Univerzita Hradec Králové

Přírodovědecká fakulta

Katedra aplikované kybernetiky

Farmaření jako ekologičtější varianta těžby kryptoměn

Bakalářská práce

Autor:	**Ondřej Malý**
Studijní program:	B0114A14CZma Informatika se zaměřením na vzdělávání
Studijní obor:	Informatika se zam. na vzd. – maior, Základy techniky se zam. na vzd. – minor
Vedoucí práce:	prof. RNDr. Štěpán Hubálovský, Ph.D.

Hradec Králové červen 2023

UNIVERZITA HRADEC KRÁLOVÉ
Přírodovědecká fakulta
Akademický rok: 2021/2022

Studijní program: Informatika se zaměřením na vzdělávání
Forma studia: Prezenční
Specializace/kombinace: Informatika se zam. na vzd. – maior,
Základy techniky se zam. na vzd. – minor (BVIN-BVZT)

Specializace v rámci které má být VŠKP vypracována: Informatika se zaměřením na vzdělávání

Podklad pro zadání BAKALÁŘSKÉ práce studenta

Jméno a příjmení:	**Ondřej Malý**
Osobní číslo:	**S20IN018BP**
Adresa:	Kostelec u Heřmanova Městce 157, Kostelec u Heřmanova Městce, 53803 Heřmanův Městec, Česká republika
Téma práce:	Farmaření jako ekologičtější varianta těžby kryptoměn
Téma práce anglicky:	Farming as a more ecological variant of cryptocurrency mining
Jazyk práce:	Čeština
Vedoucí práce:	prof. RNDr. Štěpán Hubálovský, Ph.D. Katedra aplikované kybernetiky

Zásady pro vypracování:

Tématem bakalářské práce je farmaření kryptoměn.
Cílem práce je vytvořit obecný popis fungování kryptoměn, seznámit s jejich riziky a úskalími, dále s principy těžby kryptoměn. Další část práce se zaměřuje na to, zda je farmaření kryptoměn opravdu ekologičtější než jejich těžba a jakým způsobem to lze ověřit.
Jako výzkumná metoda k potvrzení či vyvrácení hypotéz byl vybrán domácí experiment s jedním těžebním strojem (kryptoměna Ethereum) a jednou kryptofarmou (kryptoměna Chia).

Seznam doporučené literatury:

xxx

Podpis studenta: 

Datum: 12.5.2023

Podpis vedoucího práce:

Datum:

Prohlášení

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně a že jsem v seznamu použité literatury uvedl všechny prameny, ze kterých jsem vycházel.

V Hradci Králové dne 22. 5. 2023 Ondřej Malý

Poděkování

Rád bych touto cestou poděkoval svému vedoucímu bakalářské práce prof. RNDr. Štěpánovi Hubálovskému, Ph.D. za cenné rady, všestrannou pomoc při jejím zpracovávání a příjemnou spolupráci.

Anotace

MALÝ, O. *Farmaření jako ekologičtější varianta těžby kryptoměn.* Hradec Králové, 2023. Bakalářská práce na Přírodovědecké fakultě Univerzity Hradec Králové. Vedoucí bakalářské práce Štěpán Hubálovský. 45 s.

Cílem této bakalářské práce je seznámení čtenáře s obecným popisem fungování kryptoměn, jejich riziky a úskalími, dále principem těžby a farmaření kryptoměn a v druhé části se práce zaměřuje na to, zda je farmaření kryptoměn opravdu ekologičtější než jejich těžba a jakým způsobem to lze ověřit. Pro praktickou část práce byl vybrán domácí experiment s jedním těžebním strojem (kryptoměna Ethereum) a jednou kryptofarmou (kryptoměna Chia).

Klíčová slova

kryptoměny, těžba kryptoměn, farmaření kryptoměn, Ethereum, kryptoměna Chia

Annotation

MALÝ, O. *Farming as a more ecological variant of cryptocurrencies mining.* Hradec Králové, 2023. Bachelor thesis at Faculty of Science University Hradec Králové. Thesis supervisor Štěpán Hubálovský. 45 p.

