Těžba kryptoměn a její energetická udržitelnost

Jakub Trnečka

Bakalářská práce
2023

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav počítačových a komunikačních systémů

Akademický rok: 2022/2023

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Jakub Trnečka**
Osobní číslo:	**A20040**
Studijní program:	**B0688A140008 Informační technologie v administrativě**
Forma studia:	**Prezenční**
Téma práce:	**Těžba kryptoměn a její energetická udržitelnost**
Téma práce anglicky:	**Cryptocurrency Mining and its Energy Sustainability**

Zásady pro vypracování

1. Popište základní principy těžby kryptoměn.
2. Analyzujte existující možnosti pro zvýšení energetické udržitelnosti v této oblasti.
3. Prezentujte proces těžby v podmínkách běžného uživatele. Porovnejte vybrané zástupce potřebných hardwarových a softwarových nástrojů.
4. Proveďte experiment reálné těžby na vybraném grafickém procesoru při různých nastaveních a vyhodnoťte získané výsledky z pohledu ziskovosti.
5. S ohledem na výsledky reálného experimentu se pokuste navrhnout další možnosti pro zvýšení ziskovosti a energetické udržitelnosti těžby.

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. BOURBON, Roberto. *Why Bitcoin is actually good for our planet*. Independently published, 2021.
2. KONEČNÝ, Miroslav. *Systém využití odpadního tepla z výpočetní jednotky využívané pro těžbu kryptoměn*. Praha, 2019. Diplomová práce. České vysoké učení technické v Praze, Fakulta elektrotechnická, Inteligentní budovy. Vedoucí práce Ing. Vladimír Janíček, Ph.D.
3. NÁÑEZ ALONSO, Sergio Luis, Javier JORGE-VÁZQUEZ, Miguel Ángel ECHARTE FERNÁNDEZ a Ricardo Francisco REIER FORRADELLAS. Cryptocurrency Mining from an Economic and Environmental Perspective. Analysis of the Most and Least Sustainable Countries. *Energies*, 2021, Vol. 14, No. 14. https://doi.org/10.3390/en14144254.
4. PRITZKER, Yan. *Vynález jménem Bitcoin*. Praha: Braiins Publishing, 2020.
5. STROUKAL, Dominik a Jan SKALICKÝ. *Bitcoin a jiné kryptopeníze budoucnosti: historie, ekonomie a technologie kryptoměn, stručná příručka pro úplné začátečníky*. Praha: Grada Publishing, 2018.
6. ZHANG, Rong a Wai Kin (Victor) CHAN. Evaluation of Energy Consumption in Block-Chains with Proof of Work and Proof of Stake. *Journal of Physics: Conference Series*, 2020, Vol. 1584. https://doi.org/10.1088/1742-6596/1584/1/012023.

Vedoucí bakalářské práce: **doc. Ing. Radek Matušů, Ph.D.**
Ústav automatizace a řídicí techniky

Datum zadání bakalářské práce: **2. prosince 2022**
Termín odevzdání bakalářské práce: **24. května 2023**

doc. Ing. Jiří Vojtěšek, Ph.D. v.r.
děkan

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

doc. Ing. Petr Šilhavý, Ph.D. v.r.
garant oboru

Ve Zlíně dne 8. prosince 2022

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne …….

podpis studenta

ABSTRAKT

Cílem této bakalářské práce je uvést čtenáře do problematiky těžby kryptoměn, a to jak z teoretického hlediska, tak z praktického, tedy z pohledu těžaře. Teoretická část popisuje principy těžby a následně se zaměřuje na její energetickou udržitelnost, kvůli čemu bývá často terčem kritiků. Zkoumá energetickou náročnost těžby kryptoměn a analyzuje možnosti zvýšení její energetické udržitelnosti. Praktická část se zabývá praktickou těžbou kryptoměn z pohledu běžného uživatele, a to prvotní myšlenky a zvážení faktorů, zda těžit, až po samotnou těžbu a optimalizaci těžebního hardwaru, konkrétně grafické karty. Zkoumá chování jednotlivých veličin ovlivňující ziskovost těžby při různých nastaveních karty. Testovaná nastavení jsou vyhodnocena z pohledu efektivity těžby, přičemž pro vybraná nastavení je proveden výpočet profitability. V závěru práce jsou navrhnuty další možnosti pro její zvýšení.

Klíčová slova: kryptoměny, těžba, Bitcoin, udržitelnost, blockchain, blok, grafická karta, těžební algoritmus, optimalizace

ABSTRACT

The aim of this bachelor thesis is to introduce the reader to the issue of cryptocurrency mining, both from a theoretical point of view and from a practical point of view, i.e. from the perspective of the miner. The theoretical part describes the principles of mining and then focuses on its energy sustainability, for which it is often the target of critics. It examines the energy consumption of cryptocurrency mining and analyses the possibilities of increasing its energy sustainability. The practical part focuses on practical cryptocurrency mining from the perspective of the average user, from the initial thought and consideration of factors of whether to mine, to the actual mining and optimization of the mining hardware, specifically the graphics card. It examines the behaviour of various variables affecting the profitability of mining at different card settings. The tested settings are evaluated in terms of mining efficiency and profitability is calculated for the selected settings. At the end of the thesis further options for its increase are proposed.

Keywords: cryptocurrency, mining, Bitcoin, sustainability, blockchain, block, graphics card, mining algorithm, optimization

Tímto bych rád poděkoval vedoucímu mé bakalářské práce panu doc. Ing. Radku Matušů, Ph.D. za odborné vedení, vstřícný přístup, pohotové reakce na dotazy a čas, který mi věnoval při konzultacích. Zároveň bych chtěl poděkovat své rodině za poskytnutý klid pro psaní práce a podporu při vysokoškolském studiu.

Prohlašuji, že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Kryptoměny jsou tu s námi již více než 10 let a z původního koníčku pro nadšence se postupně dostaly do běžného života spousty lidí. Pravděpodobně bychom těžko hledali někoho, kdo se s tímto pojmem ještě nesetkal. Setkáváme se s nimi nejen v online prostředí, ale i v reálném světě v podobě kryptoměnových bankomatů, či podniků, které tyto digitální peníze akceptují, jejichž počet neustále roste. Častou otázkou laiků však bývá, kde se tyto měny berou, jak je možné těžit něco virtuálního a po vysvětlení základních principů těžby často argumentují vysokou spotřebou energie těžby a jejím negativním dopadu na životní prostředí. Jiné, zpravidla více technicky založené, zajímá, jak těžba z uživatelského pohledu funguje a zda si ji mohou sami vyzkoušet. Tyto otázky a argumenty mě vedly ke zvolení tohoto tématu, které je mi blízké.

V teoretické části práce se budu věnovat těžbě Bitcoinu, a to z důvodu, že kryptoměn, které je možné těžit pomocí hardwaru existují tisíce a popis všech z nich by byl zkrátka nemožný. Bitcoin je největším a zároveň nejstarším zástupcem těchto kryptoměn a principy využité u něj jsou často používány u mnoha dalších. Nejdříve vysvětlím principy a pojmy, které jsou s těžbou spojené a následně vysvětlím princip samotné těžby. V další části se budu věnovat právě energetické udržitelnosti těžby, kvůli které bývá Bitcoin a kryptoměny často terčem kritiků. Pokusím se zjistit, jaký dopad těžba na životní prostředí ve skutečnosti má a popíšu aktuální možnosti pro jeho snížení.

V praktické části se budu věnovat těžbě kryptoměn z pohledu běžného uživatele, tedy zpravidla těžbě v domácnosti při použití konvenčního hardwaru, konkrétně grafické karty. Shrnu faktory, které je nutné před těžbou či investicí do hardwaru zvážit a popíšu jednotlivé kroky, kterými si těžař před samotnou těžbou musí projít. Grafickou kartu je nutné pro efektivní těžbu optimalizovat (není pro těžbu továrně uzpůsobena), čemuž se budu věnovat v další části. Popíšu možnosti optimalizace, provedu měření pro různá nastavení karty, zjistím, jak se veličiny ovlivňující ziskovost s různými nastavení mění a jak závisí na nastavovaném parametru. Následně měření vyhodnotím a vypočítám profitabilitu těžby pro různá nastavení karty. V závěru praktické části navrhnu několik možností, jak je možné potenciálně dosáhnout vyššího zisku z těžby.

I. TEORETICKÁ ČÁST

1 TECHNOLOGIE BITCOINU

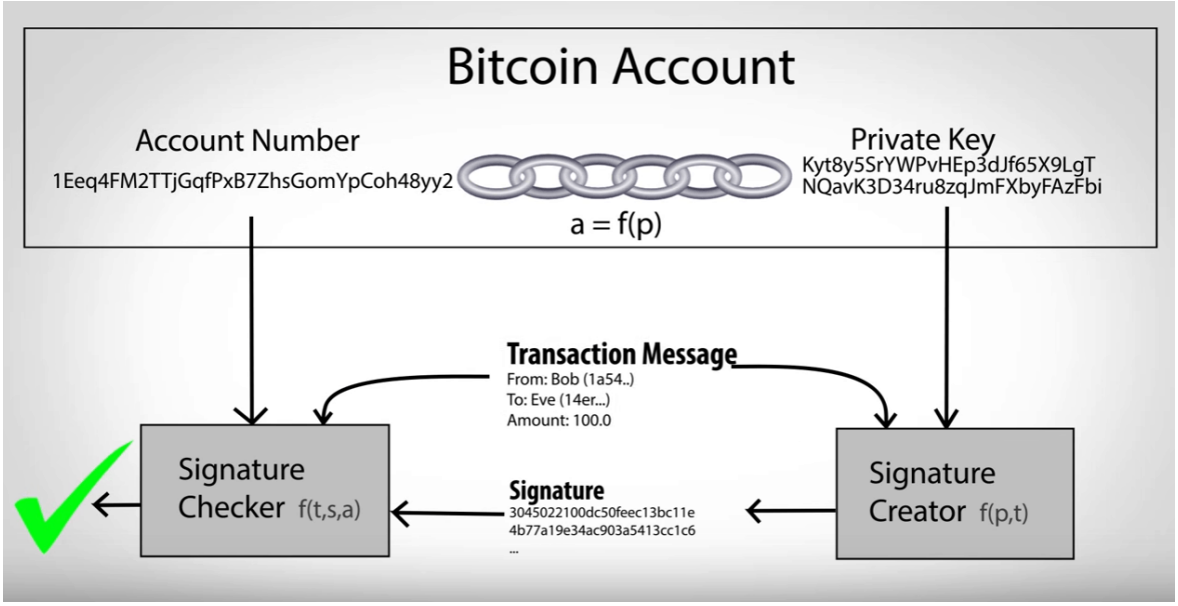
Kryptoměny využívají různé technologie, díky kterým dosahují vlastností jako je decentralizace, bezpečnost nebo transparentnost. Existují tisíce kryptoměn a jejich počet neustále roste, pokrýt je v této práci všechny by bylo nemožné. V následujících podkapitolách jsou proto popisovány technologie Bitcoinu, který je nejstarším a největším zástupcem z řady kryptoměn. Většina kryptoměn vychází právě z něj a základní principy, které využívají jsou velmi podobné.

1.1 Asymetrická kryptografie

Kryptografie je věda o utajování informací. Moderní kryptografie využívá matematiku k šifrování a dešifrování dat a k zaručení pravosti informací. Dešifrování informací je možné pouze se znalostí šifrovacího klíče. [14][15]

Pro zajištění bezpečnosti transakcí v Bitcoinu je využívána asymetrická kryptografie. Asymetrická kryptografie využívá klíčový pár (soukromý a veřejný klíč). Tato asymetrie umožňuje zveřejnění pouze veřejného klíče, ale naopak utajení klíče privátního. Veřejný klíč je matematicky odvozen od soukromého, nicméně odvození opačnou cestou možné není. Zprávu lze dešifrovat pouze soukromým klíčem. Jedním z využití asymetrické kryptografie je digitální podpis, který je využíván také Bitcoinem při odesílání transakcí. Bitcoin využívá konkrétně tzv. ESCDA (digitální podpis s využitím eliptických křivek). Níže je příklad využití digitálního podpisu v Bitcoinu. [15][16][17]

Pro demonstraci využití digitálního podpisu v Bitcoinu mějme dva uživatele – Alici a Boba, Alice chce poslat prostředky Bobovi. Pro provedení transakce je nutné znát bitcoinovou adresu Boba. Ta je vygenerována z Bobova veřejného klíče. Alice vytvoří transakci a zašifruje ji pomocí svého soukromého klíče. Tím vytvoří digitální podpis. Při odeslání transakce Alice zveřejní svůj veřejný klíč, kterým mohou ostatní uzly sítě digitální podpis Alice dešifrovat. Jeho dešifrováním si ostatní účastníci v síti ověří, že Alice musela použít svůj soukromý klíč k vytvoření podpisu. Díky tomu uzly Alici autentizují a zkontrolují, že na adrese Alice je dostupná odesílaná částka a transakce je validní. Digitální podpis je vždy jedinečný pro konkrétní transakci, takže i při případné kompromitaci ho nelze zneužít pro jinou transakci. [15][17][18]



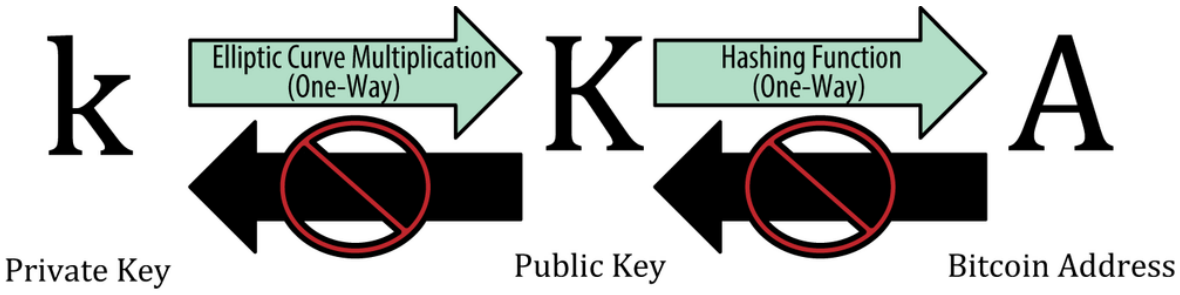
Obrázek 1. Ověření digitálního podpisu v Bitcoinu [19]

1.1.1 Soukromý klíč

Soukromý klíč je náhodně vygenerovaný alfanumerický 256bitový řetězec znaků, který se vygeneruje společně s generováním adresy v peněžence. Úroveň náhodnosti a unikátnosti tohoto řetězce je definovaná použitou kryptografickou funkcí. Jeho velikost by se dala přirovnat k počtu atomů ve vesmíru, takže je v podstatě nemožné, aby 2 uživatelé vygenerovali totožný soukromý klíč. Jak může soukromý klíč vypadat, lze vidět výše na obrázku 1. Možnost manipulovat s bitcoinem na dané adrese má pouze ten, kdo má přístup k soukromému klíči, dá se tedy říct, že vlastník soukromého klíče je vlastník daného bitcoinu. Proto je důležité dbát na bezpečné uložení tohoto klíče tak, aby nebyl kompromitován. Soukromý a veřejný klíč jsou pouze řetězce znaků, takže je možné, aby si je spravoval uživatel sám například pomocí pouhé tužky a papíru, nicméně takové řešení není velmi uživatelsky přívětivé. V případě, že uživatel používá bitcoinovou peněženku, jsou soukromé klíče spravovány právě danou peněženkou. [18][19][20]

1.1.2 Veřejný klíč

Veřejný klíč je také alfanumerický řetězec znaků, který je však pomocí násobení na eliptické křivce odvozen od klíče privátního. Tento proces je nereverzibilní. Z veřejného klíče je poté pomocí nevratné hashovací funkce generována bitcoinová adresa. Vztah mezi adresou, veřejným a soukromým klíčem lze vidět na obrázku 2. [16][21]



Obrázek 2. Vztah mezi adresou, veřejným a soukromým klíčem [16]

Bitcoinová adresa je stejně jako klíče, ze kterých vychází, řetězec alfanumerických znaků. Adresa se používá při transakci jako identifikátor příjemce zasílaných prostředků. Adresa je extrahována z veřejného klíče, a to následujícím způsobem: na veřejný klíč je nejdříve aplikována hashovací funkce SHA-256, na její výstup je poté aplikována další hashovací funkce, konkrétně RIPEMD160, jejíž výstupem je 160bitový řetězec, kterým je právě bitcoinová adresa. Ta je poté uživatelům sítě téměř vždy prezentována ve formě kódování Base58Check. Vygenerování nové bitcoinové adresy nic nestojí a je možné jich vygenerovat nespočet, z hlediska bezpečnosti je doporučováno pro každou transakci generovat novou adresu. Adresa je veřejná, v případě používání pouze jedné adresy by tudíž mohl každý vidět množství vlastněného bitcoinu danou osobou. Pro jednodušší uživatelskou interakci bývá adresa často reprezentována QR kódem. [16][22]

1.1.2.1 Formáty adres

Existuje několik formátů adres. Prvním typem jsou tzv. Legacy nebo také P2PKH (Pay-to-Public-Key-Hash) adresy. Toto je nejstarší typ bitcoinových adres a jeho adresy vždy začínají číslem 1. Jako příklad může být uvedena adresa tvůrce Bitcoinu Satoshi Nakamota – 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa. Poplatek za transakci při odesílání z této adresy bude poměrně vysoký, jelikož zde ještě nebyl aplikován tzv. Segwit (protokol, jehož implementací bylo umožněno přesunutí podpisových dat ze základního bloku do vedlejšího chainu a tím zvýšení kapacity bloku, čímž se transakce staly levnějšími). [23][24]

Druhým formátem jsou tzv. P2SH (Pay-to-Script-Hash) adresy. Tyto adresy začínají vždy číslicí 3 a jedná se již o segwitové adresy, tzn. oproti Legacy adresám jsou úspornější a umožňují nižší poplatky pro uživatele. [25][26]

Nejnovějším formátem jsou Native Segwit (Bech32). Adresy začínají vždy „bc1“. Opět se jedná o segwitové adresy, nicméně jsou ještě mírně úspornější oproti P2SH díky tomu, že

každá transakce zde již nemusí obsahovat skript Segwitu, jak tomu bylo u adres P2SH. [25][26] [27]

Speciálním typem adres jsou tzv. multisig adresy. Ty jsou odvozeny z několika veřejných klíčů a disponují vícero privátními klíči. Pro manipulaci s prostředky na této adrese je vyžadován souhlas stanoveného počtu držitelů privátních klíčů. Tyto adresy se používají například v případech, kdy by o daných prostředcích na adrese mělo rozhodovat více uživatelů. [28][29]

1.2 Blockchain

Blockchain je decentralizovaná „účetní kniha“, která obsahuje záznamy o transakcích. Jedná se o databázi, která je sdílená se všemi uzly sítě a není nikým vlastněna nebo kontrolována. Nové záznamy o transakcích jsou přidávány těžaři. [30]

Tyto transakce jsou obsaženy v blocích, které jsou skrze hash předchozího bloku propojeny a tvoří posloupnost bloků – řetězec (výjimkou je první bitcoinový blok – tzv. block genesis, který má místo hashe předchozího bloku 0). Tento řetězec bloků vede díky hashi předka až k výše zmíněnému úplně prvnímu bloku a zaručuje neměnnost obsahu jakéhokoliv předchozího bloku, aniž byly změněny všechny následující bloky. Díky vysoké energetické náročnosti těžby je však realisticky možné změnit poslední jeden až dva bloky, avšak předchozí bloky jsou již nezměnitelné. Aktuálně má bitcoinový blockchain cca 786 000 bloků a 474 GB (19. 4. 2023). [15][28][31][32]

Přestože se jedná o jednu lineární větev, může se dočasně stát, že blockchain obsahuje více větví o délce 1-2. K tomu může dojít například když těžaři vytěží jeden blok ve stejný čas. Dle bitcoinového protokolu je však za validní považována pouze nejdelší větev, v tomto konkrétním případě tedy rozhoduje, na kterou z větví bude dříve navázáno dalším blokem. Větev, na kterou je navázáno později bude ignorována. [15][33]

V následujících kapitolách jsou podrobněji rozebrány složky, z nichž se blockchain skládá.

