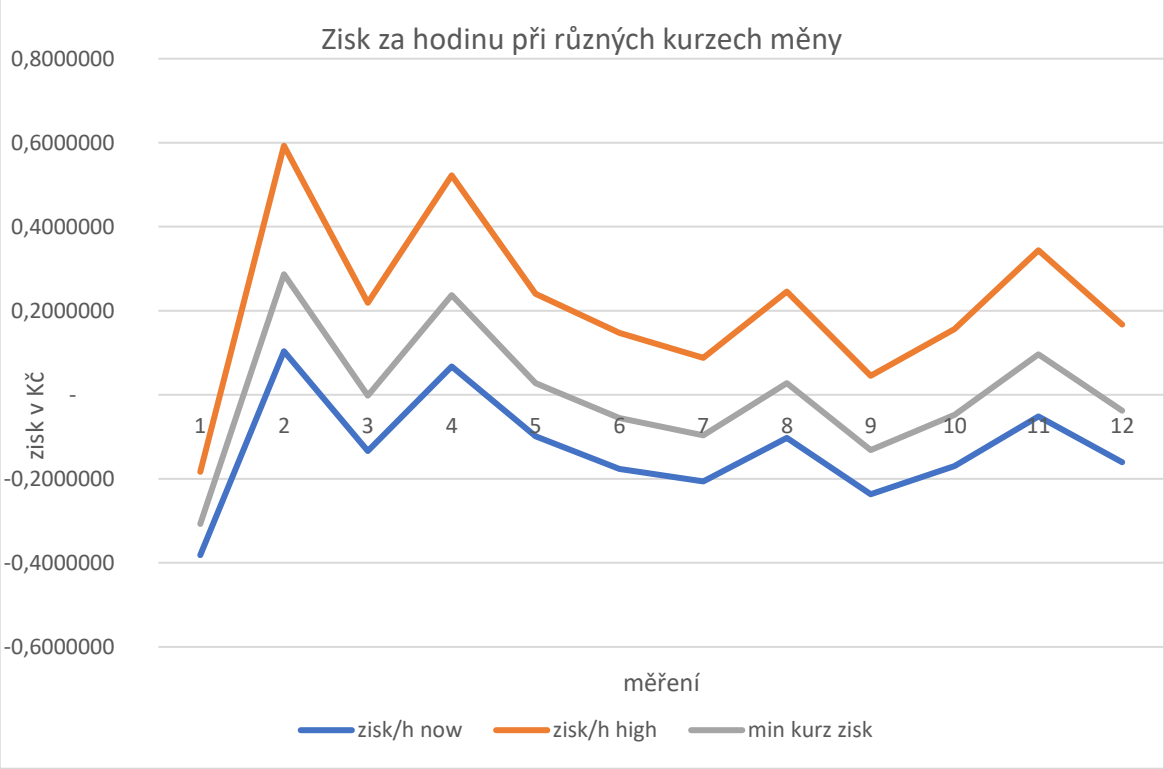
| Karta | Zisk/h nízký kurz (Kč) | Zisk/den nízký kurz (Kč) | Zisk/h vyšší kurz (Kč) | Zisk/den vyšší kurz (Kč) |
|---|---|---|---|---|
| nVidia GTX970 | -0,1290259 | -3,0966215 | 0,2154852 | 5,1716447 |

*Tabulka 5 - ziskovost GTX970*

Při nízkém kurzu je návratnost investice, která zde činila 4500 Kč samozřejmě nemožná, jelikož v průměru karta prodělávala přibližně 3 Kč denně, naopak při nejvyšším kurzu vůči dolaru byl zisk až 14,3 Kč a průměrně tedy 5,2 Kč. Při takovémto kurzu by návratnost investice byla 871 dní, což znamená 2,383 roku. Tento údaj je ale platný pouze, pokud kurz

měny nespadne pod zmíněných 1400 USD za ETH. Pravděpodobnost takto vysokého, a přitom stálého kurzu je nejen u měny Ethereum, ale u všech kryptoměn velmi nízká, a to znamená velkou nevýhodu při těžbě na spotřebitelském hardwaru.

Byl zjištěn také minimální kurz, při kterém by těžba byla rentabilní, tedy v podstatě „bod zvratu“ pro těžbu na aktuální grafické kartě, který se rovná **1058 USD/ETH (21876 Kč)**. Pokud měna dosáhne alespoň tohoto kurzu, začíná být těžba rentabilní. Průběh zisku s různým kurzem měn znázorňuje následující graf.




*Graf 6-průběh zisku při různých kurzech (oranžový – maximální, šedivý - minimální pro rentabilitu, modrý – stávající, zdroj: autor)*

Výnosnost těžby na osobním počítači s grafickou kartou střední třídy je silně závislá na stávajícím kurzu měny, který je velmi nestabilní a podmínka minimálního kurzu pro směnu z těžby činní ne příliš výhodnou činnost.

**RX470**

Následující tabulka ukazuje průměrné hodnoty spotřeby sestavy za určené časové období. Vyšší spotřebu může mít za příčinu například zdroj, který má hůře dimenzované součástky a menší účinnost, tedy poměr příkon/výkon je horší než u předchozího případu. Spotřeba samotné grafické karty horší být nemůže.

| Karta | příkon (W) | Spotřeba/ 1 těžba (kWh) | Spotřeba/h (kWh) |
|---|---|---|---|
| AMD RX470 | 199,4 | 2,39 | 0,1982 |

*Tabulka 6 - hodnoty spotřeby elektrické energie (Patrik Mička)*

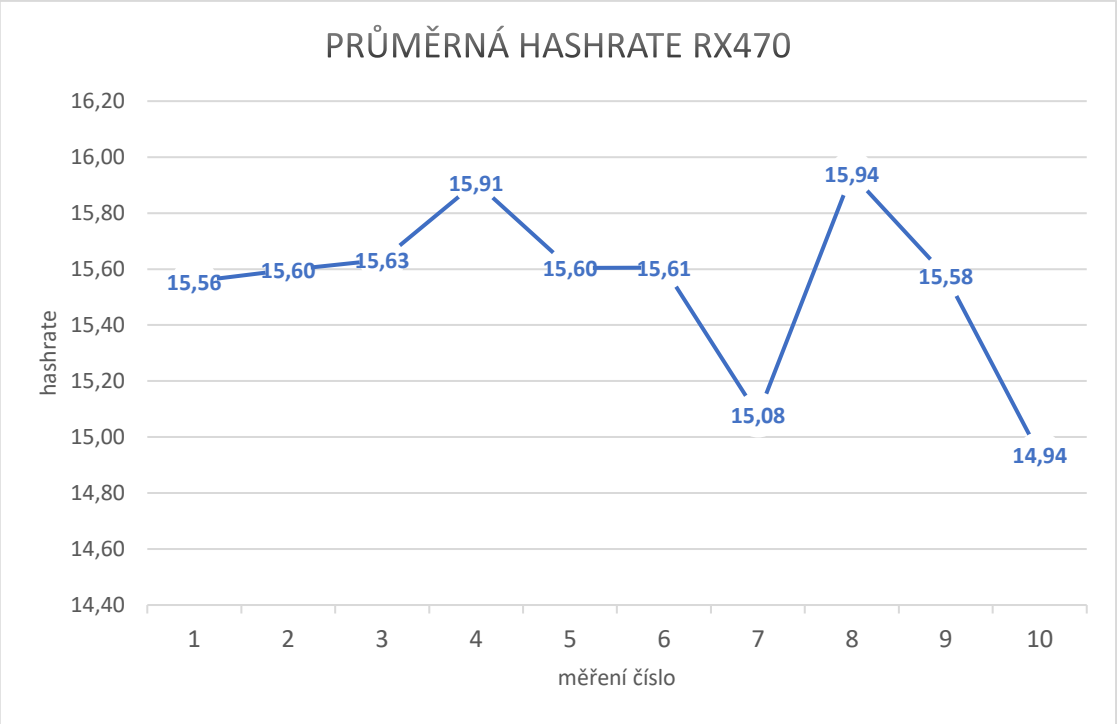
Zde jedna těžba trvala průměrně 12 hodin a podle spotřeby byla průměrná cena 9 Kč s DPH, kde cena za kWh je průměrná cena v České republice, která činí 3,82 Kč/kWh s DPH. [56]

Celková výkonnost karty od firmy AMD je větší, (jak je uvedeno v teoretické části) a průměrná hashrate má mnohem stabilnější průběh, což je určitě dáno architekturou grafického jádra, ale může být také momentálním stavem sítě.

| Karta | Vytěženo ETH /1 těžba | Vytěženo ETH / h | Průměrná hashrate | Maximální hashrate |
|---|---|---|---|---|
| AMD RX470 | 0,000552 | 0,0000468 | 15,5 MH/s | 24,4 MH/s |