The aim of this bachelor thesis is to introduce the reader to a general description of the functioning of cryptocurrencies, their risks and vulnerabilities, as well as the principles of mining and farming cryptocurrencies. In the second part, the thesis focuses on whether cryptocurrency farming is really more ecological than cryptocurrency mining and how this can be verified. For the practical part of the thesis, a home experiment with one crypto mining machine (Ethereum cryptocurrency) and one crypto farm (Chia cryptocurrency) was chosen.

Keywords

cryptocurrencies, cryptocurrency mining, cryptocurrency farming, Ethereum, Chia

Obsah

Úvod

Téma bakalářské práce jsem si vybral na základě současných trendů, kdy se o kryptoměnách mluví ve velké míře a je několik způsobů, jak je možné si je obstarat: nákup, ověřování plateb (těžba, farmaření, validace), směňování, darování a další.

Avšak kryptoměny mají svoji stinnou stránku – ověřování transakcí pomocí systému Proof of Work, neboli jejich těžba, funguje na principu náročných matematických výpočtů, k čemuž je potřeba velký příkon elektrické energie a například při těžbě pomocí grafických karet navíc vzniká odpadní teplo.

Jako odezva na tuto problematiku se objevil jiný systém, Proof of Space and Time, nazývaný jako farmaření kryptoměn, přičemž by se mělo jednat o ekologičtější variantu těžby kryptoměn.

Cílem této práce je v teoretické části seznámení čtenáře s obecným popisem fungování kryptoměn, jejich historií, riziky, úskalími a se současnými trendy. Dále se čtenář seznámí s nejznámějším principem ověřování plateb, těžebním systémem Proof of Work, dále se systémem Proof of Space and Time farmařícím kryptoměny a je zde zmíněn i nový systém Proof of Stake, zvaný validování.

V praktické části se práce zaměřuje na to, zda může být farmaření kryptoměn pomocí systému Proof of Space and Time opravdu ekologičtější než těžba pomocí systému Proof of Work, což bude ověřováno pomocí domácího experimentu s jedním těžebním strojem těžícím kryptoměnu Ethereum a kryptofarmou farmařící kryptoměnu Chia.

1 Teoretická část

Poznatky v této kapitole se opírají o autorovo zkušenosti a zároveň volně o informace ze zdrojů [1–10], přičemž dochází k jejich vzájemnému prolínání.

1.1 Kryptoměny

Kryptoměny jsou typ peněz vytvářených elektronicky. Dle vyjádření Generálního finančního ředitelství [11] se jedná o nehmotnou, movitou a zastupitelnou věc. Jednu z nejhlavnějších rolí hraje jejich decentralizace, která je popsána v podkapitole 1.2.

Mezi obecně nejznámější kryptoměny se řadí Bitcoin (BTC), Bitcoin Cash (BCH), Monero (XMR), dále Ethereum (ETH) oblíbené mezi těžaři s těžebními stroji s grafickými kartami, Solana (SOL), Polkadot (DOT) a mnoho dalších. Mezi rozkvétajícími najdeme například Dogecoin (DOGE) nebo Shiba Inu (SHIB) a mnoho dalších.

V současné době existuje dle serveru CoinMarketCap [12] přes 25 000 různých kryptoměn, avšak toto číslo se neustále navyšuje. Mezi nově vzniklými najedeme primárně různé napodobeniny vycházející z již existujících, známějších a propracovanějších kryptoměn, například na bázi kryptoměn Bitcoin nebo Ethereum, ale naopak i kryptoměny postavené na úplně nových základech.

1.2 Vlastnosti kryptoměn, pro a proti, rizika

Kryptoměny jsou jako takové, od samotného počátku, spojovány s decentralizací. Je obecně známo, že jejich fungování je zajištěno skrze P2P (peer-to-peer) sítě, které komunikují napřímo mezi jednotlivými koncovými zařízeními uživatelů konkrétní kryptoměnové sítě. Přes ně je prováděna veškerá uživatelská komunikace a potvrzování transakcí (těžba, farmaření, validace) bez jakýchkoliv prostředníků. Díky tomu se v kryptoměnovém prostředí nenachází žádná centrální autorita, například centrální banka, a nelze je tak kontrolovat vládou nebo jinými institucemi. *(I když některé státy mají regulaci v úmyslu, nebo již kryptoměny regulují, viz podkapitola 1.6.)* Zároveň se jedná o prvek transparentnosti, protože všechny transakce jsou v síti dohledatelné, avšak čím je platba starší, tím hůře se dohledává. Jako zápornou vlastnost ale můžeme uvést nemožnost stornování platby, jelikož není

přítomna žádná bankovní instituce ve funkci dozorčího a zprostředkovatelský orgán.