1.2.1 Transakce

Transakce jsou datové struktury, které převádějí hodnotu mezi uživateli. Jsou nejdůležitější součástí bitcoinového systému. Každá transakce je veřejným záznamem v bitcoinovém blockchainu a má alespoň jeden vstup (zdroj prostředků) a výstup (adresát prostředků). Výstup

transakce se skládá ze zasílaného množství a adresy příjemce. Výstup lze znovu použít jako vstup jiné transakce, avšak pouze jednou. Výstup, který takto zatím použit nebyl, se označuje jako Unspent Transaction Output (UTXO). Rozdíl součtu bitcoinů na vstupech a součtu bitcoinů na výstupech je transakční poplatek (fee). Poplatek je ve většině peněženek a služeb uživatelsky nastavitelný, jeho výše tedy záleží na odesílateli. Prioritně však budou do bloku zařazeny transakce s vyššími poplatky, nastavením příliš nízkého poplatku může být zapříčiněno velmi dlouhé trvání vypořádání transakce. Součástí transakce je také parametr Locktime, který definuje čas zařazení transakce do bloku. Většinou bývá nastaven na nulu, což interpretuje co možná nejdřívější zařazení. Kompletní datová struktura transakce je na obrázku 3. [16][28]

Size	Field	Description
4 bytes	Version	Specifies which rules this transaction follows
1-9 bytes (VarInt)	Input Counter	How many inputs are included
Variable	Inputs	One or more Transaction Inputs
1-9 bytes (VarInt)	Output Counter	How many outputs are included
Variable	Outputs	One or more Transaction Outputs
4 bytes	Locktime	A unix timestamp or block number

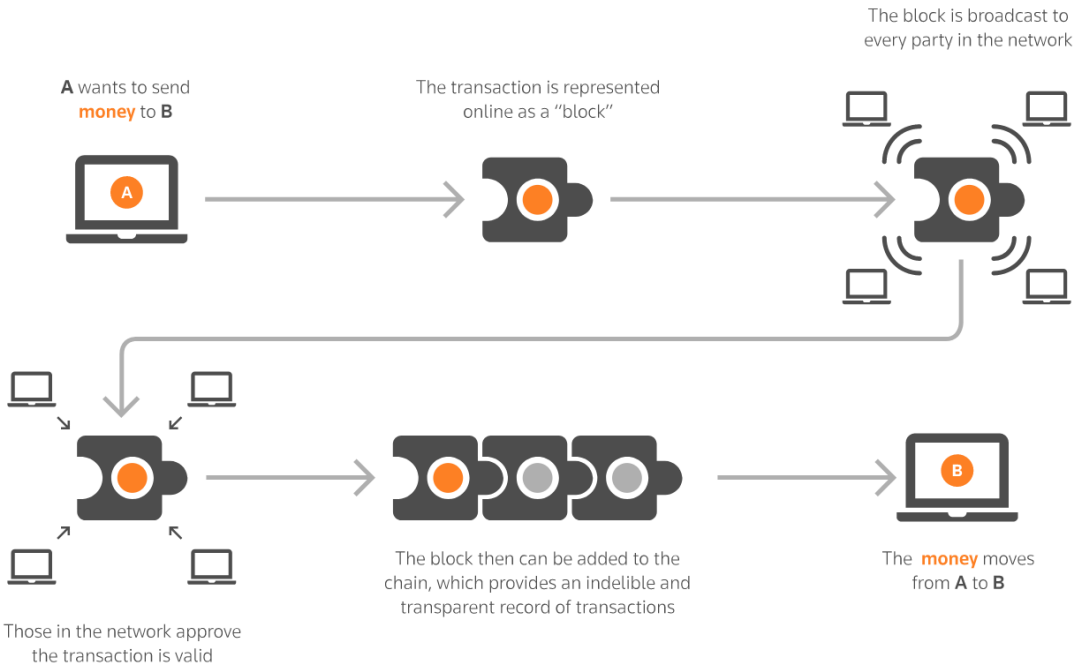
Obrázek 3. Struktura bitcoinové transakce [16]

Každá transakce má také svoje unikátní ID (TXID nebo hash transakce), alfanumerický řetězec znaků, který je jí přiřazen po zařazení do blockchainu. Díky němu je možné každou transakci jednoznačně identifikovat. Pomocí block exploreru je možné konkrétní transakci vyhledat a zobrazit detaily jako zaslanou částku, adresu odesílatele a adresáta, čas transakce a počet potvrzení. [34]

1.2.1.1 Životní cyklus transakce

Životní cyklus transakce začíná jejím vytvořením. Následně musí být transakce podepsána (vysvětleno v kapitole „Asymetrická kryptografie“) a je rozeslána mezi jednotlivé uzly sítě. Každý uzel ji ověří a pokud je transakce validní, rozešle ji mezi další uzly. Tímto způsobem je transakce rozesílána, dokud ji neověří téměř každý uzel v síti. Poté je ověřena těžebním

uzlem a zařazena do bloku, který je součástí blockchainu. Po vytěžení tohoto bloku a následném potvrzení (vytěžení určitého počtu následujících bloku) se transakce stává trvalou součástí blockchainu a je považována za platnou. [16]

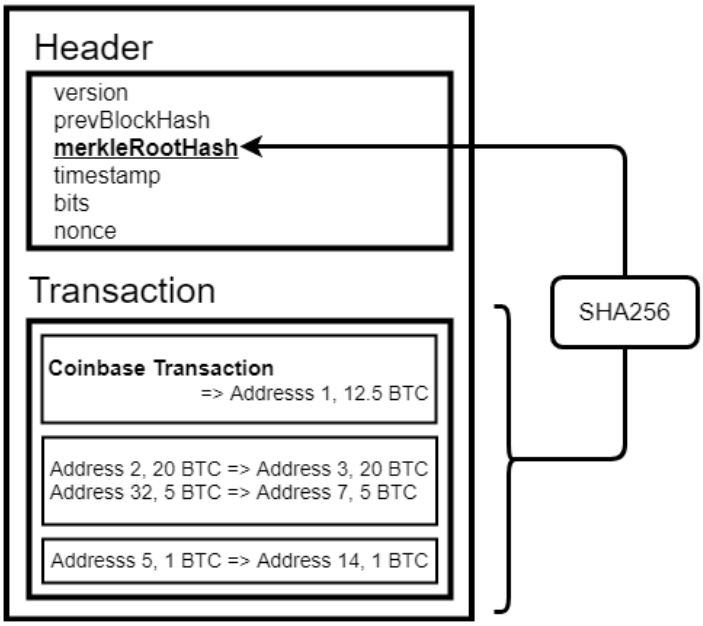


Obrázek 4. Životní cyklus transakce [35]

1.2.2 Blok

Bitcoinové bloky jsou základními stavebními kameny celé sítě. Jejím seskupením vzniká řetězec bloků – blockchain. [36]

Jedná se o kontejnerovou datovou strukturu obsahující transakce určené k vypořádání (zařazení do blockchainu). Skládá se ze záhlaví, které obsahuje metadata a seznam transakcí. Velikost jednoho bloku je 1 MB, přičemž jeho hlavička zabírá pouhých 80 bytů. Zbytek tvoří právě transakce, kterých je v jednom bloku obvykle okolo 2000. První transakcí v bloku je tzv. generující transakce (neboli coinbase transaction), které slouží pro vygenerování nových mincí a jejich distribuci jako odměnu za „vytěžený“ blok mezi těžaři. Celá struktura bitcoinového bloku je na obrázku 5. [16][37][38]



Obrázek 5. Struktura bitcoinového bloku [39]

1.2.2.1 Hlavička bloku

Hlavička každého bloku obsahuje hash hlavičky bloku předchozího (zkracuje se jako hash předchozího bloku). Pomocí tohoto hashe jsou všechny bloky v blockchainu spojeny. [16]

Dále blok obsahuje tzv. Merkle root hash, což je hash hashů všech transakcí v bloku, čímž je zajištěna neměnnost transakcí zahrnutých v bloku. V případě, že by se změnil jediný byte v jediné transakci, změnil by se i hash hlavičky bloku. [40][41][42]

Timestamp reprezentuje čas, kdy byl daný blok vytěžen, a to konkrétně počtem uplynutých sekund od 1.1.1970. [40]

Náročnost těžby aktuálního bloku stanovuje parametr bits target. Čím nižší tento parametr je, tím vyšší je obtížnost těžby. [42]

Nonce je číslo, jehož změnou je změněn výsledný hash bloku. Může nabývat libovolných hodnot. Změnou nonce je možné získat přes 4 miliardy rozdílných hashů. Výsledný hash je poté porovnáván s targetem a v případě, že je nižší než daný target, je blok úspěšně vytěžen. [15][40][42]

2 TĚŽBA

Těžba Bitcoinu má 3 zásadní účely: potvrzování transakcí, emise nových mincí a zabezpečování bitcoinové sítě. Těžaři poskytují síti svůj výpočetní výkon k potvrzování transakcí v síti za odměnu v podobě nově emitovaných bitcoinů. [16][70]

2.1 Princip těžby

Princip těžby byl nastíněn již v přechozí kapitole. Cílem těžaře je tedy nalézt validní blok. Ten je nalezen v případě, že jeho hash je nižší než target v hlavičce bloku. Pokud tomu tak není, je nutné hash spočítat znovu. To je provedeno skrze nonce v hlavičce bloku, jejíž změnou dojde k přepočítání hashe. Nonce může nabývat 2^{32} různých hodnot a je měněna do té doby, dokud není výsledkem hash, který splňuje podmínku, že na daném počtu prvních bitů obsahuje hodnotu 0. Počet těchto bitů je dán targetem, který je dynamicky upravován tak, aby byl v celé bitcoinové síti průměrně nalezen jeden blok za 10 minut. Každých 2016 bloků je automaticky přepočítáno, kolik času bylo potřeba pro jejich vytěžení. V případě, že byl průměr na jeden blok nižší než 10 minut, vzrostl výpočetní výkon celé sítě a obtížnost těžby bude zvýšena (target bude nižší). Pokud je nalezen hash začínající požadovaným počtem nul (tedy nižší než je současný target), je toto řešení považováno za správné, blok je považován za vytěžený a těžař získá odměnu (jeho adresa je přiřazena na výstup coinbase transakce bloku). Odměna za vytěžený blok je aktuálně 6,25 BTC a každé 4 roky je snižována na polovinu. Tomuto principu se říká půlení neboli halving. Součástí odměny jsou také poplatky z transakcí obsažených v daném bloku. [15][28][44][45]

2.2 Proof of work

Kvůli decentralizaci sítě není možné, aby to, že těžaři nebudou při procesu těžby podvádět zajišťovala nějaká centrální autorita. Systém musí fungovat tak, aby jakýkoliv pokus o podvod byl nákladný a aby všichni účastníci sítě (uzly) mohly zkontrolovat, že transakce zapsané v bloku jsou validní a nalezený hash je opravdu nižší než target. V Bitcoinu je toto zajištěno mechanismem Proof of Work (důkazem o vykonané práci). Díky použité hashovací funkci je nalezení požadovaného hashe při těžbě nesmírně náročné, nicméně kontrola správnosti řešení pro ostatní uzly je velmi jednoduchá. Hledání správného řešení spotřebovává

velké množství energie (tedy i peněz) a je v zájmu každého těžaře, aby nalezené řešení bylo ostatními uzly přijato. Tato shoda se nazývá síťový konsenzus. Jakýkoliv pokus o podvod nebude schválen ostatními uzly a vyústí pouze ve zbytečně spotřebovanou energii. Tímto mechanismem jsou jednotliví těžaři motivování k čestnému chování v síti. [18]

2.3 Pooly

S postupným připojováním dalších a dalších těžařů do sítě začal exponenciálně růst hashrate a difficulty, a to až do té míry, že šance jednotlivých těžařů nalézt blok byla v podstatě mizivá. Těžaři vynakládali prostředky na hardware a elektřinu, přičemž šance na nalezení bloku by se dala přirovnat k výhře v loterii. V roce 2010 se proto objevily první mining pooly. Pooly fungují na principu sdružování výpočetního výkonu těžařů a následném rozdělování získané odměny mezi ně podle poskytnutého výpočetního výkonu. Tento princip by se dal přirovnat k pojištění. V případě, že jeden těžař v poolu nalezne blok, je odměna za nalezený blok rozdělena mezi všechny účastníky poolu. Díky poolům mohou i malí těžaři, kteří poskytují malou část výpočetního výkonu získat odměnu. Účastníci poolu zpravidla platí poolu procentuální poplatek za jeho využívání. [16][18]

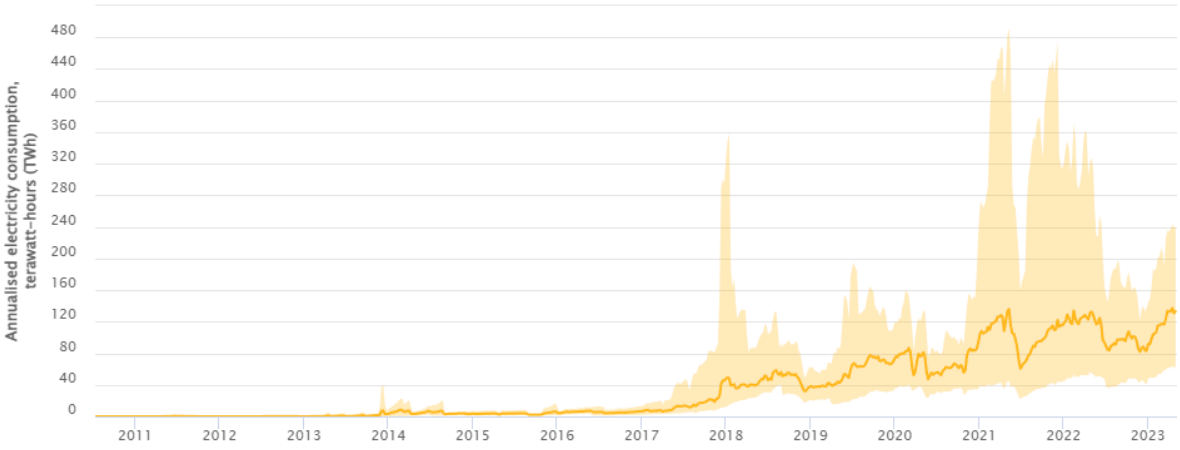
3 ENERGETICKÁ UDRŽITELNOST KRYPTOMĚN

Na kryptoměny fungující na principu Proof of Work a především na Bitcoin bývá často negativně poukazováno skrze vysokou spotřebu elektrické energie. Tato problematika však není tak jednoduchá a nelze jednoznačně odsoudit těžbu kryptoměn bez jakýchkoliv znalostí v této oblasti. Proto se následující kapitoly věnují tématu energetické udržitelnosti těžby.

3.1 Spotřeba elektrické energie bitcoinové sítě

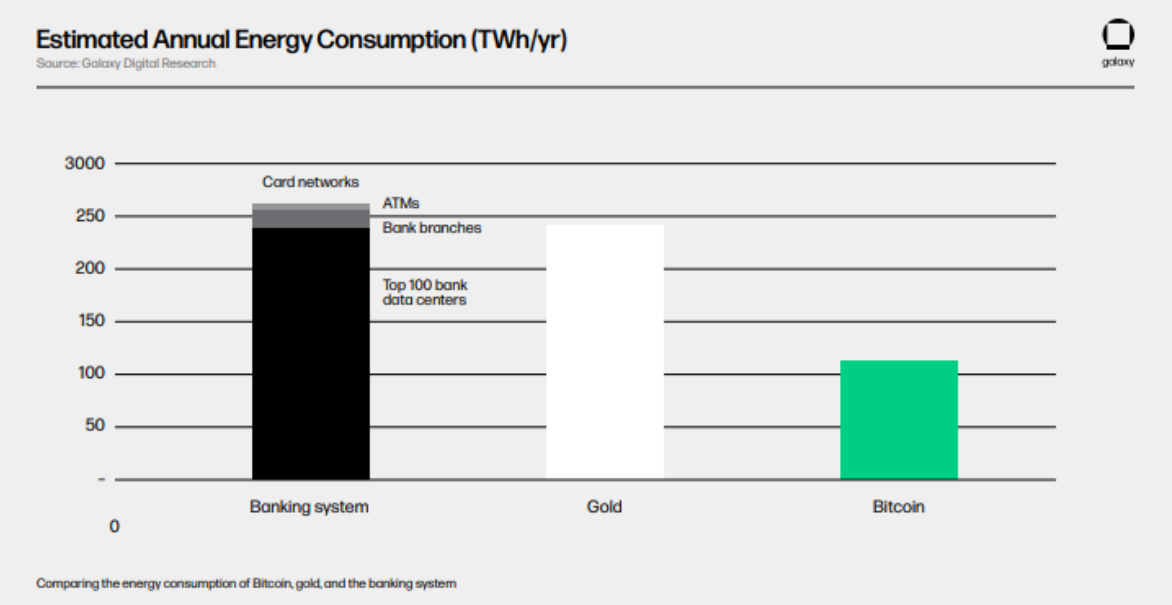
Nejprve je nutné pochopit, proč je pálení elektřiny z hlediska bitcoinové sítě důležité. Spotřebovaná energie je v bitcoinové síti důkazem práce a díky ní je zajišťována validita a bezpečnost transakcí. Z důvodu nákladnosti energie nemají těžaři motivaci v síti podvádět. S vyšším hashratem (větším množstvím spotřebované energie) se stává síť robustnější, bezpečnější a odolnější vůči útokům.

Odhady, kolik elektrické energie Bitcoin využívá se skrze různými zdroji liší, jelikož toto číslo nelze přesně a jednoduše změřit a také z důvodu, že se spotřeba sítě neustále mění. Christian Stoll, Lena Klaaßen a Ulrich Gallersdörfer odhadují k listopadu roku 2018 roční spotřebu celé sítě na 45,8 TWh a emise vyprodukované Bitcoinem přirovnávají k emisím Jordánska nebo Srí Lanky. Mikhail Bondarev ve svém článku odhaduje, že za rok 2019 bylo těžbou Bitcoinu spotřebováno 55,27 TWh elekřiny. Výzkum provedený CoinShares uvedl roční odhad pro prosinec roku 2021 ve výši 89 TWh (0,05 % globálně spotřebované elektřiny). Bitcoin Mining Council ve svém reportu z roku 2022 uvádí spotřebu 253 TWh (0,15 % globálně spotřebované elektřiny) a Cambridge Bitcoin Electricity Consumption Index, který vypočítává roční spotřebu na základě aktuálních dat odhaduje k 8.5.2023 spotřebu 134,15 TWh (vývoj spotřeby od vzniku Bitcoinu se nachází na obrázku 6.). [59][62][63][64][65]



Obrázek 6. Vývoj spotřeby elektrické energie bitcoinové sítě [65]

Celková spotřeba elektřiny bitcoinové sítě bývá často srovnávána se spotřebami celých států, což evokuje myšlenku, že je tato spotřeba enormní. Ve srovnání se zlatem a tradičním finančním systémem se však již tak extrémní nezdá. Amanda Fabiano, Rachel Rybarczyk a Drew Armstrong ve svém výzkumu z roku 2021 odhadují roční globální spotřebu celého bankovního systému na 263,72 TWh, přičemž vzali v potaz 4 hlavní aspekty: datová centra bank, bankovní pobočky, bankomaty a datová centra společností provozující platební karty. Roční spotřebu průmyslu pro těžbu a zpracování zlata odhadují na 240,61 TWh a spotřebu bitcoinové sítě na 113,89 TWh (viz obrázek 7.). Podobné porovnání provedl v roce 2015 Hass McCook, podle kterého jsou rozdíly v tomto srovnání daleko větší. Roční spotřebu bankovního systému odhaduje ve své práci na 2340 PJ (650 TWh), energii těžbu a recyklaci zlata na 500 PJ (138, 89 TWh) a energii spotřebovanou ročně pro těžbu Bitcoinu na 3,97 PJ (1,1 TWh). V tomto případě se jedná o 8 let starý zdroj, dnes je spotřeba bitcoinové sítě výrazně vyšší, nicméně dle výzkumů zmíněných v odstavci výše lze předpokládat, že je i v současnosti energetická náročnost Bitcoinu podstatně nižší než energetická náročnost bankovního systému. V blízké době samozřejmě nelze mluvit o nahrazení klasického finančního systému Bitcoinem (pravděpodobně se tak nestane ani v nejbližších desetiletích), nicméně vzhledem k vývoji ceny Bitcoinu od jeho vzniku o něm lze z dlouhodobého hlediska mluvit jako o udržiteli hodnoty s jistými podobnými vlastnostmi, jako má právě zlato. [67][68]



Obrázek 7. Srovnání roční spotřeby elektrické energie bankovního systému, zlata a Bitcoinu [67]

Energetickou náročnost Bitcoinu nelze popírat a lze předpokládat, že celková spotřeba energie dále poroste, z hlediska udržitelnosti však není tak důležité, kolik energie Bitcoin využívá, ale z jakých zdrojů daná energie pochází. I za předpokladu, že bude celková spotřeba energie bitcoinové sítě v budoucnu stoupat, je možné dosáhnout nižšího dopadu těžbu na životní prostředí, pokud bude k těžbě využívána energie z obnovitelných zdrojů. Roberto Bourbon srovnává Bitcoin s elektrickými auty, která jsou také vysoce energeticky náročná. Na rozdíl od Bitcoinu ale nemají špatnou reputaci ohledně ekologie, ve skutečnosti jsou však ve stejné situaci jako Bitcoin. Budou udržitelná a neškodná pro životní prostředí pouze za předpokladu, že energie, kterou využívají, bude produkována udržitelným způsobem. [45][69]

3.2 Možnosti pro zvýšení udržitelnosti

3.2.1 Proof of Stake

Kritici Proof of Work mechanismu často uvádějí jako udržitelnější řešení pro Bitcoin (a jiné PoW kryptoměny) přechod na mechanismus Proof of Stake.

V PoS mechanismu k ověřování transakcí a vytváření bloků slouží namísto těžařů tzv. validátoři. Validátorem se může stát kdokoliv, kdo ve svém uzlu „uzamkne“ určitý počet vlastních mincí dané kryptoměny (stake). Tento počet je dán konkrétní kryptoměnou, např. u Etherea je to 32 ETH. Těmito mincemi validátor ručí, že nebude v síti podvádět. Pro uzamčení bloku je systémem validační uzel, který zkontroluje validitu transakcí v bloku a blok uzamkne, čímž se daný blok stává součástí blockchainu. Následně validátor jako odměnu získá poplatky za transakce obsažené v bloku. V případě, že by se validátor pokoušel podvádět, přišel by o svůj stake nebo jeho část. Stake si může validátor u většiny kryptoměn kdykoliv „vybrat“ zpět, nicméně s určitou bezpečnostní časovou prodlevou po uzamčení poslední bloku pro případ, že by se v něm validátor pokoušel podvádět. [50]

Oproti PoW mechanismu tak PoS využívá minimum energie, z čehož může plynout, že by byl tento mechanismus pro Bitcoin lepší, nicméně i PoS má určité problémy.

Jedním z nich může být neférovost vůči menším validátorům. Validátoři, kteří si mohou dovolit provozovat více uzlů, kde drží stake, mají ve většině PoS systémů vyšší pravděpodobnost, že budou vybráni pro uzamčení dalšího bloku, tzn. větší pravděpodobnost získat odměnu. Mechanismus tedy upřednostňuje bohatší validátory, což by postupně mohlo vést ke kontrole sítě menším počtem „větších“ validátorů, a tudíž snížení decentralizace sítě. Potenciální vyšší centralizace sítě by potom vedla ke zvýšení pravděpodobnosti 51 % útoku. [51][52]

Jiní kritici vidí jako slabinu fakt, že PoS systém není zabezpečen vstupem z reálného světa, na rozdíl od PoW kde je důkazem spálená elektrická energie. To může u PoS vést k obavám potenciálních zpětných změn v blockchainu, což je u PoW právě z důvodu vysoké energetické náročnosti v podstatě neproveditelné (vyjma posledních 1-2 bloků). [53]

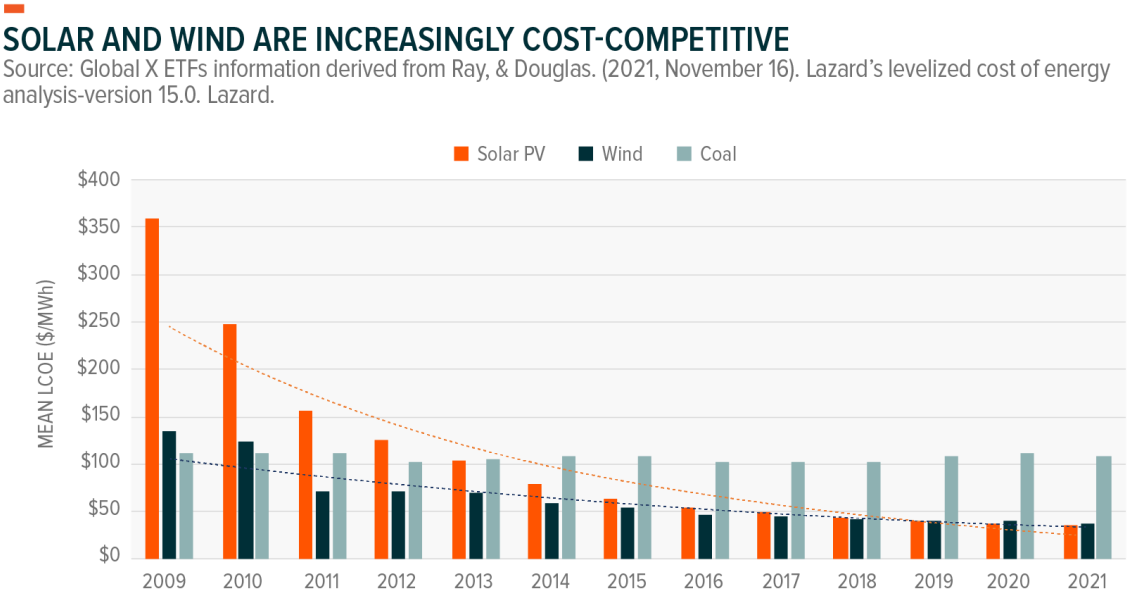
V případě, že kryptoměna funguje na principu mechanismu PoS od samého začátku jejího vzniku, je problematické následně férově rozdistribuovat jednotlivé mince mezi uživatele. Rong Zhang a Wai Kin (Victor) Chan ve svém experimentu zjistili, že při provozu kryptoměny na principu PoS od samého začátku jejího vzniku existovalo pouze několik uzlů, které vlastnily obrovské množství mincí, zatímco většina uzlů vlastnila pouze malé množství. U PoW proběhla prvotní distribuce coinů naopak mnohem spravedlivěji. [52]

Dalším problémem může být motivace uživatelů sítě kryptoměny „stakovat“ a tedy držet namísto aktivního používání, což by mohlo vést k potenciálnímu snižování počtu transakcí. [53]

Je také nutné podotknout že u většiny z těchto problémů se pracuje na jejich řešení. PoS je oproti PoW však stále relativně nový a nikdo nedokáže říct, zda se v budoucnu neobjeví nějaké bezpečnostní problémy. Přechod Bitcoinu na tento mechanismus by byl aktuálně pravděpodobně velmi riskantní, nicméně PoS a další mechanismy konsenzu se neustále vyvíjí a je možné, že v budoucnu bude situace jiná.