*Tabulka 7 - výsledky těžby (Patrik Mička)*

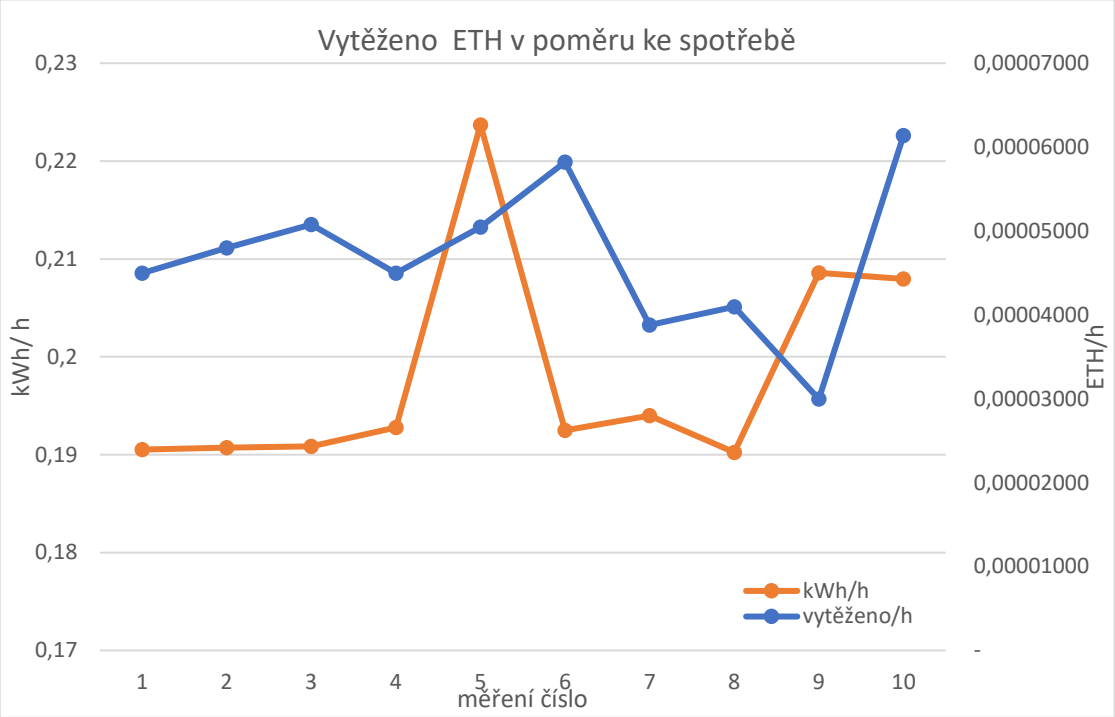
Následující graf ukazuje průběh průměrné hashrate skrze všechna měření. Hodnoty, až na poslední příliš nekolísají. Zhoršení může být způsobeno momentálním zvětšením složitosti na síti měny.




*Graf 7 - průběh hashrate RX470 (Patrik Mička)*

Jelikož je karta od firmy AMD o něco výkonnější i její zisk je při stanovené ceně za kWh (3,82 Kč s DPH) větší a výrazně se liší minimální kurz při kterém začíná být těžba rentabilní.

Následující graf ukazuje skutečnost, že těžba na této kartě v poměru se spotřebou není příliš nevýhodná. Výkyv ve spotřebě může opět znamenat práci počítače na pozadí.




*Graf 8 - poměr spotřeby a vytěžené měny za hodinu*

Pokud by se tyto skutečnosti převedly na ekonomickou výkonnost, tak je těžba při stávajícím kurzu rentabilní, což dokazuje následující tabulka.

| Karta | Zisk/h nízký kurz (Kč) | Zisk/den nízký kurz (Kč) | Zisk/h vyšší kurz (Kč) | Zisk/den vyšší kurz (Kč) |
|---|---|---|---|---|
| AMD RX470 | 0,08417 | 2,02 | 0,5745 | 13,79 |

*Tabulka 8 - ziskovost RX470*

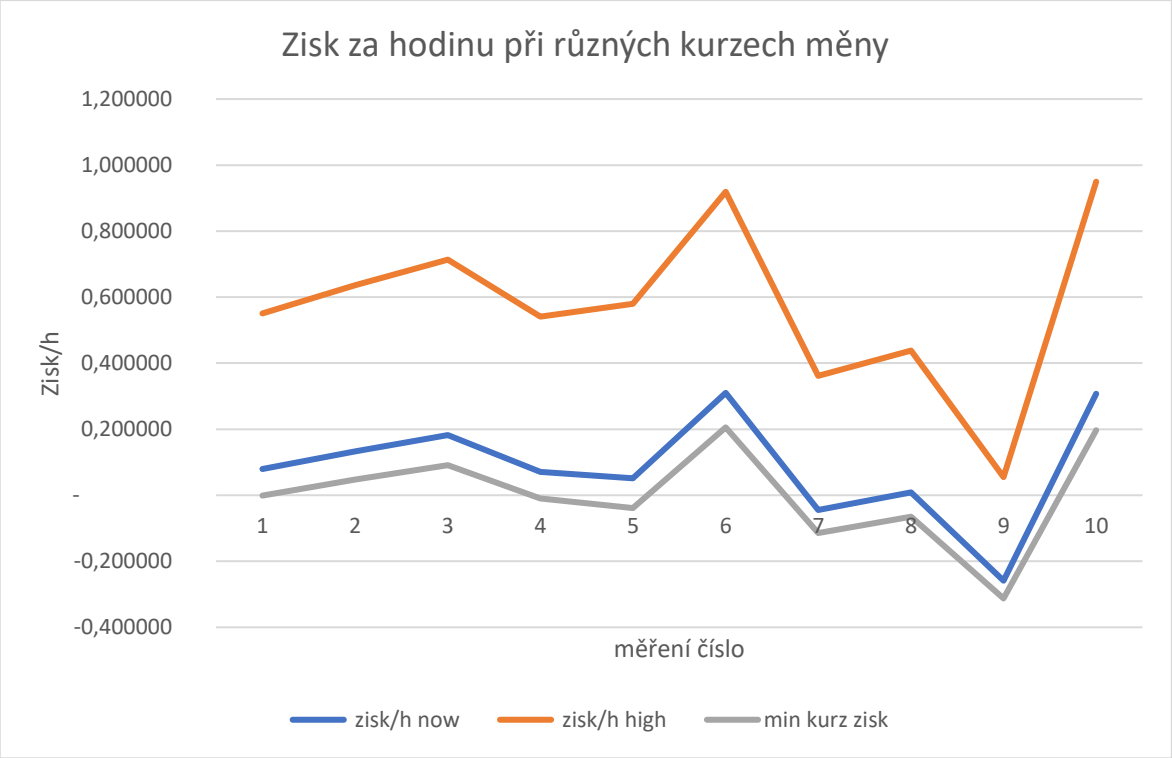
Podle ziskovosti je možné zjistit, za jak dlouho by byla splacena investice do této grafické karty.

- Nízký kurz: 3019 dní (těžba 24 h denně/7 dní v týdnu), tedy 8,3 let
- Vyšší kurz: 442 dní (těžba 24 h denně /7 dní v týdnu), tedy 1,21 roku

Překvapivá je právě rentabilita při nižším kurzu, kde předchozí grafická karta prodělávala. I přes to je ovšem nutné brát kurz v úvahu.

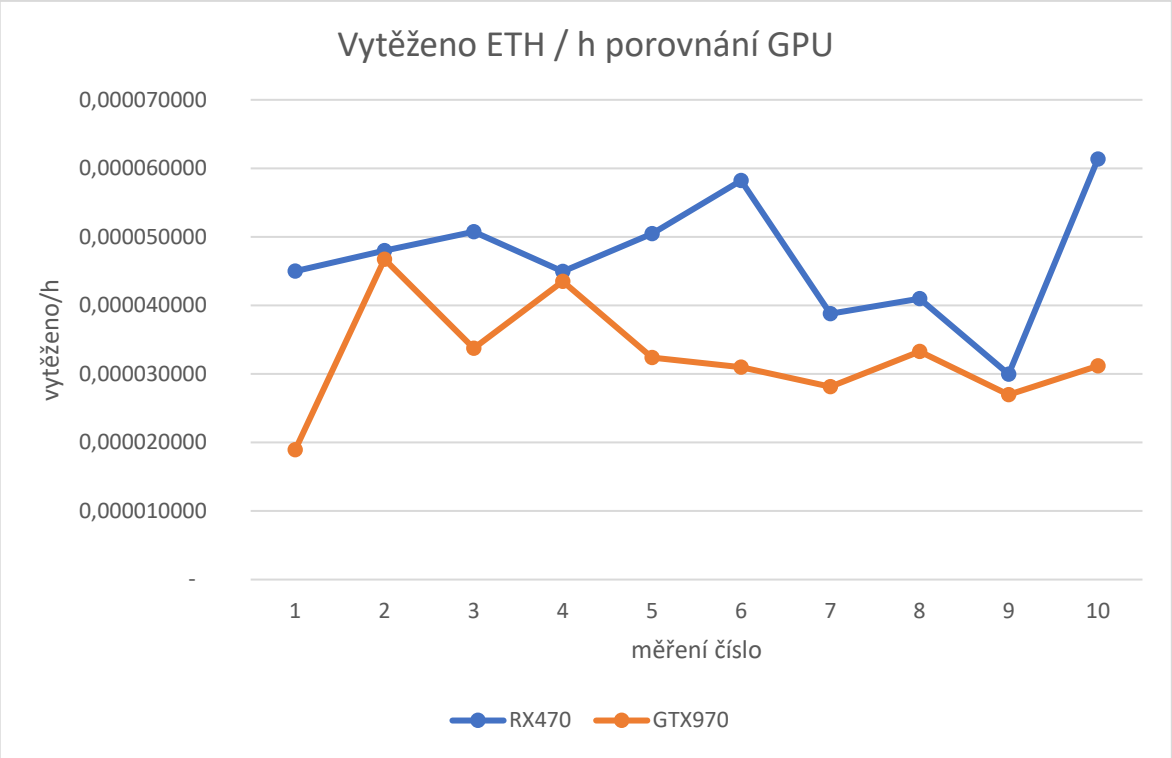
Byl zjištěn minimální kurz pro rentabilitu těžby na této grafické kartě, který se rovná **783 USD/ETH (16159 Kč).**

Následující graf ukazuje průběh zisku za hodinu při různých kurzech měny.