Vzhledem k využívání peer-to-peer sítí jsou kryptoměny globální a je tedy možné posílat peníze na druhý konec světa během chvíle. Některé státy již ovšem kryptoměny zakázaly (viz kapitola 1.6). Posílání kryptoměny mezi účty je navíc zdarma, či za drobný poplatek, díky kterému je transakce ověřena rychleji. Jelikož k posílání kryptoměn potřebujeme pouze elektronické zařízení (počítač, notebook, tablet, mobil…) s připojením k internetu (nebo bitcoinmat), kryptoměnovou peněženku, tak díky tomu mají velmi širokou dostupnost. Na druhou stranu, výčet služeb jako obchodů nebo restaurací, kde jsou uznávány jako platidlo, je do dnešní doby velmi omezený.

Další vlastností je pseudoanonymita. Ta je jak výhodou, protože s platbami nejsou spojeny žádné citlivé údaje, tak zároveň nevýhodou, jelikož se kryptoměny bohužel využívají i pro nelegální obchodování, korupci a financování nelegálních činností. Jedná se například o jedno z hlavních platidel v neviditelné části World Wide Webu s názvem Darknet, která je známa pro obchod s drogami, zbraněmi nebo nelegálními činnostmi.

Důležitým prvkem kryptoměn je jejich šifrování pomocí asymetrické kryptografie, jiným názvem kryptografie s veřejným klíčem, což je skupina kryptografických metod pracující na principu použití odlišných klíčů pro šifrování, které probíhá pomocí veřejného klíče a k dešifrování obsahu slouží privátní klíč. Asymetrická kryptografie se pro svoji míru bezpečnosti používá taktéž při ověřování autenticity elektronickým podpisem nebo třeba pro digitální certifikáty či Hypertext Transfer Protocol Secure (https) sloužící k zabezpečené síťové komunikaci.

Jako investiční aktivum mají kryptoměny potenciál k vysokému zhodnocení, tudíž mohou poskytnout vysokou návratnost investic. Avšak logicky, ruku v ruce k vysokému zhodnocení jde vysoká míra rizika ztráty hodnoty, jelikož se jejich hodnota odvíjí pouze od nabídky a poptávky, jako u jiných investičních aktiv – akcií, cizích měn, komodit atd. K tomu, aby cena kryptoměny klesla o několik desítek procent, stačí, aby například známá osobnost publikovala nějaký článek či komentář na sociální síti.

Z hlediska bezpečnosti jsou kryptoměny zabezpečeny na vysoké úrovni asymetrickým šifrováním a všechny transakce jsou uloženy v Blockchainu, o kterém pojednává podkapitola 1.7, což zajišťuje menší náchylnost k podvodům a krádežím, ale na druhou stránku mohou být kryptoměnové peněženky odcizeny, jak jejich hacknutím (i přes jejich ochranu proti malwaru), tak fyzicky. Jak již bylo zmíněno v podkapitole 1.1, obecně nejslabším článkem bezpečnosti je vždy sám člověk.

Může taktéž docházet ke kyberútokům spojenými s kryptoměnami, o kterých pojednává podkapitola 1.11.

1.3 Obstarávání kryptoměn a platby

Je všeobecně známo, že kryptoměny si lze obstarat několika způsoby. Je možné je nakoupit ve směnárně, podobně jako cizí měnu za předem daný kurz.

Dále je možný nákup nebo prodej za hotovost v automatu, takzvaném bitcoinmatu, který je na první pohled podobný klasickému vkladomatu i bankomatu.

Kryptoměny je možné samozřejmě nakoupit na internetu. K tomuto účelu slouží internetové směnárny a online burzy, nebo se nabízí využít služeb brokera (makléře), který zprostředkovává nákup a prodej místo samotného uživatele. U burz a online směnáren je nutné se verifikovat, například přes platební kartu. Dále je možné s nimi na zmíněných burzách obchodovat, nebo si vydělávat kryptoměny pomocí ověřování kryptoměnových plateb (popsáno v kapitolách 1.8, 1.9 a 1.10), takzvaně těžit nebo validovat nebo farmařit.