3.2.2 Obnovitelné zdroje elektrické energie

Nejzásadnějším způsobem, jak snížit ekologickou stopu těžby, je pravděpodobně využívání elektrické energie z obnovitelných zdrojů. Podle studie odborníků z oxfordské univerzity je trend ceny obnovitelné energie dlouhodobě klesající, v určitých případech je tato energie již levnější než energie z fosilních paliv a v budoucnu by měla dále zlevňovat. S podobnými výsledky přišla International Renewable Energy Agency, která ve svém reportu uvedla, že téměř dvě třetiny energií z obnovitelných zdrojů uvedených do provozu v roce 2021 měly nižší náklady než nejlevnější uhelné varianty v zemích G20. Trend vývoje ceny elektrické energie z obnovitelných zdrojů lze vidět na obrázku 8. [54][55]



Obrázek 8. Vývoj ceny energie z obnovitelných zdrojů [56]

O současné míře využívání obnovitelných zdrojů pro těžbu Bitcoinu se vedou diskuze. Zjistit původ energie, která je využívána k těžbě je komplikované a výsledky se napříč různými zdroji liší. Studie University of Cambridge publikovaná v září 2020 uvádí, že podíl obnovi-

telné energie na těžbě Proof of Work kryptoměn je 39 % (především energie z vodních elektráren). John Schmidt a Benjamin Curry ve Forbesu uvádí pokles podílu obnovitelné energie na těžbě ze 42 % (2020) na 25 % (srpen 2021), zapříčiněný zákazem těžby Bitcoinu v Číně. Nejnovější nalezený zdroj, Bitcoin Mining Council, ve svém průzkumu uvedl pro druhé čtvrtletí roku 2022 podíl „zelené“ energie na těžbě 59,5 %. Ač se zjištěné výsledky liší, lze s velkou pravděpodobností říct, že s klesající cenou obnovitelné energie se budou těžaři přesouvat právě k obnovitelným zdrojům z důvodu minimalizace nákladů na těžbu a tím maximalizace zisku, přičemž každým halvingem (snížením odměny pro těžaře o 50 %) je tento tlak na těžaře ještě zvýšen. [57][58][59]

Těžba kryptoměn může na rozdíl od ostatních odvětví využívat energii, která by pro jiná odvětví byla nevyužitelná. Většina energie musí být vyráběna blízko koncovým uživatelům, nicméně při těžbě kryptoměn tento faktor nehraje roli. Těžba může být tedy provozována i tam, kde provoz jiných odvětví byl komplikovaný nebo nemožný. Také dokáže využívat přebytků energie, které by jinak zůstaly nevyužity, a to nejčastěji u vodních elektráren. Například v Číně při období dešťů vyrobená energie masivně převyšuje poptávku. Technologie v současné době není tak pokročilá, aby bylo možné tuto energii skladovat a efektivně přepravovat do měst, takže tato energie, která byla využívána pro těžbu Bitcoinu by jinak zůstala nevyužita. Tato energie byla v období dešťů zodpovědná za 50 % celkové spotřeby elektřiny bitcoinové sítě. V takovém případě lze mluvit o uhlíkově neutrální těžbě. V současnosti platí v Číně zákaz těžby, nicméně využíváním přebytků energie podobnými způsoby v jiných oblastech by bylo možné energetickou udržitelnost těžby zvýšit. [60]

Sergio Luis Náñez Alonso, Javier Jorge-Vázquez, Miguel Ángel Echarte Fernández a Ricardo Francisco Reier Forradellas v roce 2021 zveřejnili studii ve které zkoumali, které země jsou nejvíce a nejméně udržitelné pro těžbu. Uvažovali faktory jako jsou cena energie, způsob její výroby, teplota, právní omezení a lidský kapitál, na jejichž základě vypočítali index, který jim umožnil jednotlivé státy porovnat. Nejvýše se umístily následující země: Denmark, Germany, Sweden, Jižní Korea a Švýcarsko. Pokud by se těžba přesunula do těchto zemí, dalo by se dle slov autorů mluvit o udržitelné těžbě, protože energie potřebná pro těžbu, pochází v těchto zemích z čistých a obnovitelných zdrojů. Nejhůře naopak dopadly země jako je Bolívie, Surinam, Libye nebo Venezuela. [61]

3.2.3 Využití odpadního tepla

Vedlejším produktem těžby, kromě nových mincí je vyprodukované teplo. Na odpadní teplo z těžby se často zapomíná, těžební stroje ho však vyprodukují obrovské množství a při jeho správném využití lze kompenzovat náklady na elektřinu potřebnou pro těžbu tím zvýšit nejen zisk, ale i udržitelnost těžby. Teplo vyprodukované těžebním hardwarem lze využít k vytápění domácností a budov nebo pro různé výrobní procesy (například v potravinářství). [70]

Využitím odpadního tepla z těžby se zabývá spousta společností. Jednou z nich je například společnost MintGreen v Kanadě, která prodává teplo z těžebního hardwaru společnostem Vancouver Island Sea Salt pro výrobu soli a Shelter Point Distillery, která jej využívá pro výrobu Whiskey. Genesis Mining ve Švédsku spolupracuje s několika dalšími organizacemi na vývoji těžebních kontejnerů se specializovaným prouděním teplého vzduchu do skleníků pro pěstování ovoce a zeleniny. Podobný způsob je využíván také v Nizozemí, kde jsou ve speciálním GreenMine kontejner umístěny ASIC minery (pojem vysvětlen v následující podkapitole), od kterých je teplo odváděno speciálním olejem a skrze tepelný výměník je ohřívána voda, která poté vyhřívá skleník. Francouzský startup WiseMining vyvinul bojler, v němž je voda ohřívána pomocí odpadního tepla z ASIC minerů, čímž by bylo možné snížit náklady na ohřev vody v budovách. [70]

Existuje mnoho dalších způsobů, jak lze odpadní teplo využít. Jeho využití je v ekonomickém zájmu těžařů, protože z vedlejšího produktu, který by běžně zůstal nevyužitý, lze získat další zdroj příjmu a tím zvýšit ziskovost těžby. Lze předpokládat, že s rozvojem odvětví těžby kryptoměn se budou výše zmíněné a jim podobné příklady stávat běžnějšími, čímž by byl výrazně snížen ekologický dopad těžby na životní prostředí. [70]

3.2.4 Vývoj efektivnějšího hardwaru

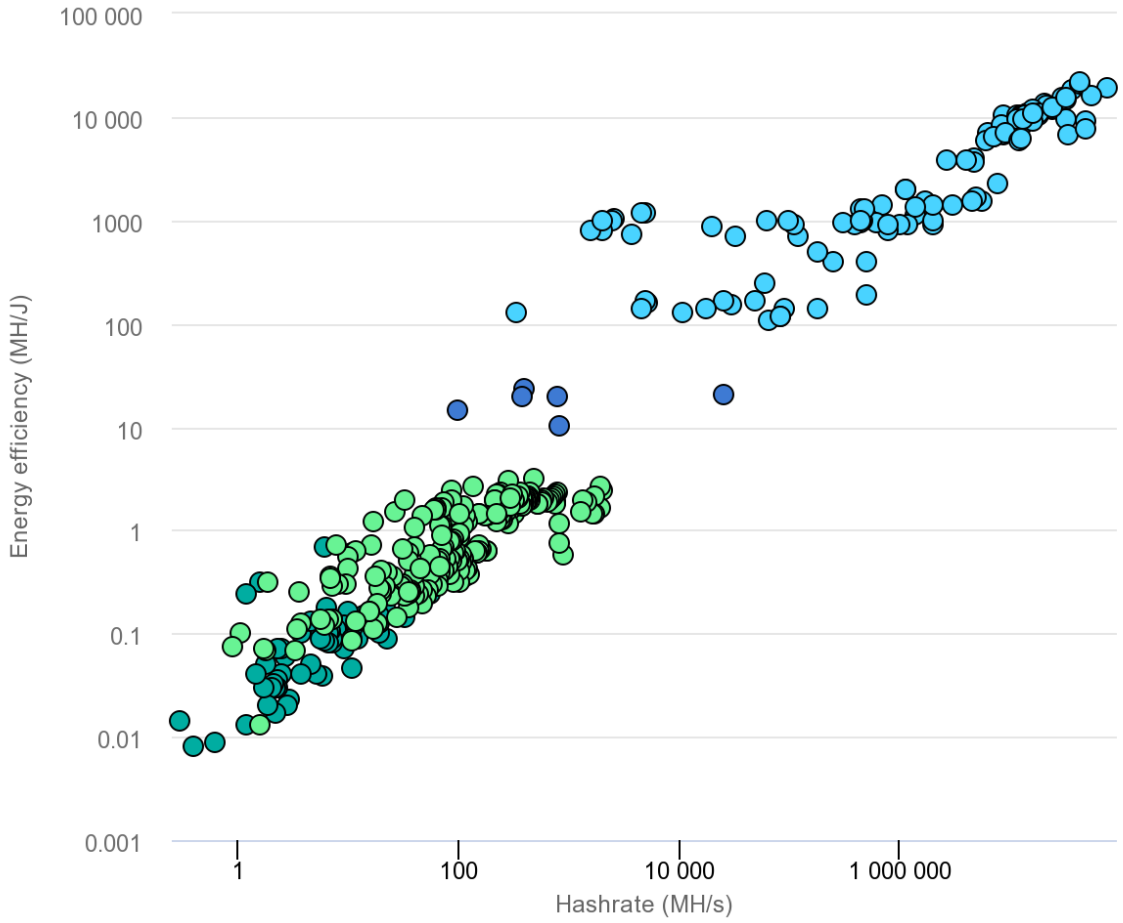
Další z možností zvýšení udržitelnosti těžby je vývoj efektivnějšího hardwaru pro těžbu. Tento vývoj se přirozeně děje od samotného vzniku Bitcoinu. Těžba kryptoměn je velmi konkurenční odvětví. Aby těžaři zůstali konkurence schopni, jsou nuceni maximalizovat svoje výnosy a minimalizovat náklady. To vede k přirozené prioritizaci hardwaru, který je schopný dosáhnout maximálního hashratu s minimální možnou spotřebou. Tato prioritizace těžařů vyvíjí tlak na výrobce těžebního hardwaru k vývoji těžebního hardwaru s vyšší efektivitou těžby, a tím dosažení totožného nebo vyššího výkonu s nižší spotřebou elektrické energie.

Těžební hardware Bitcoinu prošel od svého vzniku 4 hlavními etapami vývoje. Nejprve probíhala těžba na CPU. Obtížnost těžby byla zpočátku velmi nízká, nicméně při postupném zvyšování počtu zařízení připojených k síti obtížnost rostla a vzhledem k nízké efektivitě CPU přestala být těžba rentabilní. [46]

Z tohoto důvodu se v roce 2010 začal Bitcoin těžit na grafických kartách, které poskytovaly až 10x vyšší efektivitu než CPU. [46]

Třetí etapou vývoje hardwaru pro těžbu Bitcoinu byly tzv. FPGA (Field Programmable Gate Array) neboli programovatelné hradlové pole. FPGA opět umožnili zvýšit efektivitu těžby, ve srovnání s GPU byly až 5x energeticky úspornější. Těžba na nich však trvala přibližně pouhý rok (od roku 2011 do roku 2012). [47]

V roce 2012 přišly na trh první ASIC minery, zkratka je odvozena od Application Specific Integrated Circuit (překládá se jako zákaznický integrovaný obvod). Jedná se tedy o zařízení, které je zkonstruováno výhradně pro daný účel, v tomto případě pro těžbu Bitocinu. Díky tomuto úzkému zaměření bylo možné dosáhnout výrazně vyšší efektivity než u předchozího univerzálnějšího hardwaru. V průběhu let od prvního ASIC mineru proběhl výrazný vývoj v odvětví těžebního hardwaru, například velikost čipu byla postupně snížena z původních 130 nm na aktuálních 7 nm. Díky vývoji bylo v průběhu let bylo u současných ASIC minerů dosaženo až milionkrát vyšší efektivity těžby než při prvotní těžbě na CPU (viz obrázek 9.). Lze předpokládat, že (ač pravděpodobně už ne tak rychle) se bude těžební hardware dále vyvíjet a efektivita hardwaru bude růst. [48][49]



Obrázek 9. Efektivita těžebního HW v průběhu vývoje od CPU (tmavě zelené), přes GPU (světle zelené) a FPGA (tmavě modré), až k ASIC minerům (světle modré) [48]

II. PRAKTICKÁ ČÁST

4 PŘED TĚŽBOU

Ačkoliv může těžba laikovi připadat jako jednoduchý způsob, jak vydělat peníze a zajistit si pasivní příjem, existuje několik faktorů, které je nutné před začátkem samotné těžby zvážit. A to zvlášť v případě, kdy člověk plánuje do těžebního hardwaru investovat vyšší částky např. při nákupu většího počtu grafických karet a stavbě rigu. Jelikož je cílem těžaře maximalizovat hashrate (a tím zisky), je nutné volit poměrně výkonné karty. Výsledná investice se tedy může i při „domácí“ těžbě vyšplhat do desetitisíců až statisíců korun. Proto je nutné si nejprve udělat průzkum a zvážit všechny faktory.

4.1 Typ těžby

Drtivá většina amatérských těžařů preferuje GPU mining před jinými druhy těžby. A to z několika důvodů – grafické karty dokážou zpravidla těžit efektivněji než CPU nebo jiný hardware použitelný k „domácí“ těžbě. Navíc lze na jeden systém (základní desku, CPU, RAM, úložiště, zdroj) připojit několik grafických karet (konkrétní počet záleží na podpoře základní desky), zatímco u druhého nejpopulárnějšího způsobu „domácí“ těžby, CPU těžby, je nutné mít pro jeden procesor jeden systém. Pořizovací cena hardwaru vzhledem k zakoupenému výkonu vychází tedy u GPU těžby zpravidla výhodněji. Amatérští těžaři často těží na PC, na kterém zároveň pracují, což u GPU těžby zpravidla nebývá problém, a to za předpokladu, že při těžbě neběží na PC graficky náročné programy, jako jsou třeba programy pro úpravu videa, hry a podobně. Běžná kancelářská práce, jako je třeba prohlížení webu nebo práce s textovými editory, není těžbou prakticky vůbec ovlivněna a stejně tak není markantně ovlivněna efektivita těžby. Je možné tedy paralelně těžit a zároveň využívat PC k většině běžných činností. Naopak je tomu u CPU těžby, kde i běžná kancelářská práce výrazně snižuje efektivitu těžby, proto je nutné nezatěžovat procesor dalšími požadavky, kromě těžby, čímž se stává počítač při těžbě v podstatě nepoužitelný pro další činnosti. Pro GPU těžbu hraje také jednodušší údržba a možnost upgradu hardwaru oproti CPU. Je vhodné zmínit také těžbu na ASIC minerech, které však mezi amatérskými těžaři nejsou příliš rozšířené, a to především z důvodu zpravidla několikanásobně vyšší pořizovací ceny oproti grafickým kartám, vyšší energetické náročnosti a hlučnosti.

4.2 Výběr HW a rentabilita

Grafická karta je nejdůležitější součást počítače či rigu z hlediska těžby. Na trhu s grafickými kartami figurují 2 výrobci grafických čipů – AMD a Nvidia. Nelze říct, že by karty jednoho nebo druhého výrobce byly vhodnější pro minig – je nutné porovnávat konkrétní modely.

Cílem je zvolit hardware s co možná nejvyšší efektivitou těžby, ta je měřena jednotkou H/W (hashrate na watt, tedy jakého hashrate je hardware schopen dosáhnout při 1 wattu příkonu). Před investicí do hardwaru je nutné zvážit, zda je těžba pro těžaře za daných podmínek rentabilní. [3]

Důležité parametry grafické karty z pohledu těžby:

- Hashrate – hashrate neboli hashovací rychlost, liší pro jednotlivé těžební algoritmy, měří se v jednotce H/s (počet hashů za sekundu). Vyšší hashrate karty znamená vyšší výpočetní výkon, v praxi tedy vyšší odměnu pro těžaře. Pro jednu kartu se obvykle udává v MH/s.
- VRAM – větší a rychlejší paměti karty obecně znamenají vyšší hashrate. Pro tzv. memory-intensive algoritmy (algoritmy náročné na grafickou paměť), je velikost a rychlost VRAM tak podstatná, že v daném algoritmu je výkonnější než karta se silnějším procesorem, ale menšími či pomalejšími paměti. Některé algoritmy nepodporují karty s nižší velikostí paměti. Pro těžbu v současné době jsou obecně doporučovány karty s alespoň 6 GB VRAM. [4][5]
- Příkon – důležitý parametr z hlediska nákladů na těžbu. Nižší příkon znamená nižší náklady na energie, což vede ke zvýšení efektivity těžby (vyšší H/W). Karty s nižším příkonem také zpravidla dosahují nižších teplot, což vede k delší životnosti karet. [4]
- Chlazení – klíčový aspekt pro těžbu. Pokud je karta vybavená dobrým odvodem tepla, je možné ji následně při optimalizaci více přetaktovat a tím dosáhnout vyššího hashratu za teplot, kterých by dosáhla karta s horším chlazením při nižším taktu. Je tedy vhodné vybrat kartu s velkým heatsinkem (pokud není těžař omezen prostorem) a s ventilátory většího průměru (obecně jsou 2 ventilátory s větším průměrem tišší a účinnější než 3 menší). Kromě širších možností overclockingu a tedy vyšší výkonnosti těžby, má karta s kvalitním chlazením díky nižším provozním teplotám předpoklad k delší životnosti. [4]

- Dual/single BIOS – za předpokladu, že je těžař v problematice pokročilý a chce provádět úpravy v BIOSu karty, je vhodné vybrat kartu disponující funkcí double BIOS. Tyto karty obsahují dva BIOSy, mezi nimiž je možné přepínat. V případě, že těžař např. flashuje do karty mining BIOS (BIOS upravený speciálně pro těžbu) a něco se pokazí, může jednoduše přepnout na druhý, funkční BIOS, místo případného tzv. bricknutí karty. [4]

Existuje několik internetových srovnávačů, které porovnávají grafické karty z pohledu efektivity pro těžbu. Při výběru hardwaru mohou být dobrým pomocníkem.

Dobrým ukazatelem, zda se investice do hardwaru vyplatí je výpočet tzv. break-even pointu (bod zvratu – počet dní, kdy těžař „získá zpět“ prvotní investici do HW a začne těžit „do zisku“). Ten se dá vypočítat velmi jednoduše dle následujícího vzorce.

$$\mathrm{BEP} = \frac{\mathrm{C}_P}{\mathrm{D}_\mathrm{z}}$$

C_p – pořizovací cena těžebního hardwaru (v Kč)

D_z – denní zisk z těžby (v Kč/den)

Výpočet break-even pointu je samozřejmě pouze orientační, protože zisk z těžby je ovlivňován mnoha faktory a neustále se mění. Jedná se však o dobrý ukazatel, a to jak při vzájemném porovnávání jednotlivých karet, tak pro zvážení celkové rentability těžby.

Aktuální ziskovost těžby pro různý hardware, kryptoměny a cenu elektrické energie lze vypočítat pomocí internetových těžebních kalkulaček, názorný výpočet je proveden v kapitole „Proces přípravy SW nástrojů k těžbě“, konkrétně v podkapitole „Výběr kryptoměny k těžbě“.

4.3 Další faktory

V závislosti na konkrétní situaci může být vhodné věnovat pozornost dalším faktorům, jako jsou například dostatečné prostory pro těžební hardware, hlučnost, legislativa, dostatečné

technické znalosti, či možnosti alternativního využití hardwaru při potenciálním poklesu ziskovosti.

5 PROCES PŘÍPRAVY SW NÁSTROJŮ K TĚŽBĚ

Cílem této kapitoly je popis všech procesů a postupů, kterými si musí těžař projít pro funkční těžební stroj (ať už rig nebo grafickou kartu v PC), který je připraven a nakonfigurován k samotné těžbě, generující příjem v podobě kryptoměn do kryptoměnové peněženky. Součástí problematiky jsou různé softwarové nástroje. Těmi jsou například pooly, těžební software nebo peněženky. V této kapitole jsou tyto nástroje postupně shrnuty a analyzovány dle faktorů, které je nutné při výběru konkrétního nástroje zvážit. V určitých případech, kde figuruje několik zástupců konkrétního nástroje, je provedeno vzájemné srovnání nebo analýzy jednotlivých zástupců.

Pro celou praktickou část práce je využita grafická karta Nvidia GeForce RTX 2070 SUPER od výrobce GIGABYTE s 8 GB GDDR6 paměti.