*Graf 9 - zisk při různých kurzech těžby (modrý - stávající kurz, oranžový - vyšší kurz, šedivý - minimální kurz pro rentabilitu)*

Z grafu je tedy patrné, že na rozdíl od předchozí karty tato vydělává a nejnižší možný kurz je menší než stávající (870 USD za ETH). Stále je na něm těžba závislá, i přes to že tato karta je výkonnější, jak je uvedeno na dalším grafu.




*Graf 10 - porovnání výtěžnosti sledovaných grafických karet*

Radeon je ve výtěžnosti za hodinu o 42 % výkonnější než GeForce. Rozdíl je způsoben nejen rozdílem ve stáří grafických karet, ale nejvíce právě architekturálními rozdíly v samotných jádrech GPU.

## 4.3 Těžba na specializovaném hardwaru

Z finančních a časových důvodů nelze těžbu na specializovaném hardwaru provádět přímo s použitím vlastních zdrojů, ale pro účely diplomové práce byla sehnána data o výnosnosti takovéto těžby přímo z praxe od zdroje anonymního.

Počáteční investice závisí na zvoleném hardwaru. Pokud se jedná o grafické karty, je investice závislá hlavně na jejich počtu, kde konfigurace může mít od jedné až po prakticky libovolný počet grafických karet, který je limitován pouze možnostmi základní desky a napájecího zdroje pro provoz stroje.

ASIC jednotky jsou nedostatkovým zbožím, kvůli praktickému monopolu společnosti Bitmain jsou všechny jednotky velmi rychle vyprodány a běžný uživatel musí jednotky pořizovat od překupníků s vysokou marží.

### 4.3.1 Představení hardwaru

**GPU rig**

Sestavy s grafickými kartami jsou dvě. V obou je použita grafická karta od společnosti nVidia s modelovým označením GTX1060. V jednom případě se jedná o model s 6 GB pamětí a v druhém případě o levnější model s 3 GB. Základní konfigurace obou sestav je následující:

- Procesor: Intel Celeron G3930
- Základní deska: Biostar TB250-BTC (speciální deska pro 8 grafických karet s porty v provedení – 1x PCIe 16x a 7x PCIe 1x)
- Zdroj: EVGA G3 750 / Corsair RM850X
- Prodlužovací konektor: šest PCIe riser x1 na PCIe x16
- Systémový disk: flash 8 GB

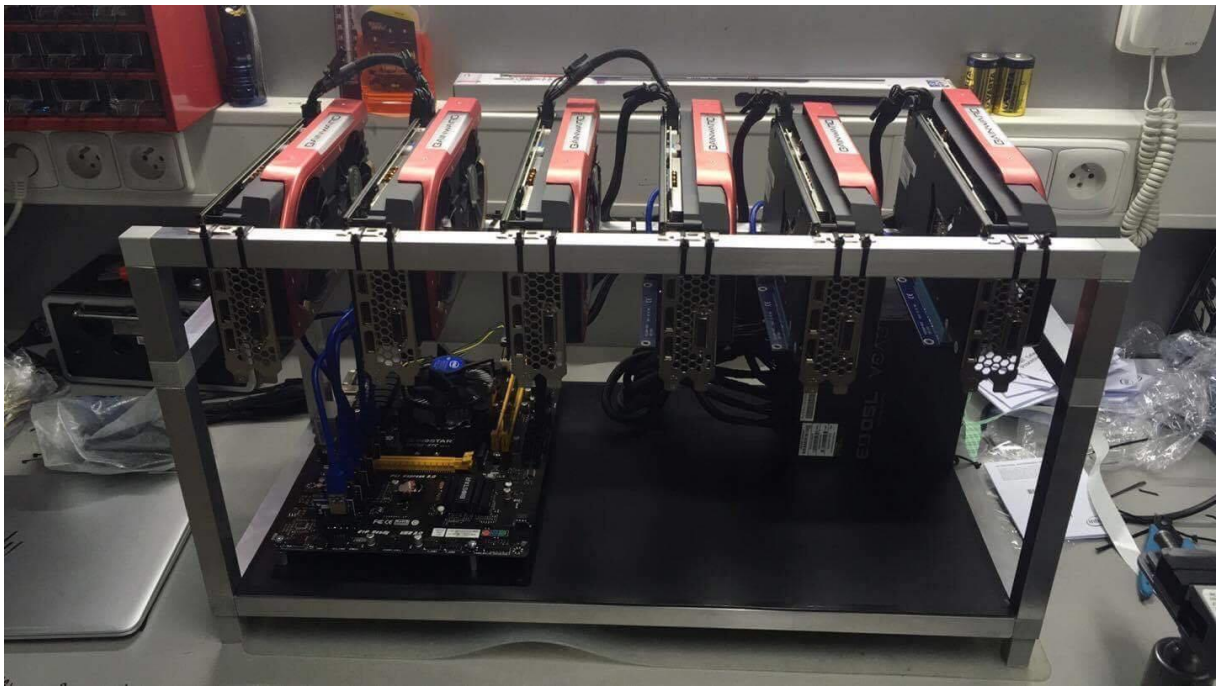
*GTX1060*

Karta byla vydána v roce 2016 v řadě grafických karet Pascal ve dvou verzích, jedna s 6 GB GDDR5 a druhá s 3 GB, přičemž oba typy karet mají stejnou frekvenci pamětí, 2002 MHz a 8008 MHz efektivně. Obsahuje jádro GP106, které je vyrobeno 16nm FinFET procesem s 4,4 miliardami tranzistorů. Na jádře je osazeno 1280 (1152 na 3 GB verzi) stream procesorů, 80 (72 na 3 GB verzi) texturovacích jednotek a 48 ROPs (méně než u předchozí, starší karty GTX970, ale nedochází k obcházení paměťových řadičů).

Takty karet s jádry architektury Pascal jsou nastaveny poměrně vysoko a začínají přibližně na 1500 MHz (1506 MHz pro GTX1060) a u nejvyšších verzí dosahují i 2 GHz, ovšem u GTX 1060 je to pouze 1709 MHz pro referenční verzi (karta přímo od výrobce) a ve verzi od společnosti MSI jsou takty nastaveny až na 1809 MHz (samozřejmě je možné přetaktování). [1]

Sestava grafických karet se pak slangově nazývá „rig“, volně přeloženo „mašina“. Obě sestavy pak vypadají následovně:

*Obrázek 22 - GPU sestava GTX1060 od MSI (anonymní)*



*Obrázek 23 - GPU sestava GTX1060 od Gainward (anonymní)*

Tyto sestavy pak těží měnu 24 hodin denně 7 dní v týdnu, jedná se tedy o nepřetržitý provoz oproti těžení na spotřebitelském hardwaru. Další fotografie specializovaného hardwaru jsou umístěny v přílohách.