Za nejstarší českou kryptoměnovou internetovou směnárnu je považována Simplecoin s.r.o., založená v roce 2013 Pavlem Niedobou, kde lze nakupovat kryptoměny za české koruny, eura, nebo za jiné kryptoměny. Lze též využívat světových burz, přičemž mezi nejznámější řadíme Coinbase, Bitfinex nebo Bittrex. V Česku je taktéž možné nakoupit kryptoměnu Bitcoin v jedné nejmenované síti trafik. Člověk si zadá objednávku na internetu a tu poté předloží obsluze trafiky.

Platba kryptoměnami ještě není zdaleka tak rozšířená. V ČR existuje několik již několik stravovacích a ostatních podniků, ale i například čerpací stanice, kde lze útratu zaplatit Bitcoinem. Dále lze pomocí Bitcoinu nakupovat na některých velkých e-shopech. Tato místa je v drtivé většině možné najít na internetovém portálu

www.coinmap.org, jehož cílem je na mapě obsáhnout všechna místa, kde je možné kryptoměnami platit nebo kde například se nachází bitcoinmaty.

1.4 Kryptoměnové peněženky

Kryptoměny se jako takové uchovávají v konkrétní kryptoměnové síti. K přístupu k nim se používají kryptoměnové peněženky, které se dají přirovnat k přístupovým terminálům. Ty slouží k přijímání, odesílání a kontrole zůstatku. Peněženka generuje a uchovává privátní klíč formou asymetrické kryptografie, ten by se dal přirovnat k číslu bankovního účtu a dále obsahuje ukazatel zůstatku.

Kryptoměnové peněženky se dělí se na softwarové, hardwarové a papírové. Na internetu lze nalézt mnoho kryptoměnových peněženek, přičemž každá z nich je v něčem odlišná od ostatních.

Softwarové peněženky jsou programy, které se dají stáhnout jako aplikace na chytrý telefon, do tabletu či do počítače, podobající se mobilnímu nebo internetovému bankovnictví. Jejich výhodou je možnost správy peněženky, přehledy o transakcích, nastavování poplatků, a to vše na jednom místě, přičemž zde existují i funkce např. pro zvětšení anonymity. Bezpečnost se však odvíjí od bezpečnostních návyků uživatele (počítač bývá zpravidla připojen většinu času k internetu, dále může dojít k úniku hesla) a typu zařízení, protože klíč je zašifrován přímo v počítači. Jako příklady si můžeme uvést softwarové peněženky Meta Musk nebo MyEtherWallet.

Hardwarové peněženky jsou fyzická zařízení vypadající podobně jako USB flash disk, přičemž se jedná zpravidla o jednoúčelový počítač velmi malých rozměrů s vlastním procesorem, pamětí, ovládacími tlačítky a displejem. Hlavní výhodou hardwarové peněženky je vysoká míra bezpečnosti (peněženka nebývá po celou dobu zapojena do počítače, navíc má bezpečnostní prvky proti malwaru), přičemž nevýhodou je její potenciální ztráta nebo možnost odcizení celého zařízení, vzhledem k jeho menším rozměrům. Cena takové peněženky se nachází v řádech jednotek tisíců korun českých.

Můžeme se i setkat s **off-line hardwarovými peněženkami**. Jedná se o kovovou destičku, která je ve většině případu rozměrově shodná s klasickou platební kartou

a vytvořená z certifikované oceli, titanu nebo jiného kovu zajišťující vysokou odolnost proti všem přírodním živlům. Po zakoupení si na tuto destičku člověk raznicí vyrazí údaje o svojí peněžence. Funkčností je srovnatelná s papírovou kryptopeněženkou.

Papírové peněženky, jak je z názvu patrné, jsou vygenerované údaje o peněžence (veřejná adresa, privátní klíč…) vytištěné na papíře, opatřené QR kódem pro snazší manipulaci. Výhodou je, že se nenachází on-line, a tudíž je mimo dosah internetových hackerů. Využívají se především k archivaci. Nevýhodou je však možnost fyzického zcizení papírové peněženky či její ztráty. Důležité je též generovat údaje přes ověřený generátor. V dnešní době se tolik nevyužívají, jelikož jejich podstatu převzaly hardwarové peněženky.