5.1 Výběr kryptoměny k těžbě

Existují tisíce různých kryptoměn fungujících na principu PoW. Aby byla těžba smysluplná a naše grafická karta konkurenceschopná, je vhodné volit pouze z tzv. ASIC – resistant coinů. To jsou kryptoměny, jejichž protokol a těžební algoritmus je navržen tak, aby bylo zabráněno těžbě ASIC minery. Těžba ASICy je u těchto coinů buď znemožněna úplně, nebo by generovala i při velmi vysokém výpočetním výkonu ASICů zisk srovnatelný nebo nižší než při použití grafické karty či jiného konvenčního hardwaru. [6]

I po odfiltrování nerelevantních coinů pro těžbu na GPU má však těžař stále na výběr z tisíců kryptoměn. Přehled aktuálně nejpopulárnějších kryptoměn k těžbě se nachází v tabulce 1.

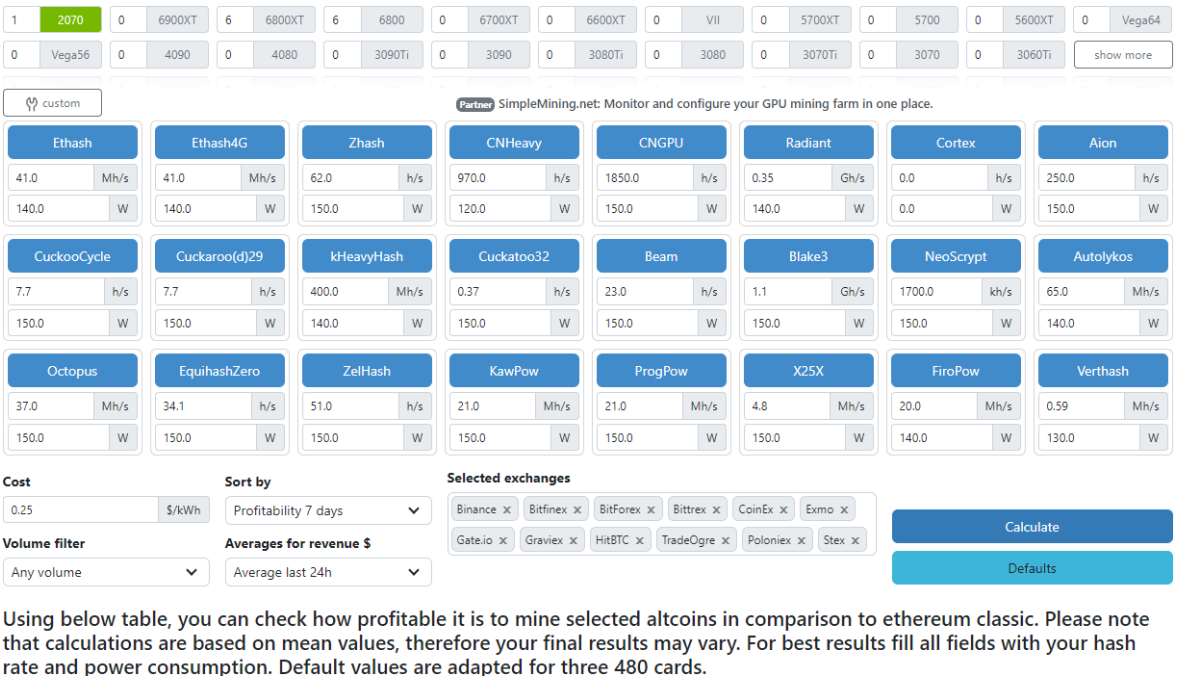
Tabulka 1. Populární coiny pro GPU těžbu

Název	Ethereum Classic	Conflux	Kaspa	Ravencoin	Firo	Ergo	Flux
Datum spuštění	2015	2018	2021	2018	2014	2019	2018
Max. množství (po vytěžení všech coinů)	210 700 000	527 816 420 274	28 704 026 601	21 000 000 000	21 400 000	97 739 924	440 000 000
Aktuální cena (23.2.2023)	$22,26	$0,294	$0,006935	$0,03557	$2,69	$1,74	$0,855
Tržní kapitalizace (23.2.2023)	$3 108 462 332	$612 337 197	$116 827 788	$431 445 646	$32 518 784	$101 909 410	$237 158 661
Trading volume za 24h (23.2.2023)	$184 619 762	$396 577 007	$2 386 523	$50 633 093	$3 823 795	$892 294	$29 438 733
Algoritmus	Etchash	Octopus	KHeavyHash	KawPow	Firo-Pow	Autolykos	ZelHash
Doba těžby 1 bloku	13 s	0,5 s	1 s	1 min	2,5 min	2 min	2 min
Odměna za blok (původní)	5 ETC	-	440 KAS	5 000 RVN	50 FIRO	-	150 FLUX
Odměna za blok (aktuální)	2,56 ETC	2 CFX	350 KAS	2 500 RVN	12,5 FIRO	48 ERG	75 FLUX
Odměna za blok (po příštím halvingu)	2,048 ETC	-	Záleží na příštím halvingu	1 250 RVN	6,25 FIRO	-	37,5 FLUX
Datum příštího halvingu	Květen 2024	Neprobíhá	Květen 2024 (odměna se snižuje průběžně)	Leden 2026	Září 2024	Neprobíhá	Srpen 2025
Omezení GPU pro těžbu	3 GB VRAM+	Nvidia 8 GB VRAM+	Není omezeno	4 GB VRAM+	5 GB VRAM+	2,5 GB VRAM+	3 GB VRAM+

Cílem těžaře je logicky snaha o maximalizaci zisku. Existují však různé strategie, kterými se může těžař při výběru coinu řídit. V této kapitole je prezentována ta nejvíce konzervativní – snaha zvolit jednu, co možná nejvíce stabilní a ziskovou kryptoměnu. Další, méně obvyklé a komplexnější strategie jsou analyzovány v kapitole „Další možnosti pro zvýšení profitability“, konkrétně v podkapitole „Mining strategie a techniky“.

Aktuální či krátkodobou ziskovost lze jednoduše vypočítat pomocí jedné z mnoha internetových těžebních kalkulaček. Po zadání vstupních parametrů (HW, na kterém chceme těžit a ceny elektrické energie) kalkulačka vypočítá ziskovost těžby pro jednotlivé coiny. Pro těžaře je tato kalkulačka velmi dobrým ukazatelem, který coin je aktuálně nejvýdělečnější,

a to nejen při prvotní volbě kryptoměny k těžbě. Faktory ovlivňující ziskovost se rychle mění, proto je dobré při těžbě občas kalkulačku použít a zjistit, zda není možné „přepnout“ na jinou kryptoměnu a tím zvýšit rentabilitu těžby. Níže je provedena ukázková kalkulace na kalkulačce WhatToMine.



Obrázek 10. Vstupní parametry do těžební kalkulačky dostupné na webu whattomine.com

Pro výpočet je nutné zadat vstupní parametry do těžební kalkulačky (viz obrázek 10.). Nejprve těžař zadá konkrétní hardware, na kterém hodlá těžit. V tomto případě je zadána 1x grafická karta Nvidia 2070, protože kalkulačka nenabízí model 2070 SUPER, který je v této práci využitý, nicméně parametry těchto karet jsou velmi podobné a jedná se pouze o orientační výpočet.

Dále nabízí kalkulačka možnost úpravy hashrate a příkonu karty pro jednotlivé těžební algoritmy, přičemž má předdefinované průměrné hodnoty pro danou kartu. Konkrétní hashrate a příkon před optimalizací karty nejsou známy, proto jsou zde ponechány výchozí hodnoty.

Poslední vstup, který musí uživatel zadat, je cena elektřiny za kWh. Zde je zadána částka 0,23 €/kWh (v přepočtu 5,45 Kč/kWh nebo $0,25/kWh), což je průměrná cena elektřiny české domácnosti v prvním pololetí roku 2022 (spotřební pásmo Dc s roční spotřebou mezi 2500 a 5 000 kWh). [1]

Zbylé nastavení je ponecháno defaultně.

Name(Tag) Algorithm	Block Time Block Reward Last Block	Difficulty NetHash	Est. Rewards Est. Rewards 24h	Exchange Rate	Market Cap Volume	Rev. BTC Rev. 24h	Rev. $ Profit	Profitability Current | 24h 3 days | 7 days
Kaspa(KAS) kHeavyHash	BT: 1.0s BR: 246.94 LB: 43,635,729	**150,676.093** 647.73 Th/s -0.8%	12.5282 12.4251	0.00000099 (CoinEx) 13.6%	$494,452,807 **45.75 BTC**	0.000012 0.000012	$0.38 **-$0.46**	279% | 284% 300% | **319%**
Alephium(ALPH) Blake3	BT: 4.0s BR: 2.90 LB: 667,379	**202,442,153M** 50.61 Th/s 0.3%	1.3614 1.3659	0.00000960 (Gate.io) 2.9%	$47,589,041 **1.73 BTC**	0.000013 0.000013	$0.33 **-$0.57**	295% | **303%** 292% | 276%
Nicehash-kHeavyHash kHeavyHash	BT: - BR: - LB: -	- 65.67 Th/s -6.0%	0.000012 0.000011	0.00003123 (Nicehash) 14.7%	- **1.89 BTC**	0.000012 0.000011	$0.26 **-$0.58**	**276%** | 247% 229% | 213%
Zano(ZANO) ProgPowZ	BT: 2m BR: 1.00 LB: 2,039,460	**5,138,368M** 42.82 Gh/s 0.8%	0.3176 0.3202	0.00003110 (Stex) 0.0%	$12,095,517 **4.12 BTC**	0.000010 0.000010	$0.27 **-$0.63**	223% | **230%** 227% | 224%
Conflux(CFX) Octopus	BT: 0.5s BR: 1.04 LB: 68,275,351	**4,293,924M** 8.63 Th/s -3.4%	0.7772 0.7261	0.00001360 (Gate.io) 6.8%	$1,030,082,189 **739.04 BTC**	0.000011 0.000010	$0.27 **-$0.63**	**239%** | 229% 222% | 222%
Sero(SERO) ProgPow	BT: 12.9s BR: 4.40 LB: 9,880,711	**567,639M** 44.00 Gh/s -8.3%	7.7316 7.0903	0.00000126 (Gate.io) -5.8%	$13,896,314 **8.50 BTC**	0.000010 0.000009	$0.29 **-$0.61**	221% | 207% 221% | **238%**
Nicehash-CuckooCycle CuckooCycle	BT: - BR: - LB: -	- 36.52 kh/s -38.0%	0.000009 0.000009	0.00120503 (Nicehash) -3.6%	- **0.07 BTC**	0.000009 0.000009	$0.25 **-$0.65**	205% | **218%** 209% | 210%

Obrázek 11. Výsledek kalkulace profitability těžby z webu whattomine.com

Po kliknutí na tlačítko Calculate kalkulačka vygeneruje výsledky. Nejméně ztrátovou kryptoměnou k těžbě je aktuálně kryptoměna Kaspa. Za posledních 24 hodin by karta vytěžila přibližně 12,5 jednotek této kryptoměny, kde i při okamžitém prodeji do USD a po odečtení nákladů na elektřinu by byl těžař ve ztrátě přibližně $0,46 (v přepočtu přibližně 10 Kč) denně (viz obrázek 11.). Při zadaných hodnotách a současných podmínkách by tedy těžba aktuálně (k 9.2.2023) rentabilní nebyla. [2]

Není však vhodné brát při výběru kryptoměny ohled pouze na kalkulačku. Tato konkrétní kalkulačka, umožňuje zobrazení ziskovosti pouze za posledních 7 dní a jak bylo zmíněno výše, faktory, jako je tržní cena kryptoměny nebo obtížnost těžby, které ovlivňují ziskovost se neustále mění. Proto je dobré sledovat dlouhodobý trend a zvolit coin, jehož ziskovost je nejvíce stabilní. Je vhodné si před těžbou udělat průzkum, zjistit, jak volatilní je tržní cena a obtížnost těžby dané kryptoměny, jaká je její tržní kapitalizace (čím vyšší, tím nižší pravděpodobnost velkých cenových výkyvů) a v neposlední řadě, zda je kryptoměna podporována na konvenčních burzách a zda je dostatečně likvidní (za předpokladu, že těžař plánuje její směnu do fiat měny).

5.2 Solo nebo pool?

Nelze jednoznačně říct, zda je pro těžaře vhodnější solo těžba nebo těžba v poolu, jelikož zde hraje velkou roli štěstí a pravděpodobnost. Obecně je však pro „domácí“ těžaře doporučována těžba v poolu. Amatérští těžaři obvykle dosahují nízkého hashratu, při kterém je pravděpodobnost nalezení bloku velice nízká. Aby si těžař dokázal představit, jaké tyto pravděpodobnosti jsou a mohl se rozhodnout, zda chce těžit v poolu nebo solo, je dobré si je spočítat pomocí následujících výpočtů.

Výpočet pravděpodobnosti nalezení následujícího bloku (v procentech):

$$\mathrm{P} = \left(\frac{\mathrm{H}_m}{H_c}\right) * 100$$

H_m = můj hashrate (v MH/s)

H_c = celkový hashrate sítě dané kryptoměny (v MH/s)

Počet dní statisticky potřebných pro nalezení bloku:

$$n = \frac{\frac{H_c}{H_m}}{\frac{1440}{t_B}}$$

H_m = můj hashrate (v MH/s)

H_c = celkový hashrate sítě dané kryptoměny (v MH/s)

t_B = block time – doba těžby jednoho bloku (v minutách)

Při modelové situaci těžby kryptoměny Kaspa na GPU Nvidia 2070 SUPER bude pravděpodobnost nalezení dalšího bloku 0,0000765 % při hashratu karty 400MH/s (obecně se na internetu pro tuto kartu a těžební algoritmus udává 300-500 MH/s) a celkovém aktuálním hashratu sítě 522,6 TH/s (522 600 000 MH/s k 15. 3. 2023).

Pro nalezení jednoho bloku je statisticky nutné těžit nepřetržitě 15,1 dne.

Při solo těžbě hraje velkou roli štěstí. Je možné najít blok během prvního dne těžby, ale zároveň může těžař těžit několik měsíců v kuse bez nalezení bloku. Proto není možné jednoznačně určit, zda je výhodnější solo těžba nebo těžba v poolu.

Pravděpodobnosti se u jednotlivých kryptoměn liší, záleží na hashratu celé sítě. Platí, že čím nižší výkon sítě je, tím je vyšší pravděpodobnost těžaře pro nalezení bloku. Obecně se tedy doporučuje solo těžba pouze pro větší těžaře, kteří jsou schopni poskytnout síti vyšší výpočetní výkon nebo pro těžbu kryptoměn s nižším celkovým výkonem sítě. Pro jednu z největších kryptoměn, kterou lze těžit na GPU, Ethereum Classic by stejná grafická karta statisticky našla blok až za 463 dní nepřetržité těžby, velmi pravděpodobně by tedy těžař těžil několik měsíců v kuse bez jakéhokoliv zisku. V tomto konkrétním případě by byla tedy rozhodně vhodnější těžba v poolu.

Jelikož těžba v poolu rozděluje vytěženou odměnu mezi účastníky poolu podle velikosti výpočetního výkonu, kterým do sítě přispějí, dá se říct, že těžbou v poolu oproti solo těžbě těžař statisticky neztratí nic, kromě poplatku danému poolu. Výhodou je pro něj ale stabilní příjem, kterým může průběžně pokrývat náklady na těžbu. Další nespornou výhodou těžby v poolu je, že těžař nemusí mít svůj vlastní uzel. Komunikuje s blockchainem skrze uzel poolu. Solo těžař musí disponovat svým vlastním plnohodnotným uzlem, jehož konfigurace a uvedení do provozu může být pro začátečníka poměrně komplikovaný proces (existují i pooly umožňující solo těžbu, v takovém případě není nutné provozovat vlastní uzel, nicméně zde těžař opět musí platit poplatek poolu).

5.3 Volba poolu

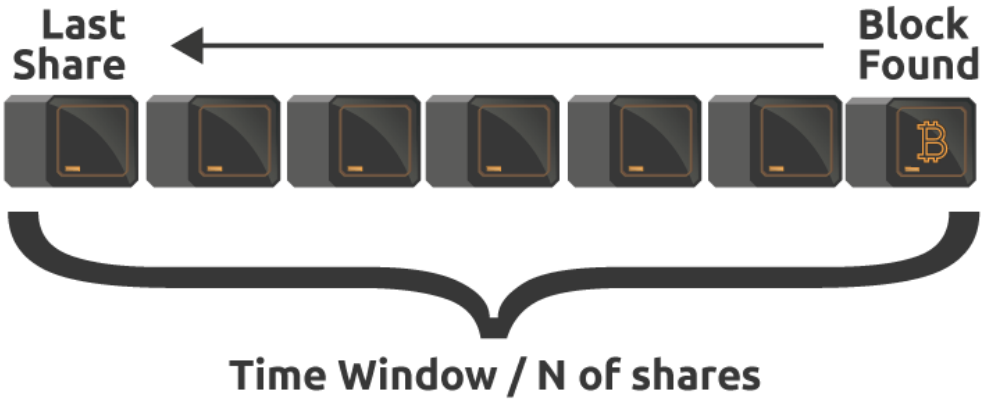
Za předpokladu, že se těžař rozhodne těžit v poolu, je nutné si udělat průzkum a důkladně zvážit, který pool je pro něj nejvýhodnější. Různé pooly disponují různými systémy odměňování a různými pravidly, jejichž preference se mezi konkrétními uživateli budou pravděpodobně lišit.

Tyto odměňovací systémy jsou metody, jimiž pool vypočítává, jak odměnit těžaře za poskytnutý výkon. Vzhledem k tomu, že tyto metody přímo ovlivňují zisk z těžby, jedná se o jeden z klíčových faktorů, které by měl těžař při volbě poolu důkladně zvážit. Níže jsou jednotlivé metody vysvětleny s konkrétními příklady.

- PPS (Pay-Per-Share) – V poolu s odměňovacím systémem PPS je stanovený celkový počet shares který je teoreticky potřebný k vytěžení bloku. Tento počet se odvíjí od aktuální obtížnosti těžby dané kryptoměny. Odměna pro každého těžaře je počítána podle toho, jakou poměrnou částí (jakým výpočetním výkonem) do tohoto celkového počtu shares těžař přispěje. Pool se zavazuje k vyplacení fixní odměny (dle poměrné části z celkového počtu shares), i když pool nevytěží daný blok. Z tohoto důvodu bývají v poolech s tímto systémem vyšší poplatky (obvykle 3-5 %). Pro pool je tato strategie poměrně riskantní, jelikož musí vyplatit těžaře stejnou částkou, nehledě na to, zda vytěžil blok. Pro těžaře je to naopak poměrně bezpečná metoda, zajišťující stabilní odměny. Nevýhodou je, že mezi těžaře nejsou rozdělovány transakční poplatky sítě. [7][8][10]

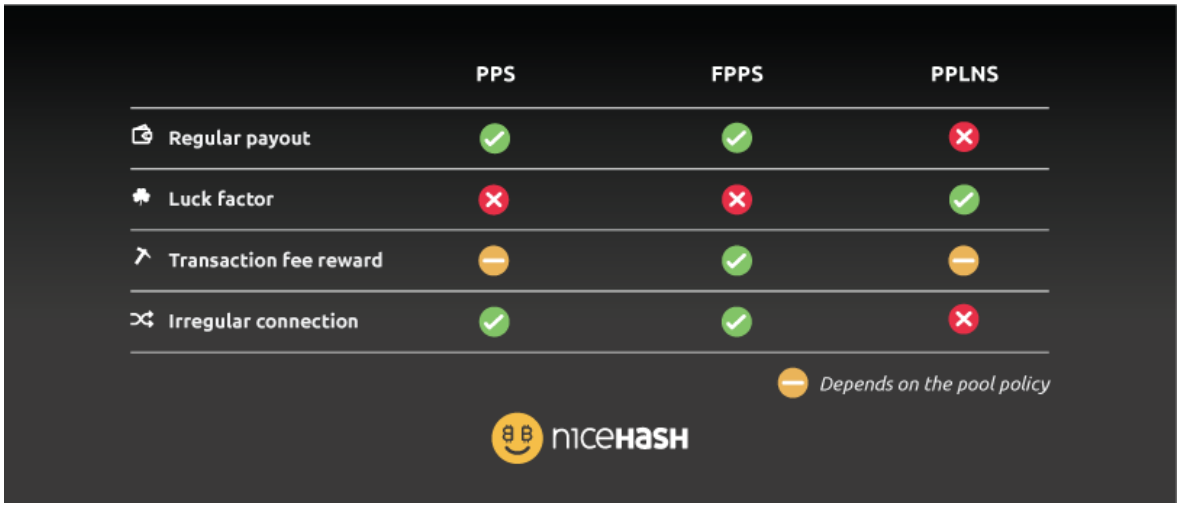
  Příklad: Pro nalezení bloku je teoreticky nutných 100 shares. Odměna za daných 100 shares je $100. Poolu se nepodaří vytěžit blok 9, ale podaří se mu vytěžit blok 10. Oba tyto bloky představují 100 a 100 shares. Do bloku 9 těžař přispěl 5 shares, do bloku 10 přispěl 7 shares. Celková odměna pro těžaře bude tedy $12.
- FPPS (Full Pay-Per-Share), PPS+ (Pay-Per-Share Plus) – Tyto dva systémy vystupující pod různými názvy jsou totožné. Jsou velmi podobné metodě PPS s jediným rozdílem, kterým je transakční poplatek. Na rozdíl od předchozího systému, v FPPS/PPS+ jsou vypláceny transakční poplatky těžařům. Samozřejmě za předpokladu, že pool vytěžil blok. Pro těžaře jsou tyto systémy oproti PPS zpravidla výhodnější, jelikož dostanou stejný podíl odměny + podíl z transakčních poplatků. [7][8][10]
- PPLNS (Pay-Per-Last N Shares) – V poolu se systémem PPLNS je také stanoven teoretický celkový počet shares nutný k nalezení bloku, nicméně těžaři je vyplacena odměna pouze v případě, že je blok poolem opravdu nalezen. Za předpokladu, že pool daný blok nenalezne, těžař odměnu nezíská (pokud se daný blok nenachází v block window). Velkou roli zde tedy hraje faktor štěstí. V případě nalezení bloku těžař získá odměnu nejen z aktuálního, úspěšně vytěženého bloku, ale i z určitého počtu předchozích bloků, které poolem vytěženy nebyly. Tomuto počtu se říká „block window“ nebo „time window“ (viz obrázek 12.). Block window se v jednotlivých poolech liší a závisí na aktuální obtížnosti těžby. Čím vyšší obtížnost těžby, tím větší block window (tzn. tím více posledních bloků od úspěšně vytěženého se

bere v potaz = tím vyšší potenciální odměna pro těžaře, nicméně pravděpodobnost nalezení bloku daným poolem je nižší). Z tohoto důvodu se těžba v PPLNS poolu vyplatí především pro těžaře, kteří jsou k danému poolu připojeni konstantně a „nepřeskakují“ mezi různými pooly. Také je důležité mít dobré internetové připojení. Rozdělování transakčních poplatků mezi těžaře zde závisí na politice konkrétního poolu. Tento systém neposkytuje tak stabilní výdělky jako předchozí systémy, nicméně pokud má daný pool štěstí, mohou těžaři dosáhnout výdělků vyšších, ale i nižších. Pro pool není tato metoda tak riskantní, protože pokud se poolu nacházet bloky nedaří, těžaře nevyplácí. Z tohoto důvodu se poplatek PPLNS poolům pohybuje okolo 1-2 %. [7][8][9][10]



Obrázek 12. Block window [10]

Příklad: Pro nalezení bloku je teoreticky potřebných opět 100 shares. Odměna za daných 100 shares je $100. Danému poolu se podaří vytěžit blok číslo 10. Těžař přispěje 5 shares. Block window se vztahuje na bloky 8 a 9 (i když pool dané bloky nevytěžil), které představují dalších 100 a 100 shares, do nich těžař svým výpočetním výkonem přispěl dalšími 7 a 10 shares. Odměna pro těžaře bude tedy dohromady $22, a to za 5 shares z bloku 10, 7 shares z bloku 8 a 10 shares z bloku 9. Za předchozí bloky, které pool nevytěžil, ani se na ně nevztahuje block window, těžař odměnu nezíská.