Následující tabulka ukazuje charakteristiky jednotlivých sestav s grafickými kartami.

| Sestava | Spotřeba | Hashrate | Investice |
|---|---|---|---|
| 6GB rig | 600 W | 140 MH/s | 68 000 Kč s DPH |
| 3GB rig | 540 W | 110MH/s | 45 000 Kč s DPH |

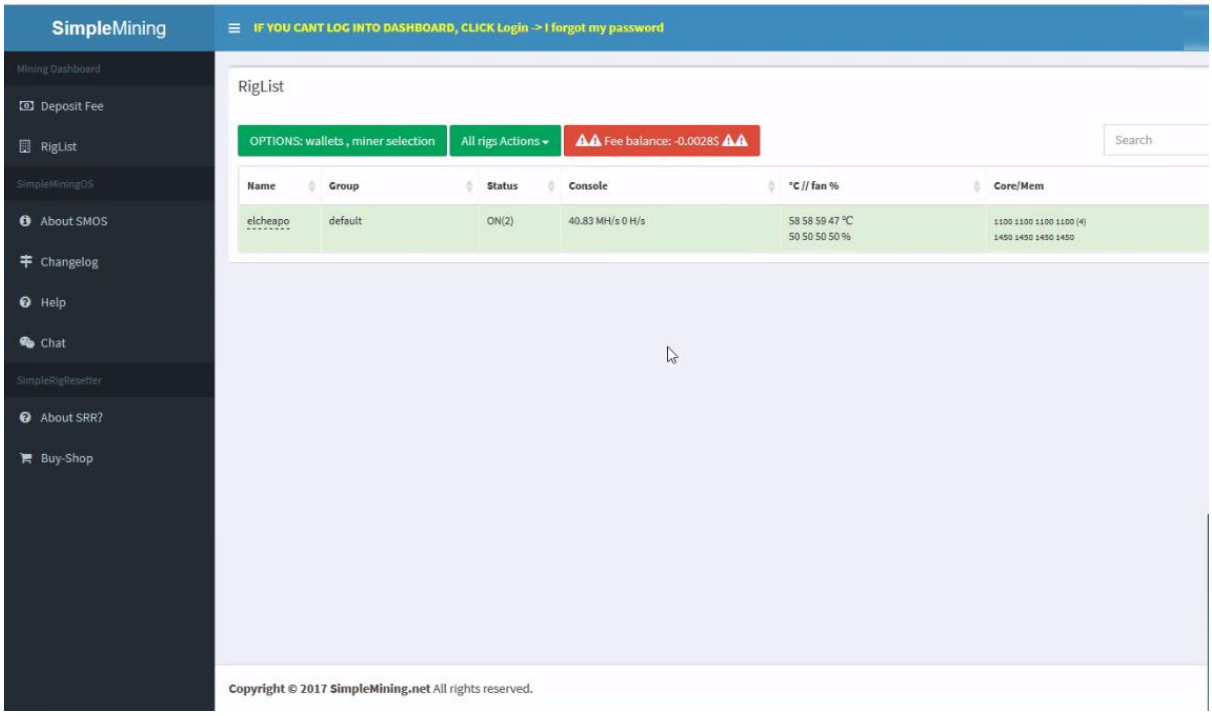
*Tabulka 9-charakteristiky sestav grafických karet (autor)*

Výhody sestavy grafických karet jsou v přenositelnosti na jednotlivé měny, protože grafická karta obsahuje GPGPU (General Purpose GPU, grafické jádro pro obecné využití) a je možné sestavu použít na těžbu v podstatě jakékoli měny. Grafické karty pak nemusí být tolik chlazeny jako jednotky ASIC, vydrží v zátěži dlouhodobě do 70 °C bez snížení životnosti (životnost pak hlavně snižuje zvýšení napětí na jádře a tím dlouhodobě zvýšené teploty). Oproti tomu ale vyžadují zkušenosti pro stabilní těžbu, tedy správné nastavení taktů, ovladačů a tak dále.

*Software*

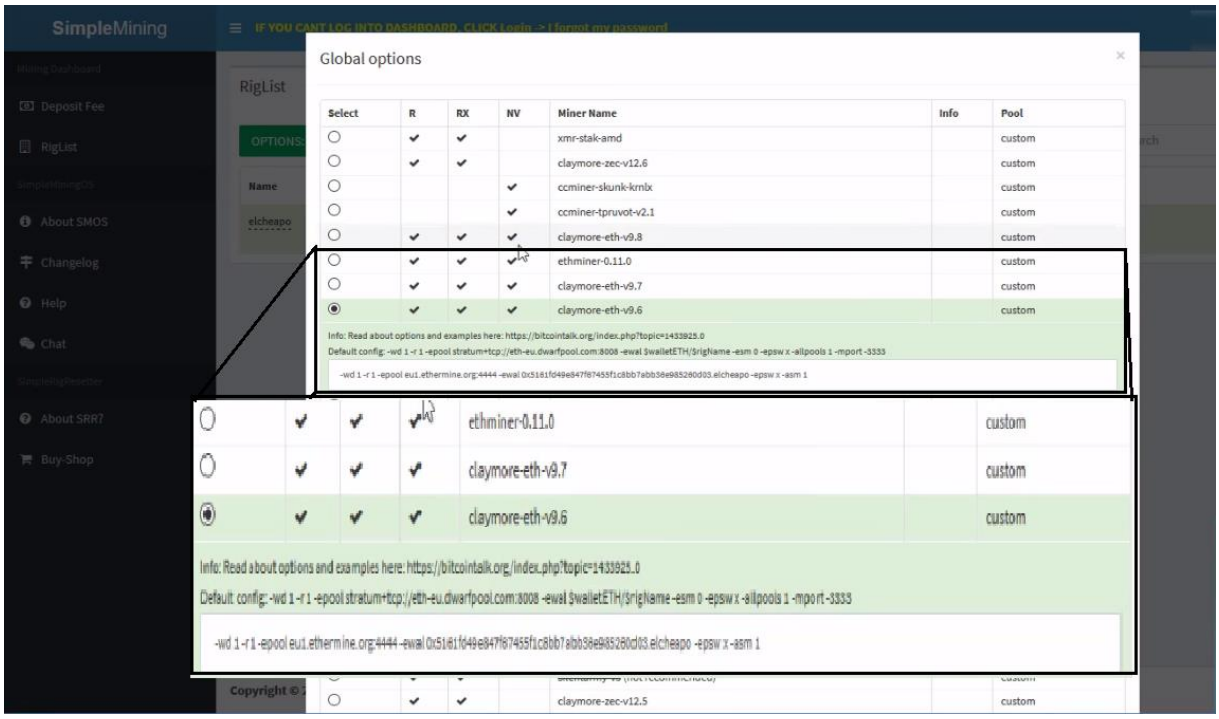
Pro těžbu se využívá stejný nebo podobný program a dávkový soubor jako na systému Windows, ovšem na sestavě je nainstalována speciální distribuce Linuxu, smOS (simple mining OS) dostupný z https://simplemining.net/.

Instalace pak proběhne na flash disk pomocí utility, poskytnuté vývojáři. Pak stačí nastavit na BIOSu základní desky boot z tohoto disku a systém spustí nastavený dávkový soubor.




*Obrázek 24 - ukázka webového rozhraní smOS [2]*

Nastavení dávkového souboru pak neprobíhá ze samotného systému, ale přes webovou aplikaci.




*Obrázek 25- nastavení programu a dávkového souboru pro těžbu [2]*

**ASIC**

Jednotka použitá na těžbu měny je v tomto případě AntMiner L3+ s dvojnásobným výkonem oproti svému předchůdci L3. Při přibližně 500 MH/s spotřebuje 500-800 W energie (záleží na měně). Obsahuje 288 čipů typu BM1485.

Hlavní výhodou těžby na jednotce je pak jednoduchost. Jediné prerekvizity pro těžbu jsou: dobře větraný prostor (jednotka je poměrné hlučná při 75 dB), protože teplotní rozsah je od 0 °C do 40 °C a připojení do internetu (jednotka obsahuje ethernetový konektor). Dále má jednotka až 5x vyšší výkon při těžbě, a tak je možné investici, pokud nedojde k výraznému pádu cen, zaplatit, ale také dále vydělat. [24]

Protiváhou jednoduchosti těžby je pak hlavně pořizovací cena, která se s velkou oblíbeností těžby neustále zvětšuje. Také jejich prodejní hodnota po eventuálním pádu cen kryptoměn a jejich možném krachu je prakticky nulová na rozdíl od grafických karet. Vysoký výkon je také možné použít jen na jeden algoritmus, který používá maximálně 10 měn.


*Obrázek 26 - ASIC AntMiner L3+ [24]*

### 4.3.2 Výsledky

Forma obdržených výsledků od anonymního zdroje je v tabulce výtěžnosti v dolarech za den v 8 po sobě jdoucích měsících od června roku 2017 a pak leden 2018, tudíž je započítána i

velká změna ceny kryptoměn z přelomu měsíců prosince a ledna. I přes tento výkyv jsou obě sestavy a jednotka ASIC rentabilní. Výsledky pak byly přepočítány na stejnou formu jako ty v předchozí části, vygenerované spotřebitelským hardwarem.

| Sestava/ měsíc | Červen | Červenec | Srpen | Září | Říjen | Listopad | Prosinec | Leden |
|---|---|---|---|---|---|---|---|---|
| 6GB rig | 7,5 | 7,5 | 7,5 | 7,5 | 7,5 | 11,2 | 15,5 | 19 |
| 6GB rig po odečtení provozních nákladů | 6 | 6 | 6 | 6 | 6 | 9,6 | 13,7 | 17,6 |
| 3GB rig | 0 | 0 | 0 | 10,5 | 10,5 | 10,5 | 14,7 | 17,4 |
| 3GB rig po odečtení provozních nákladů | 0 | 0 | 0 | 8,5 | 8,5 | 8,5 | 13 | 16,2 |
| Asic miner Antminer L3+ | 19 | 19 | 19 | 19 | 19 | 20,6 | 20,6 | 15,8 |
| Asic miner Antminer L3+po odečtení provozních nákladů | 17 | 17 | 17 | 17 | 17 | 18,7 | 18,7 | 14 |

*Tabulka 10 - výsledky těžby u specializovaného hardwaru v dolarech za 24h (anonymní)*

V tabulce lze vidět nárůst výnosnosti v prosinci a lednu, v dřívějších měsících je kurz na přibližně stejné hodnotě jako nyní.