U kryptoměnových peněženek a kryptoměn obecně platí, že nejslabším článkem bezpečnosti je vždy člověk. Některé firmy nabízejí pojištění pro kryptopeněženky.

1.5 Historie kryptoměn, současnost a budoucnost

Dle Ševčíka [13] počátky kryptoměn sahají do doby před rokem 1996. V té době se jednalo o pokus vytvořit na státě nezávislý systém měny, s jasnými pravidly, bezpečný, bez centrální autority a přístupný.

V roce 1996 založil Američan Douglas Jackson projekt jménem E-Gold. Tato služba poskytovala uživatelům virtuální zlato, které bylo zároveň kryté opravdovým zlatem uloženým v trezoru společnosti Gold & Silver Reserve Inc. Vzhledem k tomu, že objem zlata byl přes 3,5 tuny a na vrcholu projektu bylo připojeno přes 3,5 milionů účtů, americká vláda to vyhodnotila jako riziko nelegální paralelní měny, zlato zabavila a projekt ukončila.

V roce 1998 programátor Wei Dai přišel s myšlenkou digitální měny b-money, přičemž její koncept byl postaven na nevysledovatelnosti plateb.

Po delší odmlce, v roce 2008, Satoshi Nakamoto (pseudonym japonské skupiny nebo osoby s neznámou identitou, o které se pro zjednodušení mluví v jednotném čísle mužského rodu životného) navrhl a vytvořil první decentralizovanou měnu Bitcoin. Tu spolu s protokolem, manifestem "Bitcoin: A Peer-to-Peer Electronic Cash System" [14] a potřebným softwarem a systémem Proof of Stake uvedl na svět spolu

s vytěžením prvního Bitcoinu na začátku roku 2009. V tom samém roce byl Bitcoin prodáván na doméně New Liberty Standard za 5 amerických dolarů. Dále byl prodáván na burze MtGox, která po hackerském napadení přestala existovat.

Dva roky poté, v dubnu 2011, došlo ke vzniku dalších několika kryptoměn. Z dodnes funkčních můžeme jmenovat Litecoin (LTC) a Namecoin (NMC). V tom samém roce dosáhl první komerční mining pool Slush's pool výkonu 10 000 MH/s.

Kryptoměny se staly velkým finančním tématem a v současnosti jich, dle serveru CoinMarketCap [12] existuje přes 25 000, které se prodávají na přibližně 650 burzách, přičemž tři největší: Binance, BitMax, a BitMEX spravují kryptoměny o objemu okolo 20 miliard amerických dolarů. V průměru přibude každý den jedna nová kryptoměna. Ty jsou ve velké míře postavené na bázi kryptoměny Ethereum (ETH) a v mnoha případech neúspěšné. Zkušení programátoři totiž dokážou vytvořit novou kryptoměnu i za odpoledne.

Budoucnost kryptoměn je díky všem faktorům nejistá a nedá se do určité míry předpovídat. Všeobecně známým faktem je, že kryptoměny jsou a budou rizikovou investicí, k čemuž můžeme připočíst faktory jako volatilita a občasné prudké pády, které mohou být způsobeny i například jedním příspěvkem známé osobností ze světa technologií na sociálních sítích. Některé státy již kryptoměny zakázaly a mnoho státu je již reguluje nebo má v plánu regulovat.

1.6 Regulace kryptoměn

Vzhledem k pseudoanonymitě kryptoměn a jejich zneužívání k nelegálním činnostem se jednotlivé státy ve většině případů rozhodly zasáhnout a regulovat nějakým způsobem kryptoměnové sítě. Regulace je důležitá například pro ochranu investorů před podvodníky.

Některé státy jako Egypt, Čína nebo Katar či Saudská Arábie již kryptoměny zakazují, některé africké země jako Gabon, Guyana nebo Kamerun dokonce velmi implicitně.

Například Španělsko, Německo, Švýcarsko, Japonsko a další země kryptoměny oficiálně regulují a je zde používání kryptoměn legální za dodržení určitých pravidel.