Obrázek 13. Přehled jednotlivých odměňovacích systémů poolů [10]

Odměňovacích systémů existuje mnohem více, nicméně drtivá většina poolů používá tyto tři.

Dalším neméně důležitým faktorem je geografické umístění serverů poolu. Čím menší je vzdálenost mezi servery poolu a těžařem, tím je obvykle nižší pravděpodobnost zvýšeného výskytu tzv. stale shares (poskytnutí share pro vytěžení bloku v době, kdy byl daný blok již vytěžen), za které těžař nezíská odměnu.

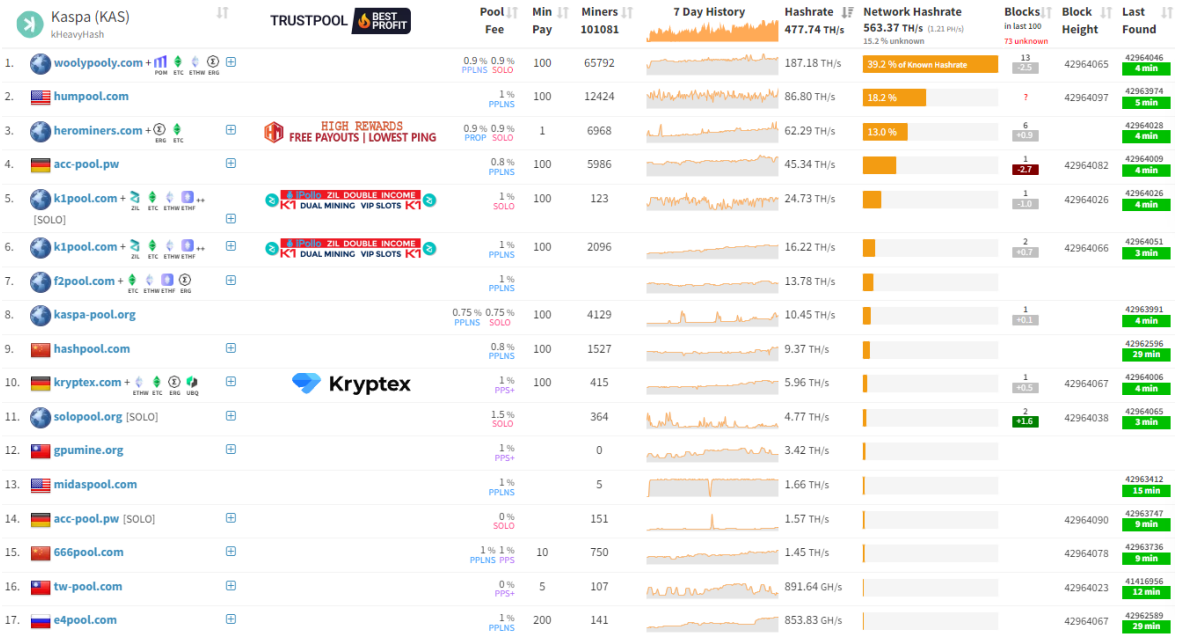
Zejména pro malé těžaře je potom také klíčovým parametrem minimum payout threshold, který určuje minimální vyplatitelnou částku, jíž si může těžař poslat do peněženky. Tato částka se mezi jednotlivými pooly může lišit až v řádu tisícinásobků. Nezřídka se stává, že si těžař neprostuduje pravidla poolu, a když si chce nechat vyplatit odměnu, zjistí, že na minimum payout zdaleka nedosahuje a je v daném poolu „uvězněn“ po několik dalších týdnů či měsíců těžby. Proto je důležité si před začátkem samotné těžby u daného poolu tento parametr zjistit.

Faktorem, který přímo ovlivňuje zisk z těžby jsou již výše zmíněné poplatky neboli fees poolu. Ty se běžně pohybují v rozmezí 0-5 % a logicky se většina těžařů snaží o jejich minimalizaci.

Zisk může ovlivňovat také stabilita poolu, proto je při průzkumu dobré zkontrolovat, zda daný pool často netrpí downtimes, útoky na pool nebo jinými problémy.

V neposlední řadě je také dobré zjistit, jakou má daný pool reputaci mezi těžaři. Recenze či zkušenosti těžařů s daným poolem se lze dočíst na sociálních sítích nebo serverech věnujících se těžbě.

Existují srovnávací servery poolů, které umožňují zobrazení dostupných poolů pro jednotlivé kryptoměny a spolu s nimi potřebné informace pro volbu poolu, čímž tento proces uživatelům podstatně usnadňují. Jedním z nich je například server MiningPoolStats dostupný na adrese miningpoolstats.stream (viz obrázek 14.)



Obrázek 14. Srovnání dostupných poolů pro kryptoměnu Kaspa na serveru miningpoolstats.stream

Pro tuto práci byl zvolen pool Kryptex který nabízí odměňovací systém PPS+ s nízkým poplatkem ve výši 1 %, servery umístěnými v Německu a minimálním payoutem 10 mincí. [11]

5.4 Volba mining software

Lze říct, že volba mining softwaru není pro těžaře tak zásadní, jako volba poolu. Většinou fungují na stejném principu a jejich uživatelské rozhraní bývá velmi podobné. Volně dostupné, základní programy většinou komunikují s těžařem skrze příkazový řádek, pokročilejší a komplexnější programy potom disponují grafickým uživatelským rozhraním (náročné

GUI však není žádoucí, jelikož by mohlo negativně ovlivnit hashrate karty). Můžou se lišit podporou různých funkcí a mírou customizace, bez toho se však běžný těžař většinou obejde. Existují desítky různých minerů, které podporují různé těžební algoritmy, výrobce hardwaru a operační systémy (srovnání některých z nich se nachází v tabulce 2.). Proto je nutné se ujistit, že daný miner podporuje požadovaný algoritmus, HW a operační systém.

Jediným faktorem, který zde přímo ovlivňuje zisk z těžby je poplatek. Podobně jako u poolu, i zde platí těžař poplatek vývojáři daného softwaru. U běžných minerů bývá poplatek zpravidla procentuální podíl z vytěžené částky. Obvykle se pohybuje od 0,5 do 3 %, ve výjimečných případech až 5 %.

Běžně se stává, že se hashrate stejné karty za totožných podmínek mírně liší napříč různými minery. Proto z hlediska maximalizace efektivity může být dobrým krokem vyzkoušet více různých programů.

Pro správu většího počtu karet či rigů jsou potom vhodné samostatné operační systémy, které jsou přímo uzpůsobené pro těžbu (např. Hiveon OS, MinerOs, Mining OS atd.). Ty jsou většinou založené na Linuxu.

Tabulka 2. Těžební SW podporující algoritmus KHeavyHash

Název	Poplatek	OS	HW
lolMiner	0,75 %	Windows/Linux	Nvidia/AMD
GMiner	1 %	Windows/Linux	Nvidia
TeamRedMiner	1 %	Windows/Linux	AMD
BZMiner	1 %	Windows/Linux	Nvidia/AMD
SRBMiner	0,85 %	Windows/Linux	Nvidia/AMD

Pro tuto práci byl zvolen těžební software lolMiner, který oproti konkurenci poptává nižší poplatek. Kromě toho nabízí funkce jako optimalizace karty skrze příkazový řádek (bez nutnosti použití externího programu) nebo vlastní customizaci okna statistik. [12]

5.5 Volba peněženky

Posledním softwarovým/hardwarovým nástrojem nezbytným k započetí těžby je peněženka. Teoreticky není nutné vlastnit peněženku jako takovou (ať už softwarovou nebo hardwaro-

vou), stačí disponovat kryptoměnovou adresou a znát privátní klíč, aby bylo možné s přijatými kryptoměnami za těžbu poté manipulovat. Nejbezpečnějším a uživatelsky nejpřívětivějším způsobem správy adresy a jejího privátního klíče je však krypto peněženka.

Pokud se jedná o malého těžaře s nízkým hashratem, který neplánuje vytěžené prostředky v peněžence dlouhodobě držet, bude mu pravděpodobně stačit softwarová peněženka. Takových peněženek existují desítky, a to ať už v podobě stažitelného software, mobilní aplikace nebo webové peněženky. Záleží tedy pouze na konkrétních preferencích daného uživatele, nicméně vždy se těžař musí ujistit, že daná peněženka podporuje konkrétní kryptoměnu, kterou hodlá těžit. Z bezpečnostních důvodů je vždy lepší volit známější peněženky od renomovaných vývojářů. V historii je známo několik případů, kdy byly tyto peněženky vykradeny samotnými vývojáři. Druhé, velké riziko leží na straně samotného uživatele. V případě napadení jeho zařízení malwarem, jsou prostředky na peněžence v ohrožení a teoreticky odcizitelné. Peněženky bývají také často terčem hackerských útoků. Softwarové peněženky se dají se považovat za bezpečné pro přeposílání prostředků, či držení malých částek, nicméně nejsou vhodné pro dlouhodobé držení většího množství peněz.

Za předpokladu že se jedná o většího těžaře, který pracuje s vyššími částkami nebo když plánuje uživatel vytěžené prostředky na peněžence dlouhodobě držet, je vhodné investovat do hardwarové peněženky. Nejlevnější z nich začínají na částce okolo 1500 Kč. Předními výrobci těchto peněženek jsou Trezor a Ledger, přičemž všechny hardwarové peněženky (nehledě na výrobce) poskytují daleko vyšší bezpečnost než peněženky softwarové. Veškerá komunikace mezi počítačem a peněženkou je offline, tudíž prostředky v peněžence jsou v bezpečí i v případě, že je dané zařízení infikované malwarem.

Prostředky lze z poolu odesílat také přímo do kryptoměnové burzy či směnárny, což značně usnadňuje jejich potenciální prodej, nicméně z bezpečnostních důvodů se to obecně nedoporučuje.

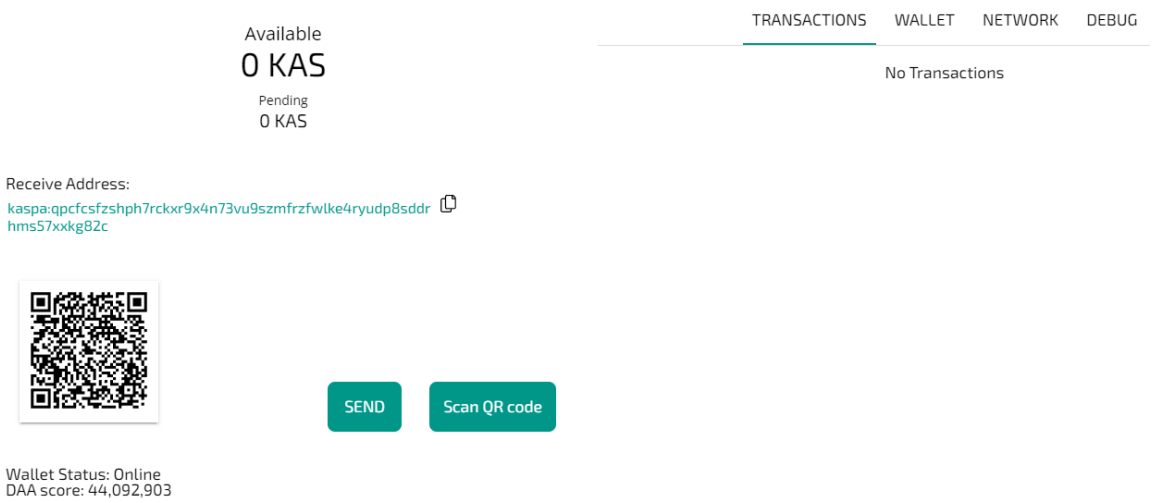
V tomto konkrétním případě (těžby kryptoměny Kaspa na jedné grafické kartě) byla zvolena webová peněženka dostupná na adrese wallet.kaspanet.io. Jedná se o nativní peněženku, která je vyvíjena samotnými vývojáři kryptoměny.

6 SPUŠTĚNÍ TĚŽBY

Samotná implementace těchto nástrojů pro spuštění těžby je z uživatelského hlediska velmi jednoduchá.

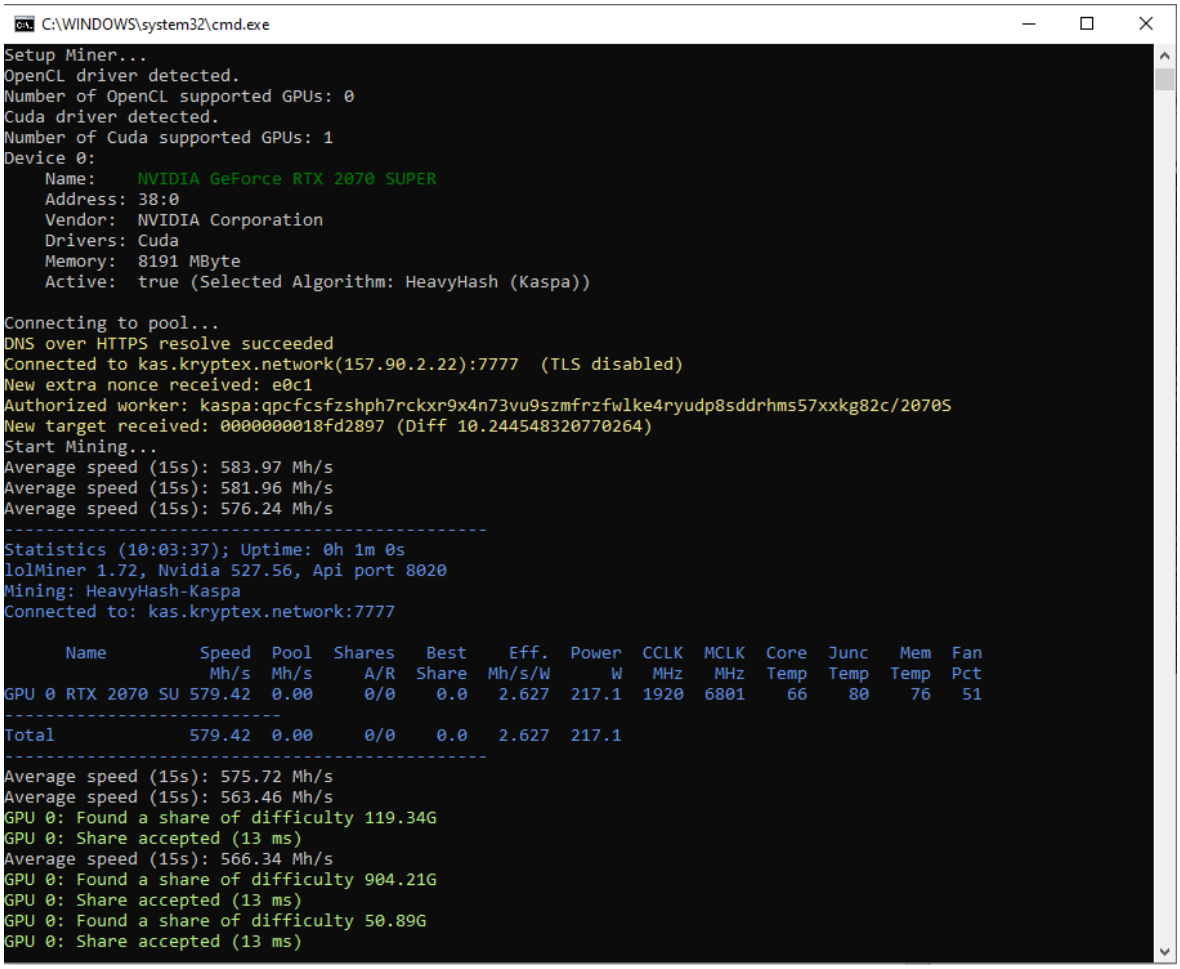
Nejdříve je nutné stáhnout těžební software (pokud možno z oficiální stránky vývojáře nebo z oficiálního repozitáře na GitHubu) pro požadovaný operační systém. Zpravidla se jedná o ZIP soubor, který obsahuje soubory s příponou BAT pro minerem podporované kryptoměny a pooly, jejichž spuštěním se spouští samotná těžba.

Před spuštěním těžby je však nutné daný soubor nakonfigurovat pro těžbu v požadovaném poolu a na požadovanou adresu. To je možné provést úpravou konkrétního BAT souboru, kam musí uživatel zadat vlastní adresu peněženky (viz Receive Address na obrázku 15.) a adresu serveru a port daného poolu (tyto informace nalezne těžař na webu konkrétního poolu).



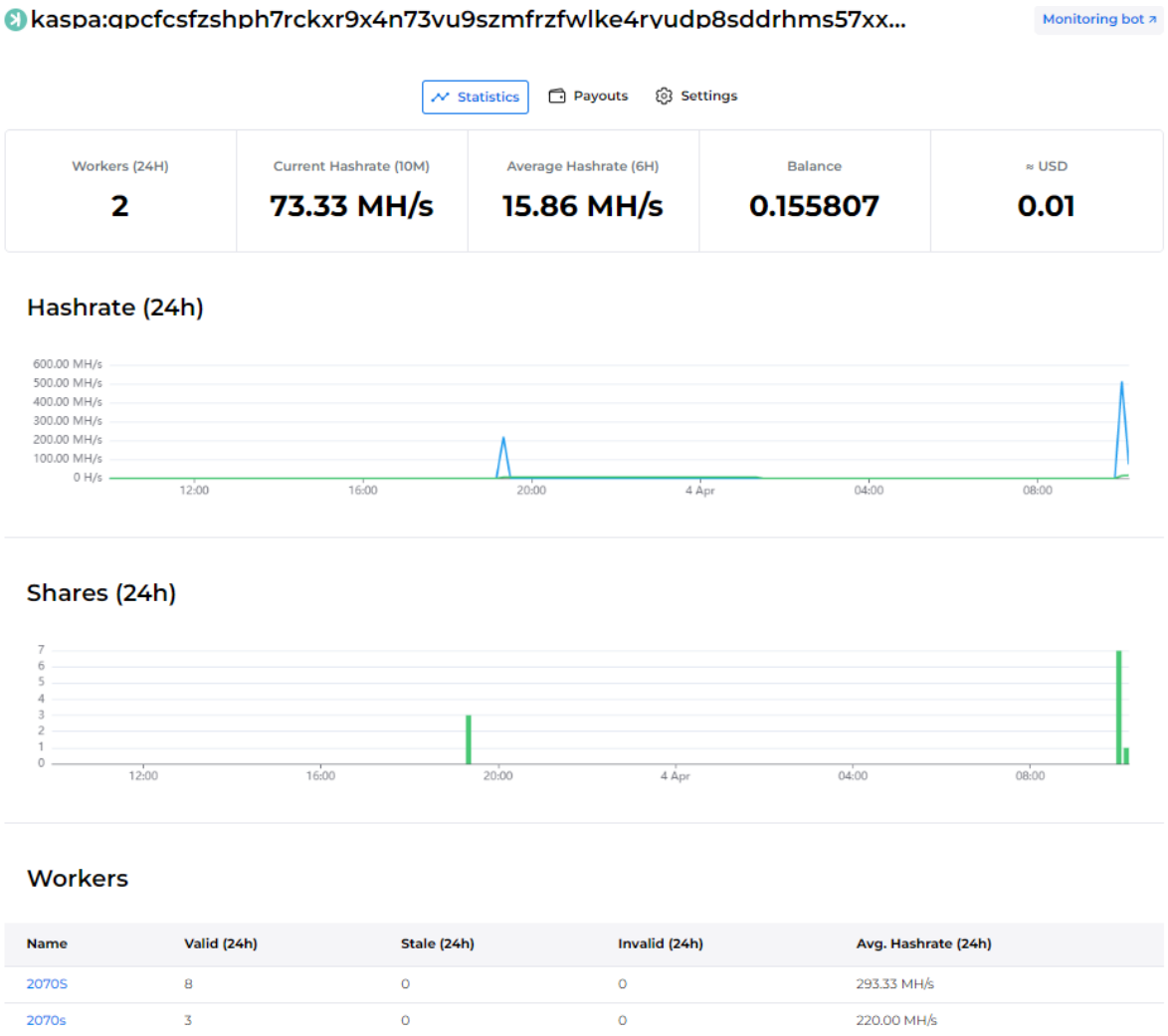
Obrázek 15. Uživatelské rozhraní peněženky dostupné na wallet.kaspanet.io

Poté je možné spuštěním tohoto souboru spustit samotnou těžbu. Otevře se jednoduché rozhraní v podobě příkazového řádku, které však obsahuje pro těžaře všechny potřebné informace, například připojení k poolu, adresu, aktuální hashrate, počet nalezených shares, efektivitu těžby, takt jádra a pamětí karty, teploty a otáčky ventilátorů GPU (viz obrázek 16.). Takováto těžba (bez jakékoliv optimalizace karty) je však extrémně neefektivní.



Obrázek 16. Uživatelské rozhraní softwaru lolMiner při těžbě

Po několika desítkách minut těžby se začnou statistiky propisovat také do webového rozhraní poolu (viz obrázek 17.), které je pro těžaře velmi důležité, protože zde po zadání konkrétní adresy vidí informace jako jsou aktuální hashrate, průměrný hashrate, počet shares a v neposlední řadě „vytěžené“ množství kryptoměny, které náleží těžaři jako odměna za poskytnutý výkon. Skrze toto rozhraní může také těžař (v některých poolech) zažádat o vyplacení odměny na svoji adresu.