Po přepočítání průměrných výsledků těžby za jednotlivé měsíce na české koruny vycházela výhodnost těžby na jednu hodinu a den následovně:

| Sestava | Výnosnost kč/h | Výnosnost kč/den |
|---|---|---|
| 6GB rig | 8,926667 | 214,24 |
| 6GB rig po odečtení provozních nákladů | 7,606979 | 182,5675 |
| 3GB rig | 6,82375 | 163,77 |
| 3GB rig po odečtení provozních nákladů | 5,868854 | 140,8525 |
| ASIC miner Antminer L3+ | 16,30833 | 391,4 |
| ASIC miner Antminer L3+ po odečtení provozních nákladů | 14,63458 | 351,23 |

*Tabulka 11- průměrná výtěžnost za hodinu a den (anonymní)*

Pokud dojde k porovnání s pořizovací cenou všech zařízení, je nalezen údaj o době návratnosti dané investice:

- 6 GB rig: 68 000 Kč s DPH investice s výnosností 182,56kč/den po odečtení nákladů: 372 dní
- 3 GB rig: 45 000 Kč s DPH investice s výnosností 140,85kč/den po odečtení nákladů: 320 dní
- ASIC L3+: 75 000 Kč s DPH investice s výnosností 351,23kč/den po odečtení nákladů: 214 dní

Do výsledků je započítána i těžba při nižším kurzu kryptoměn, která je, jak již bylo zmíněno, rentabilní a při propadu kurzu nehrozí negativní zhodnocení, i když se zvětší doba návratnosti investice nebo zmenší výdělek při těžbě po jejím splacení.
Návratnost investice platí pro měnu ethereum, která bude přecházet na nový algoritmus, ale stroje je možné použít na těžbu jiných měn a návratnost investice bude podobná.
Pro grafické karty je nyní výhoda vyšších cen při rozhodnutí o prodeji oproti ASIC jednotkám. I po zmenšení zájmu o těžbu půjde stále o žádanou komoditu, i přes nižší cenu, jelikož je očekáváno přesycení bazarového trhu.

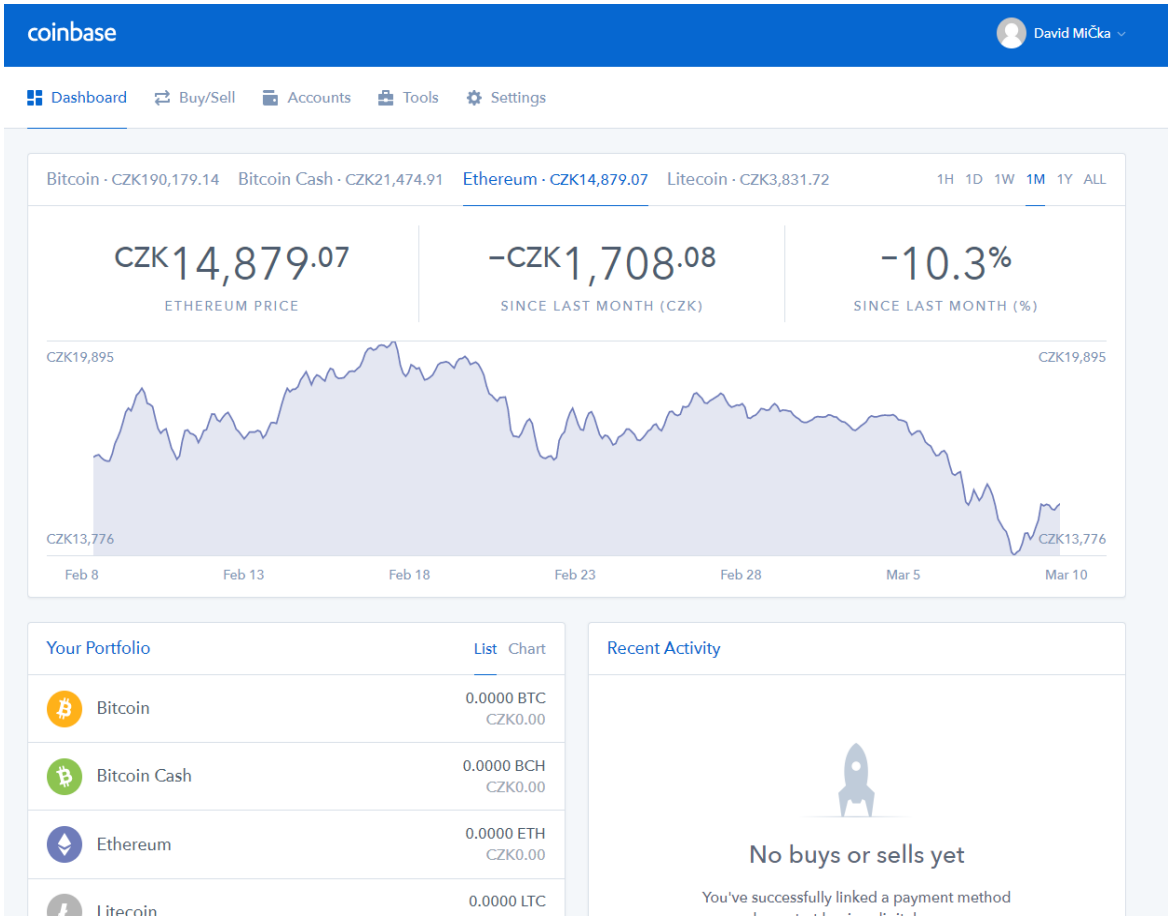
## 4.4 Nákup kryptoměny

Další možností získání měn je jejich nákup a směna na veřejných burzách. Jedna z nejznámějších internetových směnáren je coinbase.com. Po založení účtu jsou založeny adresy peněženek měn Bitcoin, Bitcoin Cash, Ethereum a Litecoin. Pro demonstraci použijeme měnu Ethereum.

Pro směnu kryptoměny je třeba splnit řadu bezpečnostních podmínek (platí i pro ostatní směnárny):

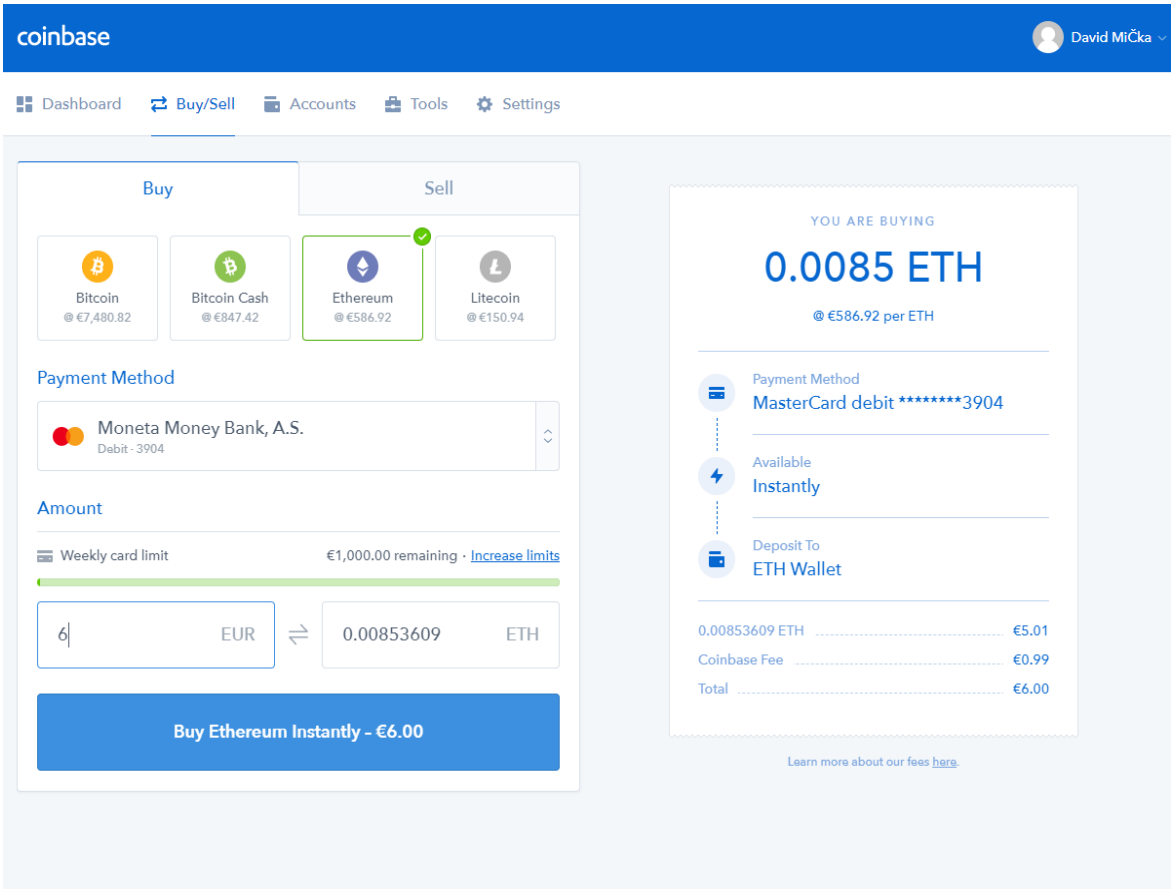
- Verifikovat e-mail nejen při založení, ale také při přihlášení (2 fázové ověření)
- Nahrát fotografie osobního dokladu (pas, řidičský průkaz, občanský průkaz)
- Uložit číslo kreditní, či debetní karty (použití technologie 3D secure je nutností)

Po splnění těchto podmínek je možnost na serveru nakupovat kryptoměny, sledovat kurzy a stav pořízených prostředků.