Jihoamerický stát Salvador dokonce uznal v roce 2021 Bitcoin jako oficiální měnu národa.

V České republice prozatím neexistuje souhrnná regulace. Jak bylo uvedeno v podkapitole 1.1, tak se jedná o nehmotnou, movitou, zastupitelnou věc. Transakce s nimi, pokud naplní zákonné znaky, tak posléze podléhají pravidlům finančního práva [11]. Podléhají zdanění sazbou 15 procent ze zisku z každé směny nebo prodeje, popřípadě 23 procent v případě přijmu vyššího než 48násobek průměrné mzdy.

Evropská unie, konkrétně Rada Evropské unie [15] schvaluje (ke květnu 2023) nařízení o trzích s kryptoaktivy MiCA (Markets in Crypto Assets), jehož účelem je povinnost registrace pro ty firmy, které vydávají kryptoměny či spravují kryptoměnové burzy. Díky tomu by měly mít úřady přístup k údajům z transakcí za účelem zabránění nelegálních operací a transparentnosti obchodování. Nařízení by mělo začít platit od roku 2024.

1.7 Technologie Blockchain, hash a hashovací funkce

Blockchain (česky „řetězec bloků“ a „bločenka“, ale tyto překlady se nepoužívají) vychází z datové struktury distribuované databáze, která je veřejná, naprosto transparentní databáze, zaznamenávající všechny proběhlé transakce v dané kryptoměně na celém světě, ve které není možné teoreticky ani prakticky dojít k podvrhu. Dala by se přirovnat k jakési nekonečné účetní knize konkrétní kryptoměny. Nevýhodou však je možná duplikace transakcí. Jako první ji popsal Satoshi Nakamoto [14] v roce 2008.

Technologie blockchainu funguje na principu hashování a opírá se o asymetrickou kryptografii a peer-to-peer sítě (většinová shoda).

Hashovací funkce je matematický algoritmus, sloužící k přepočítání bloku libovolně dlouhých vstupních dat do fixně dlouhého řetězce znaků, převážně čísel. Výstupní data jsou nazývána hash, otisk či fingerprint (angl. „otisk prstu“).

U kryptoměn se využívá toho, že různá délka vstupních dat do hashovací funkce poskytuje pokaždé stejně dlouhý výstup, a zároveň drobnou změnou obsahu na vstupu je dosaženo velké změny obsahu na výstupu – je prakticky skoro nemožné,

aby dvěma různým vstupům odpovídal stejný hash (jde o ověřování správnosti, proto „otisk prstu“. Avšak pro stejná vstupní data je výsledný hash vždy stejný. Z hashe nejde díky asymetrickému šifrování rekonstruovat původní zprávu. To vše přispívá k zabezpečení blockchainu ve velmi vysoké míře.

Hlavní funkcí je u kryptoměn řetězování bloků dat – každý blok obsahuje hash z bloku předchozího, což zaručuje jejich návaznost – v případě změny jakéhokoliv bloku přestanou odpovídat ty následující.

Každý blockchain se skládá ze dvou typů záznamu. Jedním jsou samotné transakce, což jsou data vkládaná uživatelem (např. platba). Ty se pak pomocí těžařů (a farmářů a validátorů), propojených peer-to-peer sítí, kde jsou všechny uzle rovnocenné, shromažďují, a přepočítají a ověřují do druhého typu záznamu – bloků transakcí, přičemž tento blok je, po většinové shodě na aktuálním stavu (konsenzusu) daného blockchainu, navázán na poslední blok.

Hashrate, značená H, je veličina používaná pro měření výpočetního výkonu grafických karet a celých těžebních sítí, udává se za určitý čas, H/s.

Avšak nebezpečím pro blockchain je takzvaný 51 % útok, který je zmíněn v oddíle 1.11.2.

Vzhledem k tomu, že se neustále navyšuje velikost blockchainu každým přidáním bloku a kopie jsou uchovávány na každém uzlu (u každého těžaře), tak je potřeba stále většího úložiště dat. Vzhledem k vlastnosti možných zpětných kontrol je potřeba data upravit tak, aby tuto vlastnost zachovávala. K tomu se využívá například oddělování hlaviček a vlastních dat, přičemž se řetězují pouze hlavičky. Síť však obsahuje všechna data, avšak jednoznačně svázaná s jejich hlavičkami za pomocí speciální datové struktury hashového stromu pro jejich možnou kontrolu.