Obrázek 17. Uživatelské rozhraní poolu Kryptex dostupné na pool.kryptex.com

7 OPTIMALIZACE GPU PRO TĚŽBU

Grafická karta dokáže těžit s továrním nastavením bez jakékoliv optimalizace, ale jak bylo již řečeno v předchozí kapitole, těžba s tímto továrním nastavením je velmi neefektivní. Se správnou optimalizací karty je možné dosáhnout násobně vyšší efektivity těžby.

Standartně má karta z výroby nastavené parametry jako jsou např. core clock, memory clock nebo core voltage na určitou hodnotu. Tyto hodnoty se na jednotlivých modelech karet liší. Jsou nastaveny tak, aby karta dobře fungovala pro většinu různých činností, ne však pro těžbu. Pro těžbu je žádoucí tyto parametry upravit tak, aby byla těžba co možná nejvíce efektivní. Tomuto procesu se říká optimalizace.

Úpravou výše zmíněných parametrů se mění tři základní proměnné: hashrate, příkon, teplota. Pro tuto práci je za ideální nastavení karty považováno takové, kde jsou tyto proměnné v rovnováze a je dosahováno maximální efektivity (poměru hashratu a příkonu) za co nejnižších možných teplot (vysoké provozní teploty výrazně zvyšují rychlost opotřebení hardwaru). Takové nastavení bude pravděpodobně ideální ve většině situací pro většinu těžařů.

Přesné ideální nastavení karty není možné dohledat, a to z několika důvodů:

- Preference mezi uživateli se liší – zatímco pro většinu těžařů může být vhodná výše zmíněné ideální nastavení, existuje mnoho těžařů, pro které by toto nastavení vhodné nebylo. Např. za předpokladu, že těžař těží s minimálními nebo žádnými náklady na elektřinu – zde by byla na místě maximalizace hashratu bez ohledu na rostoucí příkon.
- Rozdílné paměti – Výrobci karet běžně implementují do karet stejného modelu paměti od jiných výrobců. Nejčastěji jsou používány paměti od výrobců Samsung, Hynix a Micron. Paměti od různých výrobců se budou s totožnou optimalizací chovat jinak, proto je vhodné konkrétní nastavení přizpůsobit konkrétním pamětem. V závislosti na výrobci paměti se může hashrate karty lišit až od 12 %. [4]
- Silicon lottery – Dokonce ani žádné 2 karty se stejnými paměti se nebudou chovat při optimalizaci stejně, jelikož žádné 2 čipy nejsou totožné. Přetaktování, které jedna karta stabilně zvládá, může na druhé kartě způsobovat pády či nestabilitu. Tyto rozdíly způsobují drobné kvalitativní nuance při výrobě čipu, které však mohou zapříčinit znatelný rozdíl v maximálním taktech, při kterém je karty schopny stabilně pracovat. Tuto problematiku popisuje termín „silicon lottery“. [13]

- Každý těžař těží v jiných podmínkách – podmínky pro těžbu, jako je například okolní teplota, chlazení počítače či rigu ovlivňují teplotu jádra a pamětí karty. Těžař s dobře chlazeným hardwarem si tak může dovolit optimalizaci s vyšším hashratem, která produkuje více tepla než těžař, kterého teplota limituje.

Proto je téměř nutné experimentovat a pokusit se optimální nastavení nalézt.

Optimalizace pro rozdílné karty a různé těžební algoritmy se provádí stejným způsobem, nicméně výsledná ideální nastavení budou ve většině případů rozdílná. U karet je to zapříčiněno odlišnými parametry různých karet, u těžebních algoritmů pak povahou samotného algoritmu. Z tohoto hlediska jsou algoritmy obvykle děleny na tzv. memory-intensive (při těžbě jsou primárně zatěžovány paměti) a core-intensive (při těžbě je primárně zatěžováno jádro).

Příklad: nastavení efektivní pro těžbu kryptoměny Ethereum Classic bude extrémně neefektivní pro těžbu kryptoměny Kaspa na totožném hardwaru. Těžební algoritmus první zmíněné kryptoměny – Etchash je totiž memory-intensive (vyššího výkonu lze dosáhnout především přetaktováním pamětí), zatímco algoritmus KHeavyHash je naopak core-intensive (zde je důležitý především core overclock).

7.1 Způsoby optimalizace

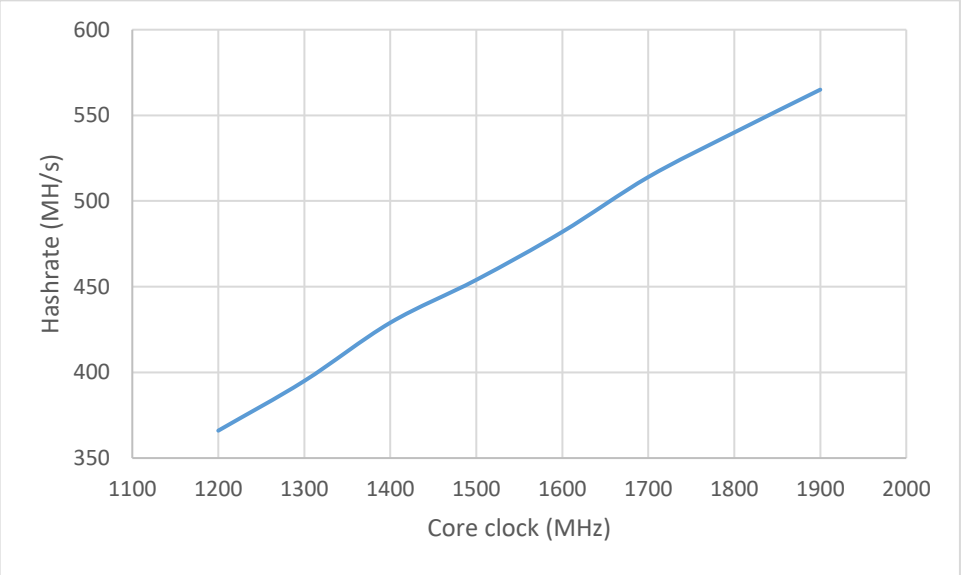
7.1.1 Overclocking

Přetaktováním je možné zvýšit počet operací, které karta zpracuje za jednotku času, v praxi to znamená vyšší výkon karty. Při těžbě je tímto úkonem dosaženo vyššího hashratu. S rostoucím hashratem však roste také roste příkon a teplota, při velmi vysokých hodnotách se může projevit nestabilita karty.

7.1.1.1 Core clock

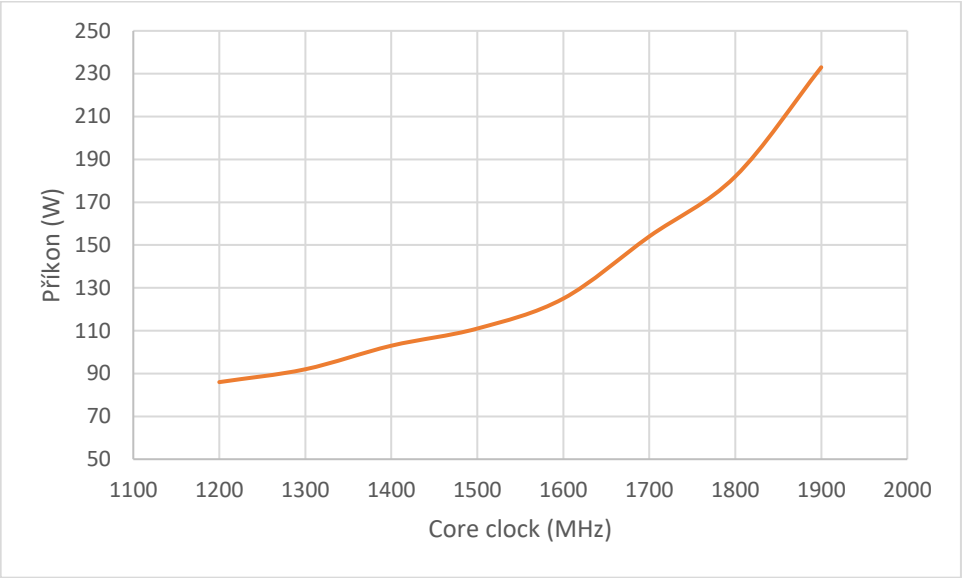
Takt jádra neboli core clock je důležitý především pro core-intensive algoritmy. Pro zjištění závislosti hashratu, příkonu a teploty bylo provedeno měření při reálné těžbě kryptoměny Kaspa (algoritmu KHeavyHash) na grafické kartě Nvidia 2070 SUPER. Veškeré úpravy v následujících měřeních byly prováděny přímo v těžebním softwaru lolMiner. V rámci tohoto měření byly v těžebním softwaru měněny hodnoty taktu jádra pomocí parametru Locked core clock od 1200 do 1900 MHz, přičemž bylo provedeno měření při zvýšení o každých

100 MHz. Ostatní parametry byly ponechány na továrním nastavení. Hodnoty byly sledovány jak v těžebním softwaru, tak v programu MSI Afterburner, který umožňuje sledovat průběh některých měřených veličin v grafu a s vyšší přesností než právě těžební software. Výsledky měření lze vidět na grafech níže.



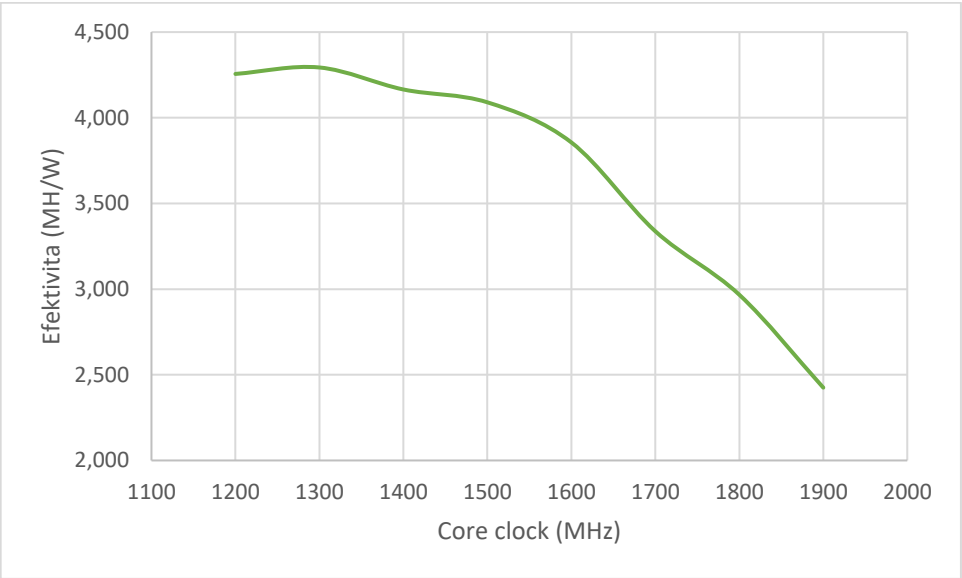
Graf 1. Hashrate v závislosti na core clock

Na grafu 1. lze vidět, že s rostoucím taktem jádra lineárně roste také výsledný hashrate. Při nejnižším měřeném taktu dosahovala karta hashratu 366 MH/s, při nejvyšším pak 565 MH/s. Mezi nejvyšší a nejnižší měřenou hodnotou tedy vzrostl hashrate o 54,4 %.



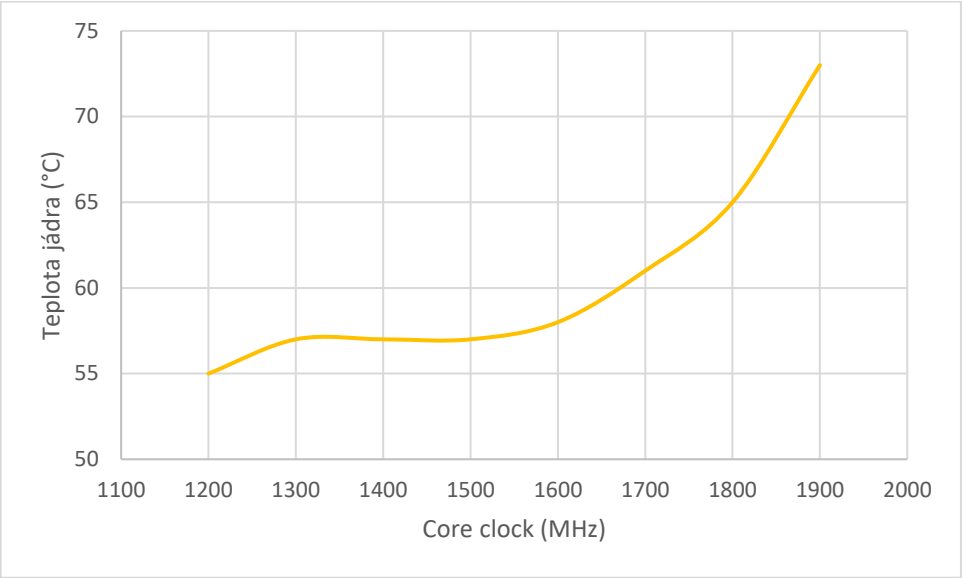
Graf 2. Příkon v závislosti na core clock

S rostoucím hashratem však také výrazně roste příkon (viz. graf 2.). Ač by se tedy z prvního grafu mohlo zdát, že přetaktování karty na nejvyšší možný stabilní takt, nesoucí s sebou výrazný nárůst hashratu je dobrá strategie, ve většině případů tomu tak nebude. Na rozdíl od hashratu, který rostl lineárně, výsledná křivka z naměřených hodnot příkonu připomíná spíše exponenciálu. Při taktu 1200 MHz potřebovala karta pro provoz 86 W, zatímco při taktu 1900 MHz to bylo 233 W. Jedná se tedy o nárůst o 170,9 %.



Graf 3. Efektivita v závislosti na core clock

Poměr těchto dvou veličin je efektivita těžby, která znázorněna v grafu 3. Maximální efektivita těžby byla při továrním nastavení karty, pouze s měnícím se taktem jádra nalezena při hodnotě 1300 MHz a to 4,293 MH/W. Minimální naměřenou efektivitou byla hodnota 2,425 MH/W při frekvenci 1900 MHz, kde karta sice dosahovala nejvyššího hashratu, ale také nejvyššího příkonu.



Graf 4. Teplota jádra v závislosti na core clock

S rostoucím taktem jádra rostla také jeho teplota, jejíž průběh je možné vidět na grafu 4. Nejnižší naměřenou teplotou jádra byla teplota 55 °C, která byla dosažena při nejnižším měřeném taktu, nejvyšší potom 73 °C, ta byla dosažena při nejvyšším měřeném taktu. Téměř všechny naměřené teploty lze považovat pro kartu za bezpečné. Výraznější nárůst teplot lze pozorovat až v pásmu od 1700 do 1900 MHz, které je ale pro těžbu neefektivní. Z tohoto důvodu není nutné se teplotami v tomto případě dále zabývat.

7.1.1.2 Memory clock

Memory clock neboli takt pamětí karty je důležitý především pro memory-intensive algoritmy. Pro core-intensive algoritmy je naopak žádoucí snížení taktu pod tovární úroveň, čímž je možné podstatně snížit provozní teploty.

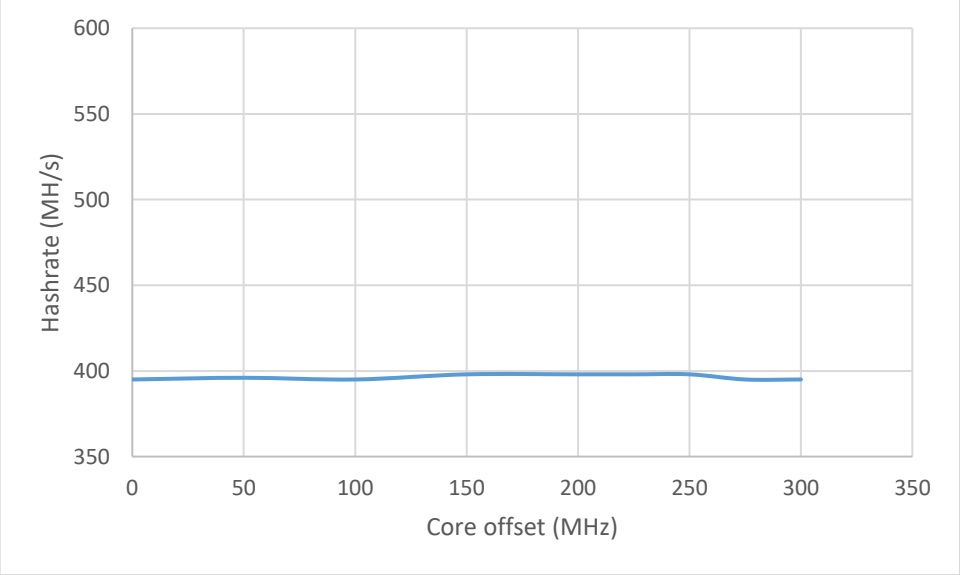
Tovární hodnota memory clocku u karty Nvidia 2070 SUPER při těžbě se uzamčeným core clockem na hodnotě 1300 MHz je 6801 MHz. Při tomto memory clocku dosahovala karta hashratu 395 MH/s při 92 W. Po snížení memory clocku na minimální možnou hodnotu 810

MHz bylo dosaženo totožného hashratu při příkonu 75 W. Snížení memory clocku je tedy u core-intensive algoritmů, jako je KHeavyHash, dalším způsobem pro zvýšení efektivity. V tomto případě bylo dosaženo zvýšení z 4,293 na 5,267 MH/W. Podobné chování lze předpokládat také u ostatních core-intensive algoritmů.

7.1.2 Undervolting

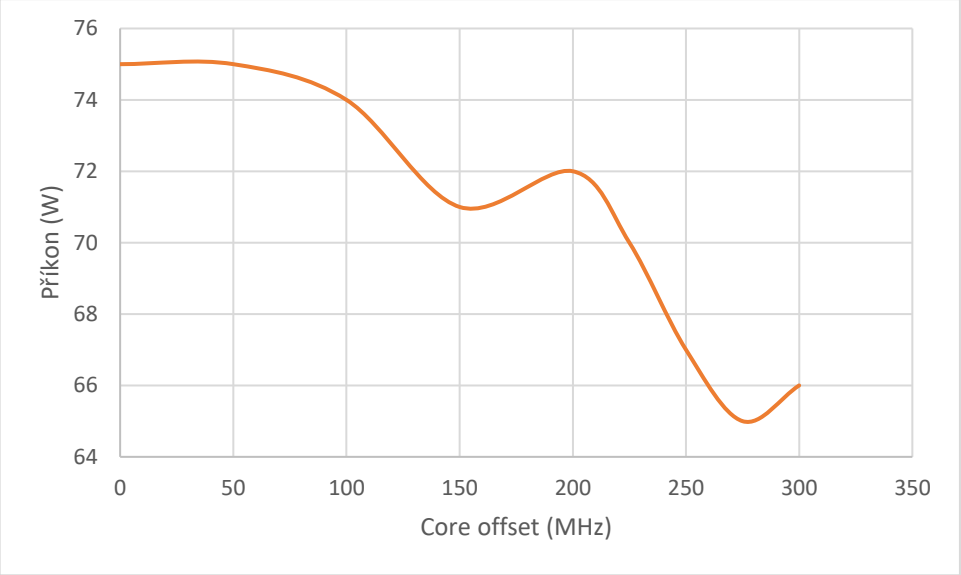
Undervolting ovlivňuje příkon karty. Lze provádět obvykle skrze úpravu nastavení core voltage nebo power limit (závisí na používaném softwaru a výrobci karty). Při výchozím nastavení karta často využívá více elektrické energie, než k danému úkonu potřebuje. Snížením příkonu karty je zvýšena efektivita těžby. Příkon však může být snížen pouze do bodu, kde je zachována stabilita karty, za přílišného snížení by karta nepracovala stabilně (pokud by nebyl snížen i core clock).

V softwaru lolMiner lze k tomuto účelu využít parametr core clock offset (zkráceně core offset). Jeho nastavením lze v kombinaci s uzamčenou frekvencí jádra snížit napětí na jádře a tím snížit příkon karty. Opět bylo provedeno několik měření pro různé hodnoty tohoto parametru (0, 50, 100, 150, 200, 225, 250, 275 a 300 MHz), a to při core clocku 1300 MHz a memory clocku 810 MHz. Výsledky lze vidět na grafech níže.



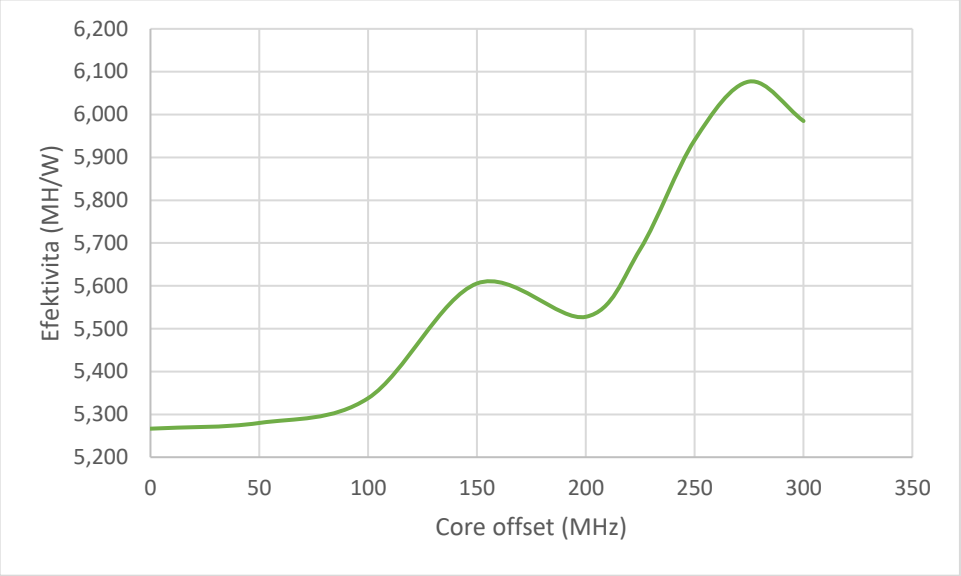
Graf 5. Hashrate v závislosti na core offset

Hashrate zůstal při různých hodnotách core offsetu téměř neměnný (viz graf 5.), minimální naměřená hodnota hashratu je 395 MH/s, maximální pak 398 MH/s, rozdíl je tedy zanedbatelný.



Graf 6. Příkon v závislosti na core offset

Cílem úpravy tohoto parametru je však dosáhnout nižšího příkonu karty, čehož bylo dosaženo. Výslednou křivku příkonu v průběhu jednotlivých měření lze vidět na grafu 6. Příkon byl nejvyšší při hodnotách 0 a 50 MHz, a to konkrétně 75 W. Při hodnotě 275 MHz byl zjištěn nejnižší příkon 65 W. Při měření na hodnotě 300 MHz karta přestala být stabilní a způsobila pád systému.