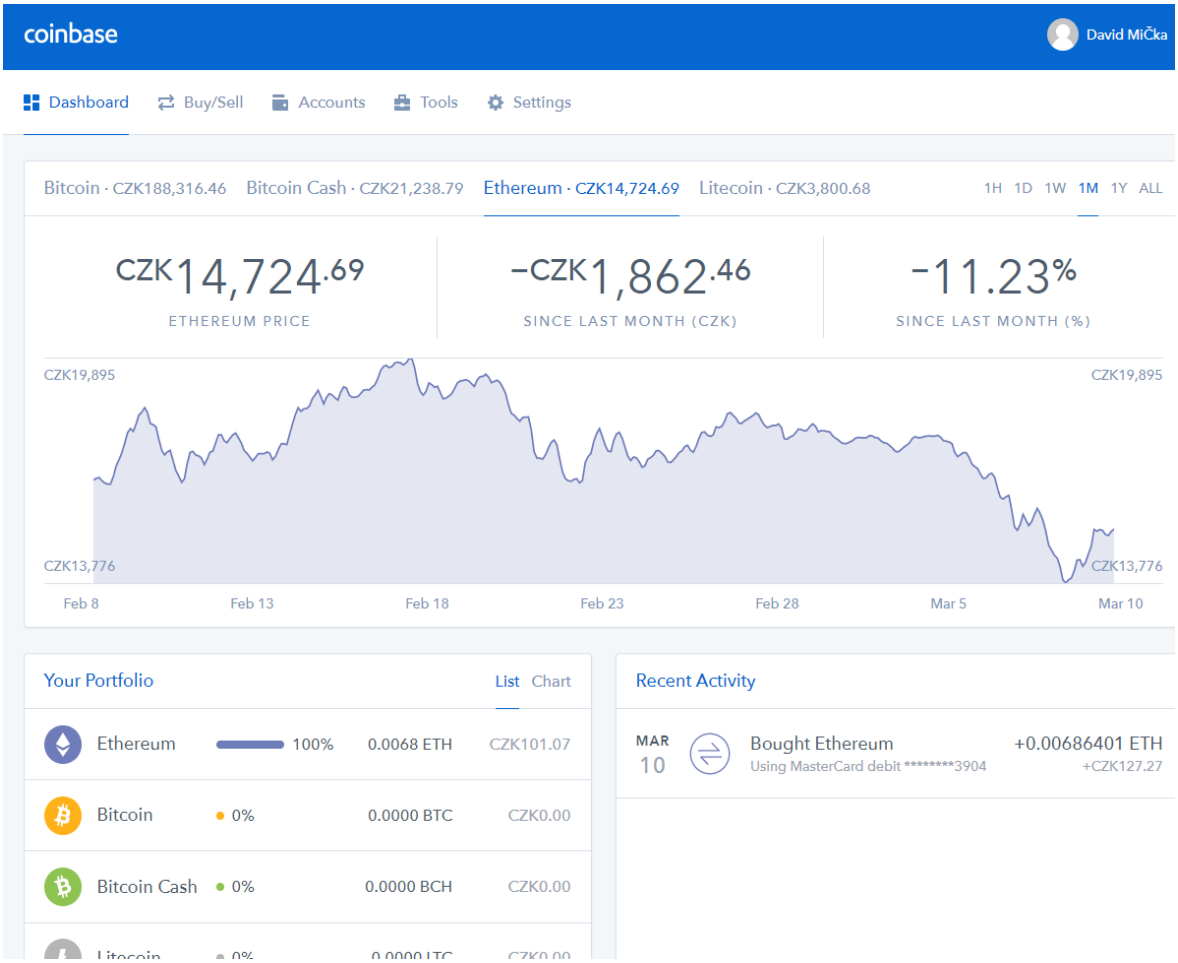

*Obrázek 27 - základní obrazovka coinbase po verifikaci účtu (coinbase.com, zdroj: autor)*

Důležitý prvek stránky je tedy směna za měnu s nuceným oběhem. Zde se bude jednat o euro a je nutné uhradit také poplatky pro poskytovatele (banku a server coinbase). Měna je k dispozici okamžitě po nákupu a pokud není nákup ověřen technologií 3D secure je nutné jej okamžitě zrušit.




*Obrázek 28 - nákup Ethereum (coinbase.com, zdroj: autor)*

Po nákupu je možné s měnou nakládat okamžitě, kupovat další měny a měnit je. Je nutné zdůraznit, že obchodování s kryptoměnami je velmi nejistá záležitost s ohledem na nestabilní kurz a může dojít jak k velkému zhodnocení vložených prostředků, tak k rychlému znehodnocení. Nyní je nákup výhodným, jelikož poptávka po měnách je stále vysoká, ovšem pokud dojde k velkým prodejům jako došlo na přelomu ledna a února 2018, ceny se sníží díky zvýšené nabídce.




*Obrázek 29 - sledování vložených prostředků (coinbase.com, zdroj: autor)*

Je nutné dodat, že první platba byla poskytovatelem Coinbase z neznámého důvodu zamítnuta, i přesto, že prošla systémem 3D secure. Druhá platba už proběhla v pořádku. To je důvod lišících se prostředků z obrázku s nákupem (Obr. 28) a se sledováním prostředků (Obr. 29).

# 5 Zhodnocení výsledků a doporučení

Virtuální měna je, zejména poslední rok, velmi oblíbenou záležitostí. Díky nárůstu oblíbenosti na konci roku 2017, která proběhla hlavně díky měně Ethereum a vydání nových grafických karet. Ethereum lze totiž velmi dobře těžit na grafických kartách, protože používá algoritmus používající zápisy do paměti.

Jelikož jsou ale měny neregulovány žádnou institucí, je investice do jakékoli z nich velmi riskantní podnik, vzhledem k fluktuaci kurzů.

## 5.1 Výsledky těžby

Výsledky těžby kryptoměn byly zpracovány na 2 řešeních. Osobní počítače s jednou grafickou kartou – domácí podmínky a specializovaný hardware – profesionální řešení.

### 5.1.1 Těžba na spotřebitelském hardwaru

V domácích podmínkách je možné kryptoměnu samozřejmě získat (k získání kryptoměny dojde každopádně), ale výhodnost této těžby závisí výhradně na kurzu. Pokud totiž dojde k porovnání se spotřebou elektřiny, je tato těžba nevýhodná.

Poměr spotřeby a vytěžené měny v českých korunách při nižším kurzu je ztrátový. Byl také spočítán minimální kurz, při kterém začíná být těžba výhodná, ale kolísající reálný kurz činí pravděpodobnost výhodné těžby velmi nízkou. Při delších těžbách také hrozí poškození samotného hardwaru a pokud se jedná o domácí počítač, může selhat zdroj a v tomto případě existuje riziko zničení ostatních komponent a ztrátu cenných dat.

Spotřebitelský hardware může sloužit spíše jako platforma pro další rozhodování, zda investovat do specializovaného hardwaru nebo také pro získání základních zkušeností s těžbou a větší zisky s ním nejsou v praxi možné.

Pro těžbu jsou lépe využitelné grafické karty od AMD, kde měřená grafická karta měla ve výtěžnosti o 42 % lepší výsledky než produkt od firmy nVidia.

### 5.1.2 Těžba na specializovaném hardwaru

Jelikož investice do hardwaru je cílená výhradně na zisk, tak se specializovaný hardware kupuje výhradně pro rentabilitu do budoucna.

Investice je pak závislá na pořizovaném hardwaru, kde u grafických karet záleží hlavně na počtu a zde platí čím více, tím lépe, protože nárůst hashrate společně se ziskovostí je větší než nárůst nákladů.

Obě řešení rozebírané v práci, tedy jak ASIC jednotka, tak sestavy grafických karet, jsou rentabilní i při nižších kurzech a při jejich zvýšení se výnosnost ještě znásobí.
Při neustálém zisku z obou řešení je možné pak investice splatit a posléze lze mít ze strojů stálý příjem, ovšem pouze u měn, kde se při těžbě provádí proof-of-work algoritmy. Komunita měny Ethereum plánuje v další verzi přechod na proof-of-stake, který eliminuje těžbu v síti, tudíž je nutný přechod na jinou měnu používající proof-of-work, kde uživatelé s grafickými kartami mají přeorientování na jinou měnu velmi jednoduchý oproti uživatelům s jednotkami ASIC.