Příklad kryptoměnové platby: *Alena chce Bořkovi poslat 0,001 BTC. Alena vytvoří transakci a ta se přidá do bloku transakcí spolu s dalšími platbami. Tento blok se odešle do celé sítě těžařů / validátorů / farmářů za účelem jeho ověření pomocí hashovací funkce. Když je vše v pořádku, tak je transakce potvrzena a přidána na konec blockchainu (řetězce bloků). V tu již chvíli všichni uživatelé sítě vědí, že transakce v tom daném bloku proběhly, a zároveň má Bořek od Aleny o 0,001 BTC na účtu víc.*

1.8 Těžba kryptoměn – systém Proof of Work

Těžba kryptoměn (anglicky *„mining“*) je proces, při kterém dochází k potvrzování a kontrole transakcí v blockchainu pomocí řetězce bloků. Byl popsán Satoshi Nakamotem [14] v průvodní dokumentaci k síti kryptoměny Bitcoin. Aby byla transakce validní, je nutné, aby splňovala podmínky, kterými jsou: patrný pohyb v peněžence uživatele, správný elektronický podpis a další.

Díky decentralizaci v síti nenajdeme žádný centrální počítač, který by ověřování transakcí zajistil, a tak ji zajišťuje peer-to-peer síť počítačů uživatelů, takzvaných těžařů (anglicky *„miners“*), kteří ověřují platby pomocí množství vynaložené práce k jejich ověření – vytvoření bloku transakcí. Pro zamezení nadvlády v síti je zde obtížnost vytvoření bloku uměle navýšena nutností vyřešení určitého problému, obsahujícího výpočetně náročnou činnost a prvek náhody, avšak vše musí být na druhou stranu jednoduše ověřitelné.

K motivaci používat zařízení těžařů k ověřování plateb slouží jejich odměňování za vytvoření bloku transakcí, který je nutný vypočítat.

O tomto systému hezky pojednává server Per Partes Consulting [6]*: „Příklad vhodného problému, používaného u Bitcoinu, je nalezení hashe s určitými vlastnostmi. Do hlavičky je přidáno náhodné číslo (nonce), čímž se změní podoba výsledného hashe. Těžaři tedy musí pro zkompletování bloku zvolit toto náhodné číslo, spočítat hash bloku a pokud neodpovídá požadovaným vlastnostem, tuto práci opakovat, dokud nezvolí takové číslo, aby hash vyhovoval. Pro ostatní uzly je snadné spočítat hash, pokud již znají toto náhodné číslo, a ověřit jeho vlastnosti, ale díky vlastnostem hashovacích funkcí je nemožné toto číslo vypočítat ze zvoleného hashe. Bitcoin používá jako vlastnost porovnání velikosti výsledného hashe (budeme-li jej považovat za velké číslo) s hodnotou nastavitelného prahu. Díky ovlivňování hodnoty prahu lze ovládat obtížnost problému.“*

Ne každý však odměnu získá, pouze ten, kdo jako první najde řešení. Čím výkonnější počítač těžař má, tím vyšší je pravděpodobnost rychlejšího nalezení správného řešení.

Jelikož se jedná se o velmi náročný proces pro výpočetní techniku, tak se pro těžbu využívají zařízení podávající co největší výpočetní výkon, k čemuž je zároveň potřeba velkého příkonu elektřiny. Mezi tato zařízení patří specializované ASIC minery, což jsou počítače, které jsou pro těžbu přímo určeny a pořizovací náklady šplhají do řádu desetitisíců až statisíců korun českých. Pro ověřování transakcí se taktéž využívají výkonné herní grafické karty. Ty lze pro zvýšení výkonů zapojovat i vícero naráz, čímž vznikají takzvané těžební stroje. Tyto těžební stroje, stejně jako ASIC minery, potřebují ke své práci příkon v řádech jednotek kW.