Graf 7. Efektivita v závislosti na core offset

Efektivitu pro jednotlivá měření je možné vidět na grafu 7. Vzhledem ke konstantnímu hashratu je nejvyšší právě při nejnižším příkonu. Maximální efektivita byla 6,077 MH/W při hodnotě 275. Úpravou core offsetu bylo tedy dosaženo dalšího zvýšení efektivity.

7.1.3 BIOS modding

Úprava BIOSu karty neboli BIOS modding je dalším způsobem optimalizace karty. Cílem je změnit časování pamětí karty za účelem dosažení vyššího hashratu. Je však složitější a rizikovější než overclocking nebo undervolting a zpravidla není tak efektivní jako právě výše zmíněné metody. Lze navíc provést pouze u některých karet a při nesprávném provedení může dojít k bricknutí karty (jejímu znehodnocení). [66]

Existuje několik dalších způsobů optimalizace, nicméně výše zmíněné jsou nejběžnější a nejefektivnější.

7.2 Teploty

Při rostoucím hashratu při optimalizaci karty se však obecně zvyšují také teploty. Ty jsou pro těžaře také velmi důležitým ukazatelem, jelikož stálá těžba při příliš vysokých teplotách z dlouhodobého hlediska snižuje životnost hardwaru. Proto se je těžaři snaží udržet na co

možná nejnižších hodnotách. Obecně jsou za bezpečné provozní teploty považovány hodnoty okolo 70 °C pro jádro a 90 °C pro paměti (karty nižších řad však obvykle nemají teplotní senzor na pamětech a je možné sledovat teplotu pouze na jádru).

Nejjednodušším způsobem pro snížení teplot je softwarová korekce otáček ventilátorů karty, zpravidla se uvádí procentuálně (kde 100 % je maximální výkon). Vyšší otáčky vedou k rychlejšímu opotřebování ložisek ventilátoru, nicméně jejich výměna (v poměru k ceně nové karty) není nákladná.

Dalším způsobem je výměna původních thermal padů karty, a to nejen v případě jejich opotřebení. Originální thermal pady často nebývají dostatečně kvalitní (zejména u karet Nvidia řady 30) a jejich výměna za kvalitnější může vést k podstatnému snížení teplot. Tímto krokem však uživatel ve většině případů přichází o záruku.

Snížit teploty karty je možné samozřejmě kromě softwarové optimalizace karty také snížením okolní teploty nebo přidáním externího chlazení.

7.3 Optimální nastavení

Pro nalezení nejefektivnějšího nastavení je vhodné výše zmíněné způsoby kombinovat. V tabulce 3. je možné vidět všechna testovaná nastavení a hodnoty, kterých bylo při měření dosaženo, seřazené sestupně podle nejvyšší dosažené efektivity.

Tabulka 3. Všechna testovaná nastavení a dosažené hodnoty

Core clock (MHz):	Memory clock (MHz):	Core offset (MHz):	Hashrate (MH/s):	Příkon (W):	Efektivita (MH/W):	Denní profitabilita* (USD):
1300	**810**	**275**	395	65	6,077	-0,163
1320	**810**	**275**	399	66	6,045	-0,167
1280	**810**	**275**	390	65	6,000	-0,166
1300	**810**	**300**	395	66	5,985	-0,169
1300	**810**	**250**	398	67	5,940	-0,173
1500	**810**	**275**	454	78	5,821	-0,207
1470	**810**	**200**	444	77	5,766	-0,207
1200	**810**	**275**	362	63	5,746	-0,170
1350	**810**	**275**	412	72	5,722	-0,195
1300	**810**	**225**	398	70	5,686	-0,191
1400	**810**	**275**	426	75	5,680	-0,205
1300	**810**	**150**	398	71	5,606	-0,197
1300	**810**	**200**	398	72	5,528	-0,203
1300	**810**	**100**	395	74	5,338	-0,217
1300	**810**	**50**	396	75	5,280	-0,222
1300	**810**	**0**	395	75	5,267	-0,223
1600	**810**	**250**	484	93	5,204	-0,280
1400	**810**	**0**	426	86	4,953	-0,271
1300	**6801**	**0**	395	92	4,293	-0,325
1200	**6801**	**0**	366	86	4,256	-0,306
1400	**6801**	**0**	429	103	4,165	-0,372
1500	**6801**	**0**	454	111	4,090	-0,405
1600	**6801**	**0**	482	125	3,856	-0,473
1700	**6801**	**0**	514	154	3,338	-0,629
1800	**6801**	**0**	540	182	2,967	-0,782
1890	**6801**	**0**	562	230	2,443	-1,057
1900	**6801**	**0**	565	233	2,425	-1,073

Maximální efektivita | Nestabilní nastavení | Tovární nastavení

*Denní profitabilita pro dané nastavení vypočítaná podle vzorce v kapitole „Výpočet profitability“ ke dni 27.4.

Defaultní nastavení karty, kde nebyly žádné parametry jakkoliv upravovány, je vyznačeno žlutě, při něm bylo dosaženo poměrně vysokého hashratu, ale za cenu velmi vysokého příkonu, s výslednou efektivitou 2,443 MH/W. Při červeně vyznačených nastaveních nebyla

karta při těžbě stabilní. Nejvyšší dosažená efektivita byla zjištěna při nastavení core clock 1300 MHz, memory clock 810 MHz a core offset 275 MHz. Při tomto nastavení byl sice oproti továrnímu nastavení snížen hashrate z 562 na 395 MH/s (pokles o 29,7 %), nicméně byl výrazně snížen příkon, a to z 230 W na 65 W (pokles o 71,7 %). Výsledná efektivita dosažená při tomto nastavení byla 6,077 MH/W. Optimalizací bylo tedy v tomto případě dosaženo téměř 2,5násobného zvýšení efektivity oproti defaultnímu nastavení karty. Tato nastavení se však týkají pouze této konkrétní karty Nvidia 2070 SUPER a algoritmu KHeavyHash, nicméně principy optimalizace jsou u všech karet a algoritmů totožné či velmi podobné.

V reálném čase bude pro těžaře pravděpodobně směrodatnější aktuální profitabilita než efektivita, nicméně faktory jako jsou difficulty nebo aktuální tržní cena kryptoměny se neustále mění, čímž se mění také profitabilita, zatímco efektivita karty zůstává konstantní. Z dlouhodobého hlediska nebo při porovnání karet či jejich nastavení lze uvažovat efektivitu, která ve většině případů je přímo úměrná s profitabilitou.

V krajních případech, například při extrémním růstu cen a pádu cen elektrické energie se vyplatí upřednostňovat vyšší hashrate za cenu vyššího příkonu a naopak.

8 VÝPOČET PROFITABILITY

Pro výpočet ziskovosti těžby za 24 hodin lze pro tento těžební algoritmus využít následující vzorec (výnosová část vzorce převzata z příspěvku z diskusního fóra viz odkaz do sezamu použité literatury, nákladová část vypracována autorem).

$$\left(\frac{H_m \times B_r \times 86400 \times 10^6}{\mathrm{D} \times 2^{32}}\right) \times \mathrm{C_k} - \left(\frac{\mathrm{P}}{1000} \times 24\right) \times \mathrm{C_e}$$

[43]

H_m = můj hashrate (v MH/s)

B_r = block reward – odměna za vytěžený blok dané kryptoměny

D = difficulty – obtížnost těžby dané kryptoměny

C_k = aktuální kurz za jednu minci dané kryptoměny (v USD)

P = příkon hardwaru na kterém probíhá těžba (ve W)

C_e = Cena za 1 kWh energie (v USD)

Níže je výpočet proveden pro těžbu při továrním nastavení karty, tedy bez jakékoliv optimalizace (k 27.4.2023 s cenou elektřiny 5,45 Kč ($0,25) vycházející z českého průměru pro rok 2022). [1]

$$\left(\frac{562 \times 233{,}08 \times 86400 \times 10^6}{250281{,}9 \times 2^{32}}\right) \times 0{,}03067 - \left(\frac{230}{1000} \times 24\right) \times 0{,}25 = -1{,}057$$

Tentýž výpočet je proveden pro nejefektivnější nalezené nastavení (k 27.4.2023 s totožnou cenou elektrické energie jako ve výpočtu výše).

$$\left(\frac{395 \times 233{,}08 \times 86400 \times 10^6}{250281{,}9 \times 2^{32}}\right) \times 0{,}03067 - \left(\frac{65}{1000} \times 24\right) \times 0{,}25 = -0{,}163$$

Těžba kryptoměny Kaspa na grafické kartě Nvidia 2070 SUPER bez jakékoliv optimalizace, při ceně elektřiny 5,45 Kč/kWh by generovala denní ztrátu $1,057 (přibližně 23 Kč), zatímco při totožných podmínkách, ale při nejefektivnější nalezené optimalizaci by byla denní ztráta $0,163 (přibližně 3,5 Kč).

Je nutné podotknout, že výpočty výše uvažují pouze příkon grafické karty, nikoliv příkon celé sestavy. Pro každé testované nastavení v tabulce 3. byl měřen wattmetrem také příkon celé sestavy ze zásuvky, přičemž přírůstek příkonu způsobený ostatními komponenty sestavy se pohyboval od 85 W při energeticky nejúspornějším nastavení, po 105 W při energeticky nejnáročnějším nastavení. Přírůstky u ostatních nastavení se pohybovaly vždy mezi těmito krajními hodnotami (popis komponentů testované sestavy v této práci se nachází v tabulce 4.). Pokud by byla uvažována těžba s jednou grafickou kartou v PC, který by nebyl při těžbě aktivně využíván k jiným účelům, tzn. jeho jediným účelem by byla právě těžba, bylo by nutné přičíst tyto přírůstky k příkonu grafické karty, čímž by byl uvažován příkon celé sestavy. Tento přírůstek je však individuální a nelze s ním kalkulovat vždy. Za předpokladu, že by těžař disponoval více grafickými kartami připojenými k jednomu systému, dělil by se příkon zbytku systému právě počtem grafických karet. V rámci těžebního rigu lze připojit k jednomu systému desítky grafických karet, s rostoucím počtem karet vliv příkonu zbytku systému na profitabilitu klesá.

Tabulka 4. Testovaná sestava

Komponenta	**Výrobce a model**
CPU	AMD Ryzen 5 3500X
GPU	GIGABYTE GeForce RTX 2070 SUPER WINDFORCE OC 3X 8G
HDD	WESTERN DIGITAL WD BLUE 1TB WD10EZEX
SSD	ADATA Ultimate SU630 240GB
Základní deska	MSI B450 GAMING PLUS (MS-7B86)
RAM	A-DATA Technology 16GB 1333MHz DDR4
Zdroj	GIGABYTE P650B - 650W

Výsledkem obou výpočtů bylo zjištěno, že je těžba i aktuálně jedné z neziskovějších kryptoměn pro těžbu (viz obrázek 11.) při daných podmínkách v tuto chvíli ztrátová (jak bylo již v práci predikováno dříve). Tato ztrátovost je však způsobena současnou ne příliš příznivou situací na kryptoměnových trzích a zároveň aktuálně vysokými cenami elektrické energie v České republice. Za předpokladu růstu cen kryptoměn a snížení cen elektrické energie lze

očekávat zvýšení rentability těžby. I skrze ztrátovost lze však na výsledcích výpočtů pozorovat výrazný vliv optimalizace karty.

9 DALŠÍ MOŽNOSTI PRO ZVÝŠENÍ PROFITABILITY

Jsou těžaři, pro které je těžba koníčkem a zisk je až na druhém místě, drtivá většina těžařů však těží pro zisk. Proto se jej snaží maximalizovat. Základním způsobem je vhodná optimalizace hardwaru, které se věnuje kapitola „Optimalizace GPU pro těžbu“. Existují ale i další způsoby, jak potenciálně zvýšit ziskovost těžby, těmi se zabývá tato kapitola.

9.1 Mining strategie a techniky

9.1.1 Dual mining

Dual mining umožňuje těžbu dvou kryptoměn současně na jedné grafické kartě. Zpravidla se provozuje těžba jedné core-intensive a druhé memory-intensive kryptoměny, jejichž současnou těžbou jsou zatíženy jak paměti karty, tak jádro. Vyšší zatížení karty způsobuje zvýšení provozních teplot a vyšší spotřebu elektrické energie. Předpokladem pro rentabilní dual mining je nízká cena energií, účinné chlazení a podpora této techniky těžebním softwarem. Pokud jsou tyto podmínky splněny, lze dosáhnout touto technikou vyšší ziskovosti.

9.1.2 Spec mining

Spec mining je strategie, kdy těžař spekuluje na pozdější růst ceny těžené kryptoměny. Zpravidla je těžena nově vytvořená kryptoměna s nízkou obtížností těžby, což umožňuje těžaři získat velký počet mincí, které těžař drží a prodává až po potenciálním růstu tržní ceny. Tato strategie má však také jistá rizika. Nově vytvořené kryptoměny často nelze nikde z počátku obchodovat a nemusí se tak stát ani v budoucnu, ve výsledku tedy těžař spotřebuje energii pro těžbu kryptoměny, jejíž prodej není možné realizovat. Pokud se však těžaři spekulace podaří, lze při prodeji dosáhnout velkého zisku. Vývojáři však neustále vyvíjejí tisíce nových kryptoměn, přičemž uspěje pouhý zlomek z nich a potenciální úspěch konkrétního projektu lze jen velmi těžko predikovat.

9.1.3 Profit Switch

Profit switch umožňuje automaticky přepínat těžaři mezi několika kryptoměnami. Těžař si zvolí několik kryptoměn, pro které software následně z parametrů jako je aktuální obtížnost těžby, aktuální tržní cena a odměna za blok vypočítává aktuální ziskovost. Následně probíhá

těžba vždy nejziskovější kryptoměny. Tato funkce musí být podporována těžebním softwarem, který zpravidla poskytuje těžaři další možnosti, jako například nastavení rozdílu v ziskovosti pro přepnutí na jinou vybranou kryptoměnu nebo minimální čas těžby těžené kryptoměny. Rentabilita těžených kryptoměn se neustále mění a díky této technice může těžař dosáhnout vyšších zisků z těžby. [71]

9.2 Využití energie z fotovoltaické elektrárny

Solární panely jsou již dnes v domácnostech poměrně běžné a předpokládá se, že jejich popularita dále poroste. Často se však stává (obzvláště v létě), že fotovoltaická elektrárna vyrobí více energie, než domácnost spotřebuje, čímž vznikají tzv. přebytky elektřiny. Ty lze využít různými způsoby. Bez uzavření smlouvy proudí tato elektřina zpět do sítě zadarmo. Po uzavření smlouvy na výkup přebytků je lze odprodat zpět dodavateli, nicméně výkupní ceny bývají zpravidla daleko nižší než ceny odebírané elektřiny. Efektivnějším způsobem pro využití těchto přebytků může být těžba kryptoměn. Při těžbě pouze z přebytků (těžba pouze při svitu slunce) bude však návratnost pravděpodobně investice do těžebního hardwaru poměrně dlouhá. Řešením může být nepřetržitá těžba při napájení z baterií, nicméně v takovém případě dochází k jejich rychlejšímu opotřebování. Výsledná rentabilita tohoto řešení je ovlivněna mnoha faktory, které je nutné před investicí zvážit. [72][73][74]

9.3 Využití odpadního tepla pro vytápění

Způsobům využití odpadního tepla v průmyslové těžbě se věnuje kapitola „Využití odpadního tepla“, nicméně využít odpadní teplo lze i při těžbě v domácnosti. Nejčastějším způsobem pro využití tepla z těžby v domácnosti je pravděpodobně vytápění. Vytápět lze jednoduše buď místnost, ve kterém se těžební hardware nachází, nebo celý dům napojením výpočetní jednotky pro těžbu na topný okruh objektu. Miroslav Konečný provedl ve své diplomové práci experiment druhého zmíněného příkladu, kde do otopné soustavy rodinného domu implementoval výpočetní jednotku pro těžbu kryptoměn skládající se ze 6 grafických karet s vodním chlazením. Nepřetržitou těžbou kryptoměn na výpočetní jednotce byla ohřívána voda v akumulační nádobě, kterou byl následně vytápěn objekt. Experiment probíhal nepřetržitě od ledna do prosince roku 2018. Výsledkem byla úspora elektrické energie na vytápění a ohřevu vody oproti předchozímu roku (při téměř totožné celkové roční spotřebě

tepla) téměř 82 % s tím, že bylo využito 65 % odpadního tepla vyprodukované výpočetní jednotkou. Pořizovací náklady výpočetní jednotky byly 160 000 Kč a čistý zisk z prodeje vytěžených kryptoměn za rok 2018 byl 50 306 Kč. Je však nutné podotknout, že experiment probíhal v roce 2018, který byl oproti současnosti pro těžbu kryptoměn příznivější. [75]

9.4 Housing

Dalším způsobem, jak je možné snížit náklady na těžbu a tím zvýšit ziskovost může být pronájem prostor pro těžbu. Existují různé společnosti, které se specializují na provoz datových center pro těžbu kryptoměn a následný pronájem těchto prostor pro těžaře. Tyto prostory bývají obvykle průmyslové haly, ve kterých je možné provozovat tisíce karet/ASIC minerů. Největší výhodou housingu je výrazně levnější energie, kde právě díky velkoobjemovým odběrům energie tohoto hardwaru dokáže poskytovatel dosáhnout zlomku ceny elektrické energie oproti domácnostem. Další výhodou bývá zpravidla profesionální chlazení a zabezpečení těchto prostor. Provozovatelé housingu často nabízejí další služby, jako je kompletní servis hardwaru či jeho případné restarty, lze tedy využívat housing i v zahraničí, kde je to obvykle výhodnější díky nižším cenám elektrické energie. Pronájem těchto prostor však většinou dává smysl při až těžbě s větším výpočetním výkonem.

Velmi výhodné housingy pro těžbu kryptoměn jsou nabízeny například na Islandu, kde je cena elektrické energie nízká. V červnu 2022 zde byla cena elektrické energie pro podniky s ročním odběrem 1000000 KWh pouhých $0,07/KWh, v přepočtu přibližně 1,5 Kč/KWh (tedy přibližně 3,5x levnější než ve stejném období pro českou domácnost). Zhruba 85 % celkové produkce elektrické energie Islandu navíc pochází z obnovitelných zdrojů (primárně geotermální energie), v takovém případě tedy lze mluvit o udržitelné těžbě. Níže je proveden výpočet ziskovosti těžby podle vzorce z kapitoly „Výpočet profitability“ pro potenciálním housingu s cenou energie $0,07. Zbylé proměnné jsou ponechány stejně jako ve výpočtu pro těžbu s optimálním nastavením. [1][76][77]

$$\left(\frac{395 \times 233{,}08 \times 86400 \times 10^6}{250281{,}9 \times 2^{32}}\right) \times 0{,}03067 - \left(\frac{65}{1000} \times 24\right) \times 0{,}07 = \ 0{,}118$$

Z výpočtu je patrné, že při těchto podmínkách by bylo možné těžit ziskově, a to při denním zisku zhruba $0,118 (přibližně 2,6 Kč). Do tohoto výpočtu není započítán poplatek za housing, který si určuje poskytovatel. Pro smysluplnou těžbu v těchto podmínkách by však bylo nutné disponovat daleko vyšším výpočetním výkonem.

ZÁVĚR

Cílem práce bylo seznámit čtenáře s problematikou těžby kryptoměn, a to jak principiálně z teoretického hlediska, tak z praktického – z pohledu těžaře.

Teoretická část se v úvodu zabývá technologiemi kryptoměn, které souvisejí se samotnou těžbou. Konkrétně jsou popisovány technologie Bitcoinu, jelikož se jedná o největšího a nejstaršího zástupce kryptoměn, jehož principy využívají tisíce dalších z nich. Nejprve je vysvětlena asymetrická kryptografie, kterou Bitcoin využívá ve formě digitálního podpisu k odesílání transakcí. Dále je vysvětlena technologie blockchain, která je základním stavebním kamenem celé sítě. Blockchain je tvořen bloky, které obsahují transakce. Se znalostí těchto technologií je možné pochopit teoretický princip těžby a mechanismus Proof of Work, čemuž se věnuje další část.

Druhá polovina teoretické části se zabývá často kritizovanou udržitelností těžby a možnostmi pro její zvýšení. Snížit energetickou náročnost Bitcoinu na zlomek současné by bylo možné přechodem na algoritmus Proof of Stake, to by bylo v současnosti však pravděpodobně velmi riskantní. Nižšího dopadu těžby na životní prostředí by mohlo být také dosaženo vyšším poměrem energie z obnovitelných zdrojů v energetickém mixu, který těžaři využívají. Vzhledem ke klesajícímu trendu cen obnovitelné energie, lze předpokládat, že se tento poměr „zelené“ energie bude zvyšovat. Dalšími popsanými možnostmi jsou průmyslové využití odpadního tepla, což představuje další příjem pro těžaře a vývoj efektivnějšího hardwaru pro těžbu. Vzhledem k vysoce konkurenčnímu prostředí v odvětví těžby kryptoměn, lze ve výše zmíněných možnostech očekávat přirozený vývoj k udržitelnější těžbě.

Praktická část se zaměřuje na těžbu z pohledu těžaře. V první kapitole jsou popsány faktory, které by měly být zváženy před samotnou investicí do hardwaru. Prvním faktorem ke zvážení je typ těžby. V této práci je prezentována těžba na grafické kartě, která je vhodná pro většinu amatérských těžařů. Dále je nutné zvážit výběr konkrétního hardwaru, zda se investice vyplatí, zda má těžař vhodné podmínky pro těžbu a podobně. Další kapitoly se věnují procesu vedoucímu ke spuštění těžby, kterým si musí projít každý těžař. Existuje několik softwarových prostředků, které jsou pro těžbu nezbytné, v těchto kapitolách je provedena analýza jejich zástupců, vzájemná srovnání a konkrétní volby pro tuto práci (preference mezi těžaři se však budou lišit). Následně je provedeno názorné spuštění samotné těžby.

Pro efektivní těžbu je však nutné hardware optimalizovat. Cílem optimalizace je dosažení rovnováhy veličin jako je hashrate, příkon a teplota. Tyto veličiny ovlivňují profitabilitu

těžby. Tomu se věnuje následující kapitola, ve které jsou popsané možné způsoby optimalizace GPU pro těžbu a ty nejběžnější z nich jsou předvedeny prakticky. Bylo provedeno několik měření s různými nastavení karty, vyhodnocení z hlediska efektivity a zkoumána závislost výše zmíněných veličin na měněném parametru karty. Při optimálním nastavení z hlediska efektivity bylo dosaženo téměř 2,5násobného zvýšení efektivity těžby, oproti továrnímu nastavení karty. Pro tato nastavení byl proveden také výpočet denního zisku z těžby, přičemž při těžbě s továrním nastavením by byl těžař ve ztrátě přibližně 23 Kč denně a při optimálním nastavení by byla potenciální ztráta z těžby přibližně 3,5 Kč denně. Na těchto výpočtech lze sice pozorovat výrazný vliv optimalizace hardwaru na profitabilitu, ale také nerentabilita těžby v současné době a testovaných podmínkách. Tato nerentabilita je zapříčiněna nepříznivou situací na kryptoměnovém trhu a zároveň vysokými cenami elektrické energie.