Pokud upadne zájem o kryptoměnu, budou grafické karty dobře prodejné na bazarovém trhu i přes jeho přesycení a možné opotřebení, nyní jsou velmi žádaným artiklem, protože stále probíhá jejich hromadné skupování a jejich cena je díky tomu velmi vysoká.
Investice do sestavy grafických karet se tedy jeví jako lepší možnost, ale bohužel nejsou v tomto období u prakticky žádného dodavatele skladem a nákupní cena bude mnohem vyšší než investice uvedená v této práci.
Těžba bude rentabilní do doby, než opadne zájem o nákup kryptoměn a jejich cena klesne pod úroveň, kde těžba nemá smysl, i přesto, že stále generuje zisk.

### 5.1.3 Nákup kryptoměn

Nákup kryptoměn je nejjednodušší varianta jejich získání a vyžaduje takové prostředky jaké je uživatel schopen uvolnit.
Zakoupená kryptoměna se poté řídí aktuálními kurzy směnárny, kam byly prostředky vloženy. Stále platí, že kurzy měn jsou velmi nestabilní a z vložené prostředky mohou být zhodnoceny, či úplně ztraceny.
Kryptoměny po výrazném pádu na začátku roku 2018 pomalu posilují, i když občas dojde k velkému propadu nynější trend ukazuje pomalý nárůst od propadu k minimu v únoru, tudíž investice při nižších cenách je celkem výhodná.
Stále se ale musí počítat s všudypřítomným rizikem, které v podstatě není odhadnutelné díky absenci regulace.

# 6 Závěr

Stanovené cíle byly splněny. V první části byl představen vývoj kryptografických měn napříč historií, koncept, na kterém tyto měny fungují, tedy jakým způsobem jsou zabezpečeny, jak probíhají transakce, těžba a co je blok. Dále byl poskytnut přehled o používaném hardwaru jak v teoretické, tak v praktické části. Byly předloženy očekávané směry vývoje kryptografických měn do budoucna společně s vývojem na trhu. V praktické části byl porovnán hardware specializovaný, tedy jednotka ASIC s dvěma sestavami grafických karet a spotřebitelský ve formě osobního počítače s grafickými kartami. Otestována a porovnána byla výnosnost těžby na obou typech hardwaru a na základě výsledků byly formulovány závěry doporučení.

Přínosem k danému tématu je jak představení kryptoměn, tak ukázání možností jejich získání (těžbou a směnou). Představený hardware k těžení pak pomůže například při rozhodování pro investici do těžby kryptoměn nebo pouze v lepší orientaci v problematice.

# 7 Seznam použitých zdrojů


[1] NVIDIA GeForce GTX 1060 6 GB. *TechPowerUp* [online]. 2004 [cit. 2018-03-21]. Dostupné z: https://www.techpowerup.com/gpudb/2862/geforce-gtx-1060-6-gb

[2] How to Use Simple Mining OS SMOS GPU Miner Software. In: *YouTube* [vid]. San Bruno, CA: YouTube, 2005 [cit. 2018-03-21]. Dostupné z: https://www.youtube.com/watch?v=wEo3jgIAwds

[3] MSI GeForce GTX 970 Gaming 4 GB Review. *TechPowerUp* [online]. 2004, 17.12.2014 [cit. 2018-03-21]. Dostupné z: https://www.techpowerup.com/reviews/MSI/GTX_970_Gaming/

[4] BURNES, Andrew. Introducing The Amazing New GeForce GTX 980 & 970. In: *GeForce.com* [online]. Santa Clara, CA: NVIDIA Corporation, 1999, 18.9.2014 [cit. 2018-03-21]. Dostupné z: https://www.geforce.com/whats-new/articles/maxwell-architecture-gtx-980-970

[5] What is PPLNS. *Give Me COINS* [online]. [cit. 2018-03-21]. Dostupné z: http://give-me-coins.com/support/faq/what-is-ppln s/

[6] Pool vs. solo mining. *Bitcoin wiki* [online]. San Francisco, CA: Wikimedia foundation, 2014, 21.12.2017 [cit. 2018-03-21]. Dostupné z: https://en.bitcoin.it/wiki/Pool_vs._solo_mining

[7] Dagger-Hashimoto.md. *GitHub* [online]. San Francisco, CA: GitHub, 2008 [cit. 2018-03-21]. Dostupné z: https://github.com/ethereum/wiki/blob/master/Dagger-Hashimoto.md

[8] Ethash. *GitHub* [online]. San Francisco, CA: GitHub, 2008, 3.8.2017 [cit. 2018-03-21]. Dostupné z: https://github.com/ethereum/wiki/wiki/Ethash

[9] Ethash DAG. *GitHub* [online]. San Francisco, CA: GitHub, 2008, 22.2.2018 [cit. 2018-03-21]. Dostupné z: https://github.com/ethereum/wiki/wiki/Ethash-DAG

[10] What actually is a DAG?. *Ethereum Stack Exchange* [online]. New York, NY: Stack Exchange, 2008 [cit. 2018-03-21]. Dostupné z: https://ethereum.stackexchange.com/questions/1993/what-actually-is-a-dag

[11] SABIN, Dyani. *Everything You Need to Know About Cryptocurrency And Why It's The Future Of Money* [online]. Brooklyn, NY: Futurism, 2015, 3.1.2018 [cit. 2018-03-21]. Dostupné z: https://futurism.com/cryptocurrency-future-money-bitcoin/

[12] ISMAIL, Nick. What was learned from cryptocurrency in 2017 and what to expect in 2018. *Information Age* [online]. Londýn: Vitesse Media, 1995, 17.1.2018 [cit.

2018-03-21]. Dostupné z: http://www.information-age.com/learned-cryptocurrency-2017-expect-2018-123470399/

[13] Bitcoin Price. In: *Bitcoin.com* [online]. San Francisco, CA: Saint Bitts, 2014 [cit. 2018-03-21]. Dostupné z: https://charts.bitcoin.com/chart/price

[14] TSIHITAS, Theo. Ripple vs Bitcoin Comparison. *CoinCentral* [online]. CoinCentral, 7.10.2017 [cit. 2018-03-21]. Dostupné z: https://coincentral.com/ripple-vs-bitcoin/

[15] *Ripple Wiki* [online]. San Francisco, CA: Wikimedia Foundation, 2014 [cit. 2018-03-21]. Dostupné z: https://wiki.ripple.com/

[16] 51% Attack: DEFINITION of '51% Attack'. *Investopedia* [online]. New York, NY: Investopedia, LLC., 1999 [cit. 2018-03-21]. Dostupné z: https://www.investopedia.com/terms/1/51-attack.asp

[17] ROSE, Kristýna. Ripple: Startup za miliardy. V čem je jiný než bitcoin?. *Roklen24* [online]. Praha: Echo Media, 2014 [cit. 2018-03-21]. Dostupné z: https://roklen24.cz/a/ww46z/ripple-startup-za-miliardy-v-cem-je-jiny-nez-bitcoin

[18] HERTIG, Alyssa a Maria KUZNETSOV. How Ethereum Works. *CoinDesk* [online]. New York, NY: Coindesk, 2013 [cit. 2018-03-21]. Dostupné z: https://www.coindesk.com/information/how-ethereum-works/

[19] A Beginner's Guide to Ethereum. *Medium* [online]. A Medium Corporation, 2012, 8.3.2017 [cit. 2018-03-21]. Dostupné z: https://medium.com/blockchannel/a-beginners-guide-to-ethereum-5e7e132a854d

[20] XIE, Linda. A beginner's guide to Ethereum: What is Ethereum?. *The Coinbase Blog* [online]. San Francisco, CA: Coinbase, 2011 [cit. 2018-03-21]. Dostupné z: https://blog.coinbase.com/a-beginners-guide-to-ethereum-46dd486ceecf

[21] *Litecoin Wiki* [online]. San Francisco, CA: Wikimedia foundation, 2014 [cit. 2018-03-21]. Dostupné z: https://litecoin.info/index.php/Main_Page

[22] OLŠAN, Jan. 3,5GB záhada u GeForce GTX 970 objasněna. Má míň ROP a L2, než Nvidia tvrdila. *CNews* [online]. Praha: Mladá fronta, 28.1.2015 [cit. 2018-03-21]. Dostupné z: https://www.cnews.cz/35gb-zahada-u-geforce-gtx-970-objasnena-ma-min-rop-a-l2-nez-nvidia-tvrdila/

[23] AMD Radeon RX 470. *TechPowerUp* [online]. 2004 [cit. 2018-03-21]. Dostupné z: https://www.techpowerup.com/gpudb/2861/radeon-rx-470

[24] Antminer L3 specifications. *CRYPTO MINING BLOG* [online]. Crypto Mining Blog, 2014, 11.4.2017 [cit. 2018-03-21]. Dostupné z: http://cryptomining-blog.com/tag/antminer-l3-specifications/

[25] *Bitcoin Wiki* [online]. San Francisco, CA: Wikimedia foundation, 2014 [cit. 2018-03-20]. Dostupné z: https://en.bitcoin.it/wiki/Main_Page

[26] Bitcoin Difficulty. In: *Bitcoin Wisdom* [online]. [cit. 2018-03-20]. Dostupné z: https://bitcoinwisdom.com/bitcoin/difficulty

[27] What is Proof of Work / Proof of Stake. In: *Youtube* [vid]. San Bruno, CA: Youtube, 2005 [cit. 2018-03-20]. Dostupné z: https://www.youtube.com/watch?v=ASCGQFZgcT8

[28] ROSIC, Ameer. Proof of Work vs Proof of Stake: Basic Mining Guide. *Blockgeeks* [online]. California: Blockgeeks, 19.2.2017 [cit. 2018-03-20]. Dostupné z: https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/

[29] Proof-of-work. *Bitcoin wiki* [online]. San Francisco, CA: Wikimedia foundation, 2014 [cit. 2018-03-20]. Dostupné z: https://en.bitcoin.it/wiki/Proof_of_work

[30] JUSTIN ALLEN SEXTON, Michael. The Ethereum Effect: Graphics Card Price Watch. *Tom's hardware* [online]. [cit. 2018-03-20]. Dostupné z: http://www.tomshardware.com/news/ethereum-effect-graphics-card-prices,34928.html

[31] Bitcoin Energy Consumption Index. *Digiconomist* [online]. Digiconomist, 2014, 2018 [cit. 2018-03-20]. Dostupné z: https://digiconomist.net/bitcoin-energy-consumption

[32] ASIC. *Bitcoin wiki* [online]. San Francisco, CA: Wikimedia foundation, 2014 [cit. 2018-03-20]. Dostupné z: https://en.bitcoin.it/wiki/ASIC

[33] Antminer S9: World's Most Efficient Miner. *Bitmain* [online]. Peking: Bitmain Technologies, 2013 [cit. 2018-03-20]. Dostupné z: https://shop.bitmain.com/antminer_s9_asic_bitcoin_miner.htm?flag=overview

[34] Why a GPU mines faster than a CPU. *Bitcoin wiki* [online]. San Francisco, CA: Wikimedia foundation, 2014 [cit. 2018-03-20]. Dostupné z: https://en.bitcoin.it/wiki/Why_a_GPU_mines_faster_than_a_CPU

[35] Caractéristiques GPU / CPU. In: *Institut d'électronique et d'informatique Gaspard-Monge* [online]. Paříž: Université Paris-Est Marne-la-Vallée, 2011 [cit. 2018-03-20]. Dostupné z: http://igm.univ-mlv.fr/~dr/XPOSE2011/CUDA/caracteristiques.html

[36] Transactions Speeds: How Do Cryptocurrencies Stack Up To Visa or PayPal?. *HowMuch.net* [online]. Spojené státy Americké: How Much, 2015 [cit. 2018-03-20]. Dostupné z: https://howmuch.net/articles/crypto-transaction-speeds-compared

[37] How bitcoin transactions work. *Bitcoin.com* [online]. San Francisco, CA: Saint Bitts, 2008, 8.6.2017 [cit. 2018-03-20]. Dostupné z: https://www.bitcoin.com/info/how-bitcoin-transactions-work

[38] Ever wonder how Bitcoin (and other cryptocurrencies) actually work?. In: *YouTube* [vid]. San Bruno, CA: YouTube, 2005, 7.7.2017 [cit. 2018-03-20]. Dostupné z: https://www.youtube.com/watch?v=bBC-nXj3Ng4

[39] How do Bitcoin Transactions Work?. *CoinDesk* [online]. New York, NY: Coindesk, 2013, 29.1.2018 [cit. 2018-03-20]. Dostupné z: https://www.coindesk.com/information/how-do-bitcoin-transactions-work/

[40] Mining. *Bitcoin wiki* [online]. San Francisco, CA: Wikimedia foundation, 2014 [cit. 2018-03-20]. Dostupné z: https://en.bitcoin.it/wiki/Mining

[41] SHEPHERD, Adam. What is cryptocurrency mining?. *IT PRO* [online]. Londýn, Spojené království: Dennis Publishing Limited [cit. 2018-03-20]. Dostupné z: http://www.itpro.co.uk/digital-currency/30249/what-is-cryptocurrency-mining

[42] MADEIRA, Antonio. What is scrypt. *Crypto Compare* [online]. Londýn, Spojené království: Crypto Coin Comparison, 2014, 20.3.2018 [cit. 2018-03-20]. Dostupné z: https://www.cryptocompare.com/coins/guides/what-is-scrypt/

[43] SHA-256 Cryptographic Hash Algorithm. *Movable type* [online]. Cambridge, Spojené království: Movable Type, 2009 [cit. 2018-03-20]. Dostupné z: https://www.movable-type.co.uk/scripts/sha256.html

[44] SHA-256. *Bitcoin wiki* [online]. Bitcoin Project, 2009 [cit. 2018-03-20]. Dostupné z: https://en.bitcoin.it/wiki/SHA-256

[45] Nonce. *Bitcoin wiki* [online]. San Francisco, CA: Bitcoin Project, 2014 [cit. 2018-03-20]. Dostupné z: https://en.bitcoin.it/wiki/Nonce

[46] FAIFE, Corin. Bitcoin Hash Functions Explained. *CoinDesk* [online]. New York, NY: Coindesk, 2013, 19.2.2017 [cit. 2018-03-20]. Dostupné z: https://www.coindesk.com/bitcoin-hash-functions-explained/

[47] VONDRUŠKA, Pavel. Úvod do klasických a moderních metod šifrování: Elektronický podpis. In: *Matematická sekce* [online]. Praha: Karlova univerzita v Praze, 2004 [cit. 2018-03-20]. Dostupné z: http://www.karlin.mff.cuni.cz/~tuma/nciphers/elektronicky_podpis.pdf

[48] History of Cryptocurrency, Part I: From Bitcoin's Inception to the Crypto-Boom. *Coin Telegraph: The future of money* [online]. Idaho: Cointelegraph, 2013, 11.4.2015 [cit. 2018-03-20]. Dostupné z: https://cointelegraph.com/news/history-of-cryptocurrency-from-bitcoins-inception-to-the-crypto-boom

[49] MARTUCCI, Brian. What Is Cryptocurrency: How It Works, History & Bitcoin Alternatives. *Money Crashers* [online]. Waldhaven, New Jersey: SparkCharge Media, LLC., 2017 [cit. 2018-03-20]. Dostupné z: https://www.moneycrashers.com/cryptocurrency-history-bitcoin-alternatives/

[50] Block. *Bitcoin wiki* [online]. San Francisco, CA: Wikimedia foundation, 2014 [cit. 2018-03-21]. Dostupné z: https://en.bitcoin.it/wiki/Block

[51] MADEIRA, Antonio. What is a Merkle Tree?. *Crypto Compare* [online]. Londýn, Spojené království: Crypto Coin Comparison, 2014 [cit. 2018-03-21]. Dostupné z: https://www.cryptocompare.com/mining/guides/what-is-a-merkle-tree/

[52] Radeon™ RX 580 Graphics. *AMD* [online]. Santa Clara, CA: Advanced Micro Devices, 1999 [cit. 2018-03-21]. Dostupné z: https://www.amd.com/en/products/graphics/radeon-rx-580

[53] Česko je ráj pro virtuální měny. Bitcoinem zaplatíte už i na vesnici. *IDnes* [online]. Praha: MAFRA, 1999, 10.6.2017 [cit. 2018-03-21]. Dostupné z: https://ekonomika.idnes.cz/bitcoin-kryptomena-placeni-retezce-praha-brno-vranovice-pks-/ekonomika.aspx?c=A170610_091831_ekonomika_fer

[54] HERTIG, Alyssa a Maria KUZNETSOV. How Do Ethereum Smart Contracts Work?. *CoinDesk* [online]. New York, NY: Coindesk, 2013 [cit. 2018-03-21]. Dostupné z: https://www.coindesk.com/information/ethereum-smart-contracts-work/

[55] For pool mining, what exactly is a share?. *Ethereum Stack Exchange* [online]. New York, NY: Stack Exchange, 2008 [cit. 2018-03-21]. Dostupné z: https://ethereum.stackexchange.com/questions/4529/for-pool-mining-what-exactly-is-a-share

[56] Cena za 1 kWh. *Energie123* [online]. [cit. 2018-03-21]. Dostupné z: https://www.energie123.cz/elektrina/ceny-elektricke-energie/cena-1-kWh/

# 8 Přílohy

*Obrázek 30 - mining rig (anonymní)*

*Obrázek 31- těžící hala (anonymní)*


*Obrázek 32 - těžící hala (anonymní)*

*Obrázek 33 - těžící hala (anonymní)*