V poslední kapitole byly navrhnuty možnosti, kterými by mohla být profitabilita těžby zvýšena. První z nich jsou různé těžební techniky či strategie. Následuje využití vlastních fotovoltaických elektráren, jejichž popularita v současnosti roste. Ty generují přebytky energie, které lze efektivně využít k těžbě kryptoměn. Další možností může být využití odpadního tepla k vytápění místnosti či domu nebo pronájem těžebních prostor (housing) v zahraničí, díky čemuž je možné se dostat na zlomek ceny elektřiny ve srovnání s cenami pro české domácnosti. V modelovém výpočtu denního zisku z těžby při housingu na Islandu byl výsledkem potenciální zisk přibližně 2,6 Kč denně.

Práce může sloužit čtenářům k uvedení do problematiky těžby kryptoměn, pochopení principů těžby a zároveň přiblížení problematiky udržitelnosti těžby, která bývá často diskutovaným tématem. Praktická část může být užitečná zejména začínajícím těžařům nebo čtenářům, kteří by si rádi těžbu vyzkoušeli. Informace ohledně těžby jsou často roztříštěné a ne příliš ucelené. V případě začínajícího těžaře lze využít praktickou část jako ucelený zdroj informací k těžbě nebo návod pro zprovoznění těžby a optimalizaci hardwaru. V práci byl proces těžby a optimalizace prezentován na konkrétní grafické kartě a kryptoměně, jejíž těžba byla v době psané nejziskovější, nicméně stejné či velmi podobné principy lze uplatnit pro různé těžební algoritmy a grafické karty.

SEZNAM POUŽITÉ LITERATURY

[1] Tax excluded electricity prices for households in the Czechia from 2018 to 2022, semi-annually. Statista [online]. 2022 [cit. 2023-02-09]. Dostupné z: https://www.statista.com/statistics/1046839/electricity-prices-for-households-excluding-taxes-czechia/

[2] WhatToMine [online]. 2020 [cit. 2023-02-09]. Dostupné z: https://whattomine.com/

[3] What is power efficiency?. Minerstat [online]. 2023 [cit. 2023-02-21]. Dostupné z: https://minerstat.com/help/what-is-power-efficiency

[4] TUZI, Daren. Cryptonight GPU mining efficiency [online]. 2018 [cit. 2023-02-22]. Dostupné z: https://trepo.tuni.fi/bitstream/handle/123456789/26464/Tuzi.pdf?sequence=4&isAllowed=y. Master of Science Thesis. Tampere University of technology.

[5] MUNAM, Hammad Ali. Is The Amount Of VRAM Important When Mining?. CPUGPU Nerds [online]. [cit. 2023-02-22]. Dostupné z: https://cpugpu-nerds.com/amount-of-vram-important-mining/

[6] Explained: ASIC resistance and why it is good for small-scale miners. CNBCTV18 [online]. 2022 [cit. 2023-02-23]. Dostupné z: https://www.cnbctv18.com/cryptocurrency/explained-asic-resistance-and-why-it-is-good-for-small-scale-miners-14007682.htm

[7] MINEBEST TEAM. Different mining pool payouts explained: PPS vs. FPPS vs. PPLNS vs. PPS+. MineBest [online]. 2021 [cit. 2023-03-17]. Dostupné z: https://minebest.com/blog/pps-vs-fpps-vs-pplns-vs-pps-mining-pool-payouts-explained

[8] SIDE OF BURRITOS. Mining Pools Explained - PPLNS vs PPS | Payout Methods. In: Youtube [online]. 2021 [cit. 2023-03-17]. Dostupné z: https://www.youtube.com/watch?v=6WcV4nS4ti0

[9] PACIFIC POOL. PPLNS Mining Explained. Medium [online]. 2020 [cit. 2023-03-17]. Dostupné z: https://medium.com/@pacificpool/pplns-mining-fungibly-xyz-870c045018fe

[10] SKORJANC, Matjaz. How mining pools distribute rewards? PPS vs FPPS vs PPLNS. NiceHash [online]. 2019 [cit. 2023-03-17]. Dostupné z: https://www.nicehash.com/blog/post/how-mining-pools-distribute-rewards-pps-vs-fpps-vs-pplns

[11] MiningPoolStats [online]. 2021 [cit. 2023-03-21]. Dostupné z: https://mining-poolstats.stream/kaspa

[12] LolMiner [online]. 2023 [cit. 2023-03-25]. Dostupné z: https://lolminer.site/

[13] A., George. CPU Silicon Lottery: What Are The Prizes?. ByteXD [online]. 2023 [cit. 2023-04-06]. Dostupné z: https://bytexd.com/hardware/cpu-silicon-lottery-what-are-the-prizes/

[14] Cryptography. Binance Academy [online]. 2023 [cit. 2023-04-16]. Dostupné z: https://academy.binance.com/en/glossary/cryptography

[15] STROUKAL, Dominik a Jan SKALICKÝ. Bitcoin a jiné kryptopeníze budoucnosti: historie, ekonomie a technologie kryptoměn, stručná příručka pro úplné začátečníky. Třetí rozšířené vydání. Praha: Grada Publishing, 2021. Finance pro každého. ISBN 978-80-271-1043-8.

[16] ANTONOPOULOS, Andreas M. Mastering bitcoin. Sebastopol CA: O'Reilly, [2015]. ISBN 9781449374044.

[17] BITCOINOVEJ KANÁL. #61 - Asymetrická kryptografie a digitální podpisy. In: Youtube [online]. 2020 [cit. 2023-04-16]. Dostupné z: https://www.youtube.com/watch?v=09h3pFk4tXI

[18] PRITZKER, Yan. Vynález jménem bitcoin. Přeložil Tereza WONGOVÁ. [Praha]: Braiins Publishing, 2020. ISBN 978-80-907975-0-5.

[19] AGRAWAL, Harsh. Bitcoin Private Keys: Everything You Need To Know. CoinSutra [online]. 2022 [cit. 2023-04-17]. Dostupné z: https://coinsutra.com/bitcoin-private-key/

[20] Základní pojmy: soukromý klíč. ŠkolaBitcoinu [online]. [cit. 2023-04-17]. Dostupné z: https://www.skolabitcoinu.cz/zakladni-pojmy/soukromy-klic

[21] DOLEŽAL, Martin a Matouš VONDRÁK. K čemu u kryptoměn slouží privátní a veřejný klíč? Jaký je mezi nimi rozdíl?. Finex [online]. 2022 [cit. 2023-04-17]. Dostupné z: https://finex.cz/kryptomeny-privatni-verejne-klice/

[22] JOKO. How is a Bitcoin address created?. Shift Crypto [online]. 2022 [cit. 2023-04-17]. Dostupné z: https://shiftcrypto.ch/blog/how-is-a-bitcoin-address-created/

[23] DOLEŽAL, Martin. SegWit - Upgrade Bitcoinu, který umožňuje divy a řeší zásadní problém!. Finex [online]. 2021 [cit. 2023-04-17]. Dostupné z:

https://finex.cz/segwit-upgrade-bitcoinu-ktery-umoznuje-divy-a-resi-zasadni-problem/

[24] ROWDEN, Seth. What Is Satoshi Wallet Address? How Many Bitcoins Does Satoshi Nakamoto Have?. Bitkan [online]. 2023 [cit. 2023-04-17]. Dostupné z: https://bitkan.com/learn/what-is-satoshi-wallet-address-how-many-bitcoins-does-satoshi-nakamoto-have-11741

[25] BITCOINOVEJ KANÁL. Formáty bitcoinových adres a Segwit - #71. In: Youtube [online]. 2021 [cit. 2023-04-17]. Dostupné z: https://www.youtube.com/watch?v=2h_u0fp5zTA

[26] KARMA. Vzděláváme se: Bitcoinová adresa detailně. KRYPTOPORTAL [online]. 2019 [cit. 2023-04-17]. Dostupné z: https://kryptoportal.cz/bitcoinova-adresa-detailne/

[27] SEDGWICK, Kai. Everything You Should Know About Bitcoin Address Formats. Bitcoin.com [online]. 2019 [cit. 2023-04-17]. Dostupné z: https://news.bitcoin.com/everything-you-should-know-about-bitcoin-address-formats/

[28] LÁNSKÝ, Jan. Kryptoměny. V Praze: C.H. Beck, 2018. ISBN 9788074007224.

[29] BANKLESS, David. Co to je multisignature wallet. Bankless [online]. 2021 [cit. 2023-04-17]. Dostupné z: https://bankless.cz/studium/co-to-je-multisignature-wallet

[30] SWAN, Melanie. Blockchain: blueprint for a new economy. Sebastopol, CA: O'Reilly, February 2015. ISBN 978-1-491-92049-7.

[31] Bitcoin Blockchain Size (I:BBS). YCharts [online]. 2023 [cit. 2023-04-19]. Dostupné z: https://ycharts.com/indicators/bitcoin_blockchain_size

[32] Blocks List. BTC.com [online]. 2023 [cit. 2023-04-19]. Dostupné z: https://explorer.btc.com/btc/blocks

[33] TĚTEK, Josef. Kryptoměnové forky (VŠE, CO CHCETE VĚDĚT). Alza.cz [online]. 2019 [cit. 2023-04-19]. Dostupné z: https://www.alza.cz/kryptomenove-forky

[34] Transaction ID (TXID). Binance Academy [online]. 2023 [cit. 2023-04-19]. Dostupné z: https://academy.binance.com/en/glossary/transaction-id

[35] Are you ready for blockchain?. Thomson Reuters [online]. [cit. 2023-04-19]. Dostupné z: https://www.thomsonreuters.com/en/reports/blockchain.html

[36] FRANCO, Pedro. Understanding Bitcoin: Cryptography, Engineering and Economics. Wiley, 2014. ISBN 978-1-119-01916-9.

[37] What is block size?. Bitstamp Learn [online]. 2022 [cit. 2023-04-19]. Dostupné z: https://www.bitstamp.net/learn/crypto-101/what-is-block-size/

[38] AKASHKUMARSEN4. What is Coinbase Transaction?. GeeksforGeeks [online]. 2021 [cit. 2023-04-19]. Dostupné z: https://www.geeksforgeeks.org/what-is-coinbase-transaction/

[39] LEE, Suhyeon. Bitcoin block structure. ResearchGate [online]. 2018 [cit. 2023-04-19]. Dostupné z: https://www.researchgate.net/figure/Bitcoin-block-structure_fig1_343236094

[40] Anatomie bloku. Bitcoinový slovník naučný [online]. 2021 [cit. 2023-04-19]. Dostupné z: https://btc-slovnik.cz/pages/block.html

[41] Blockchain Merkle Tree. JavaTpoint [online]. 2021 [cit. 2023-04-19]. Dostupné z: https://www.javatpoint.com/blockchain-merkle-tree

[42] IVAN ON TECH. What is inside a Bitcoin block? Programmer explains. In: Youtube [online]. 2017 [cit. 2023-04-19]. Dostupné z: https://www.youtube.com/watch?v=qLM-UC_eqIY

[43] Formula to calculate mining profit. Bitcoin Forum [online]. 2018 [cit. 2023-04-27]. Dostupné z: https://bitcointalk.org/index.php?topic=3140185.0

[44] NARAYANAN, Arvind. Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton: Princeton University Press, [2016]. ISBN 9780691171692.

[45] KALISKÝ, Boris. Bitcoin a ti druzí: nepostradatelný průvodce světem kryptoměn. [Praha]: IFP Publishing, 2018. ISBN 978-80-87383-71-1.

[46] VRANKEN, Harald. Sustainability of bitcoin and blockchains. Current Opinion in Environmental Sustainability [online]. 2017, 28, 1-9 [cit. 2023-04-30]. Dostupné z: doi:https://doi.org/10.1016/j.cosust.2017.04.011

[47] TAYLOR, Michael Bedford. The Evolution of Bitcoin Hardware. Computer [online]. IEEE, 50, 58 - 66 [cit. 2023-05-05]. Dostupné z: doi:https://doi.org/10.1109/MC.2017.3571056

[48] KAMIYA, George. Bitcoin energy use - mined the gap. IEA [online]. 2019 [cit. 2023-05-05]. Dostupné z: https://www.iea.org/commentaries/bitcoin-energy-use-mined-the-gap

[49] KIM, Christine. The Rise of ASICs: A Step-by-Step History of Bitcoin Mining. CoinDesk [online]. 2020 [cit. 2023-05-05]. Dostupné z: https://www.coindesk.com/tech/2020/04/26/the-rise-of-asics-a-step-by-step-history-of-bitcoin-mining/

[50] SIMPLY EXPLAINED. Proof-of-Stake (vs proof-of-work). In: Youtube [online]. 2018 [cit. 2023-05-06]. Dostupné z: https://www.youtube.com/watch?v=M3EFi_POhps

[51] GEHMLICH, Ben. Pros and Cons of Proof of Stake for Ethereum Blockchain Security. Gigster [online]. 2022 [cit. 2023-05-06]. Dostupné z: https://gigster.com/blog/pros-and-cons-of-pos-for-ethereum-security/

[52] ZHANG, Rong a Wai Kin (Victor) CHAN. Evaluation of Energy Consumption in Block-Chains with Proof of Work and Proof of Stake. Journal of Physics: Conference Series [online]. IOP Publishing, 2020, 1584 [cit. 2023-05-06]. Dostupné z: doi:https://doi.org/10.1088/1742-6596/1584/1/012023

[53] BITCOINOVEJ KANÁL. #47 - Jak funguje Proof of Stake?. In: Youtube [online]. 2020 [cit. 2023-05-06]. Dostupné z: https://www.youtube.com/watch?v=CpheakmDeak

[54] WAY, Rupert, Matthew C. IVES, Penny MEALY a J. Doyne FARMER. Empirically grounded technology forecasts and the energy transition. Joule [online]. 2022, 6, 2057-2082 [cit. 2023-05-07]. Dostupné z: doi:https://doi.org/10.1016/j.joule.2022.08.009

[55] IRENA. Renewable Power Generation Costs in 2021 [online]. Abu Dhabi: International Renewable Energy Agency, 2022 [cit. 2023-05-07]. ISBN 978-92-9260-452-3.

[56] ANDERSON, Erik a Rohan REDDY. Bitcoin Mining Is Set to Turn Greener. Global X [online]. 2023 [cit. 2023-05-07]. Dostupné z: https://www.globalxetfs.com/bitcoin-mining-is-set-to-turn-greener/

[57] BLANDIN, Apolline, Dr. Gina PIETERS, Yue WU, Thomas EISERMANN, Anton DEK, Sean TAYLOR a Damaris NJOKI. 3rd Global Cryptoasset Benchmarking

Study [online]. 2020 [cit. 2023-05-07]. Dostupné z: https://www.jbs.cam.ac.uk/wp-content/uploads/2021/01/2021-ccaf-3rd-global-cryptoasset-benchmarking-study.pdf

[58] SCHMIDT, John a Benjamin CURRY. Why Does Bitcoin Use So Much Energy?. Forbes [online]. 2022 [cit. 2023-05-07]. Dostupné z: https://www.forbes.com/advisor/investing/cryptocurrency/bitcoins-energy-usage-explained/

[59] BITCOIN MINING COUNCIL. GLOBAL BITCOIN MINING DATA REVIEW Q2 2022 [online]. 2022 [cit. 2023-05-07]. Dostupné z: https://bitcoinminingcouncil.com/wp-content/uploads/2022/07/2022.07.19-BMC-Presentation-Q2-22-Presentation.pdf

[60] CARTER, Nic. How Much Energy Does Bitcoin Actually Consume?. Harvard Business Review [online]. 2021 [cit. 2023-05-07]. Dostupné z: https://hbr.org/2021/05/how-much-energy-does-bitcoin-actually-consume

[61] ALONSO, Sergio Luis Náñez, Javier JORGE-VÁZQUEZ, Miguel Ángel Echarte FERNÁNDEZ a Ricardo Francisco Reier FORRADELLAS. Cryptocurrency Mining from an Economic and Environmental Perspective. Analysis of the Most and Least Sustainable Countries. Energies [online]. 2021, 14(14) [cit. 2023-05-07]. Dostupné z: doi:https://doi.org/10.3390/en14144254

[62] STOLL, Christian, Lena KLAASSEN a Ulrich GALLERSDÖRFER. The Carbon Footprint of Bitcoin. Joule [online]. 2019, 3, 1647-1661 [cit. 2023-05-08]. Dostupné z: doi:https://doi.org/10.1016/j.joule.2019.05.012

[63] BONDAREV, Mikhail. Energy Consumption of Bitcoin Mining. International Journal of Energy Economics and Policy [online]. 2020, 10(4), 525-529 [cit. 2023-05-08]. Dostupné z: doi:https://doi.org/10.32479/ijeep.9276

[64] THE BITCOIN MINING NETWORK ENERGY AND CARBON IMPACT. In: Coinshares.com [online]. 2022 [cit. 2023-05-08]. Dostupné z: https://a.storyblok.com/f/155294/x/0c3f3837c8/coinshares_bitcoin_mining_report_jan_2022.pdf

[65] Cambridge Bitcoin Electricity Consumption Index. University of Cambridge [online]. 2023 [cit. 2023-05-08]. Dostupné z: https://ccaf.io/cbnsi/cbeci

[66] MINING CHAMBER. Basics Of Overclocking And BIOS Modding | Miners Edition. In: Youtube [online]. 2021 [cit. 2023-05-09]. Dostupné z: https://www.youtube.com/watch?v=3EFf3mvEk7o&list=WL

[67] RYBARCZYK, Rachel, Drew ARMSTRONG a Amanda FABIANO. On Bitcoin Energy Consumption: A Quantitative Approach to a Subjective Question. In: Galaxy Digital [online]. 2021 [cit. 2023-05-09]. Dostupné z: https://assets.ctfassets.net/h62aj7eo1csj/2KQ4HLVZYBA4CTG6HxtpKY/f9aa3d2f37c56862df70e10cef6a7ced/GLXY_2022_ResearchReport_BTC-Energy-Consumption.pdf

[68] MCCOOK, Hass. An Order-of-Magnitude Estimate of the Relative Sustainability of the Bitcoin Network [online]. In: . 2015 [cit. 2023-05-09]. Dostupné z: https://www.academia.edu/7666373/An_Order-of-Magnitude_Estimate_of_the_Relative_Sustainability_of_the_Bitcoin_Network_-_3rd_Edition

[69] BOURBON, Roberto. Why Bitcoin is actually good for our planet. A sustainable and ethical revolution to the current financial system: Reflecting about Cryptocurrency and Bitcoin in 2021, ahead of a lifetime opportunity. 2021. ISBN 979-8726005102.

[70] FRUMKIN, Daniel, Dave WHITE, Tyler COHOON, Magdalena GRONOWSKA, Zack VOELL a Matyas KUCHAR. Braiins Insights: bitcoin mining handbook. [Prague]: Braiins Insights, [2022]. ISBN 9788090797598.

[71] How does the profit switch work?. Minerstat [online]. 2023 [cit. 2023-05-10]. Dostupné z: https://minerstat.com/help/how-does-the-profit-switch-work

[72] CHMELAŘ, Robert. Prodáváte přebytky z domácí fotovoltaické elektrárny? Hledejte výkupní ceny navázané na ty velkoobchodní. Kurzycz [online]. 2022 [cit. 2023-05-10]. Dostupné z: https://www.kurzy.cz/zpravy/647778-prodavate-prebytky-z-domaci-fotovoltaicke-elektrarny-hledejte-vykupni-ceny-navazane-na-ty/

[73] Vyplatí se solární elektřina na těžbu kryptoměn?. MyPower.CZ [online]. 2019 [cit. 2023-05-10]. Dostupné z: https://forum.mypower.cz/viewtopic.php?t=4658

[74] HLADÍK, Richard. Výkupní cena elektřiny z fotovoltaických elektráren 2023. Evolty [online]. 2023 [cit. 2023-05-10]. Dostupné z: https://evolty.cz/fve/vykupni-cena-elektriny-z-fve/

[75] KONEČNÝ, Miroslav. Systém využití odpadního tepla z výpočetní jednotky využívané pro těžbu kryptoměn [online]. 2019 [cit. 2023-05-10]. Dostupné z:

https://dspace.cvut.cz/bitstream/handle/10467/82564/F3-DP-2019-Konecny-Miroslav-Bc_Konecny_Miroslav_Diplomova_prace.pdf?sequence=-1&isAllowed=y. Diplomová práce. České vysoké učení technické v Praze.

[76] Electricity prices for enterprises worldwide in June 2022, by select country. Statista [online]. 2023 [cit. 2023-05-11]. Dostupné z: https://www.statista.com/statistics/1369634/business-electricity-price-worldwide-in-selected-countries/

[77] Energy. Government of Iceland [online]. [cit. 2023-05-11]. Dostupné z: https://www.government.is/topics/business-and-industry/energy/

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ECDSA	Elliptic Curve Digital Signature Algorithm
SHA	Secure Hash Algorithm
RIPEMD	RACE Integrity Primitives Evaluation Message Diges
QR	Quick Response
P2PKH	Pay-to-Public-Key-Hash
P2SH	Pay-to-Script-Hash
GB	gigabyte
UTXO	Unspent Transaction Output
ID	identification
TXID	Transaction ID
MB	megabyte
BTC	Bitcoin
TWh	terawatthodina
PJ	petajoule
PoW	Proof of Work
PoS	Proof of Stake
ETH	Ethereum
G20	Group of Twenty
ASIC	Application Specific Integrated Circuit
CPU	Central Processing Unit
FPGA	Field Programmable Gate Array
GPU	Graphics processing unit
nm	nanometr
HW	hardware

PC	Personal Computer
H/W	hash per watt
H/s	hash per second
VRAM	Video Random Access Memory
BIOS	Basic Input/Output System
GDDR	Graphics Double Data Rate
kWh	kilowatthodina
€	euro
$	USD
USD	United States dollar
Kč	koruna česká
MH/s	megahash per second
TH/s	terahash per second
h	hodina
PPS	Pay-Per-Share
FPPS	Full Pay-Per-Share
PPS+	Pay-Per-Share Plus
PPLNS	Pay-Per-Last N Shares
GUI	Graphical User Interface
MHz	megahertz
W	watt
°C	stupeň Celsia
MH/W	megahash per watt

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM GRAFŮ

SEZNAM PŘÍLOH

PŘÍLOHA P I: NÁZEV PŘÍLOHY

Elektronická podoba bakalářské práce