Vzhledem k potřebě vysokého výpočetního výkonu se těžaři seskupují do takzvaných těžařských bazénů, anglicky *„mining pools“*. Jde o platformu, kde se uživatelé těžařské sítě navzájem spojují, a kde pomocí svých těžebních strojů pracují dohromady jako jeden. V síti se tak reprezentují jako jeden uzel, stejně jako to je u samotného těžaře. Případná odměna je posléze teoreticky spravedlivě přerozdělena podle množství zapojeného výpočetního výkonu do sítě, avšak záleží na podmínkách užívání konkrétního mining poolu.

Na systému Proof of Work pracují nejznámější kryptoměny Bitcoin (BTC), Bitcoin cash (BCH) nebo Monero (XMR), Ethereum (ETH) a mnoho dalších.

Tento systém je tedy nevýhodný pro svou náročnost na elektrickou energii na zabezpečení chodu kryptoměnových sítí, ale je v současnosti snad nejpoužívanějším systémem. Dále zapříčiňuje odpadní teplo, protože grafické karty při těžbě pracují v teplotách okolo 40-60 °C.

Příklad transakce: *Alena se rozhodla poslat Bořkovi 0,001 BTC. Transakci je třeba ověřit, a tak stroje všech těžařů, spolu s těžebními stroji uživatelů Cyrila a Dalibora, (ti jsou narozdíl od ostatních spolu v mining poolu), musí natěžit (vypočítat) blok transakcí, do kterého bude transakce Aleny a Bořka zaznamenána spolu s dalšími několika transakcemi a ověřit jej, aby získali odměnu v podobě poplatku za transakci. Všichni těžaři, včetně mining poolu Cyrila a Dalibora úspěšně natěží blok, a aby se v něm transakce nezdvojila, tak proběhne hlasování o tom, kdo z těžařů blok našel, a ten následně dostane odměnu. To se odvíjí od toho, kdo zapojil největší výpočetní výkon do sítě. Mining pool Cyrila a Dalibora měl zrovna v tu chvíli největší výpočetní výkon v síti a tím pádem vyhráli odměnu. Cyril s Daliborem si následně odměnu*

přerozdělí podle poměru zapojeného výkonu do jejich mining poolu. Po tom, co je blok transakcí zapsán do blockchainu, se objeví Bořkovi na účtě 0,001 BTC od Aleny.

1.9 Validace – Systém Proof of Stake

Systém Proof of Stake, česky nazváno „důkaz o vkladu/podílu“, vznikl v reakci na systém Proof of Work, a to dle portálu Binance Academy v roce 2011 [1]. Důvodem k vytvoření tohoto systému byla snaha omezit vysokou spotřebu elektrické energie, jako tomu je u systému Proof of Work.

U kryptoměn, které využívají Proof of Stake, se navíc nevytvářejí žádné bloky, protože všechny byly vytvořeny najednou a jejich číslo se v blockchainu nikdy nezmění. To znamená, že v systému Proof of Stake neexistuje žádná odměna za vytěžení nového bloku, jak je to u Bitcoinu, Etherea nebo jiných kryptoměn, které používají systém Proof of Work, ale u Proof of Stake se účtují pouze poplatky za transakce.

Potvrzení transakce neboli ověření bloku zde probíhá tak, že uživatel zvaný validátor, anglicky *„validator“,* je vybrán systémem. K tomu, aby se uživatel vůbec mohl stát validátorem, je třeba, aby v rámci svého uzlu „vsadil“, anglicky *„stake“*, určitý počet dané kryptoměny jako zástavu (množství kryptoměny v zástavě bývá zpravidla větší, než poplatek za transakci), pomocí které se zaručuje čestné jednání a má větší důvěryhodnost. Čím větší množství kryptoměny validátor vloží za účelem zástavy, tím je pro něj pravděpodobnější získání bloku transakcí pro ověření. Systémem vybraný validátor následně ověří platnost všech transakcí v bloku. Pokud je vše v pořádku, tak blok uzavře a přidá jej do blockchainu. jako odměnu pak získá kryptoměnu ve výši poplatku za transakci. Pokud již validátor nemá zájem o ověřování, tak mu systém vydá jeho kryptoměny v zástavě spolu s odměnami. Mezi ukončením a následným vydáním kryptoměn je bezpečnostní prodleva, kdyby se přišlo na nějaký způsob podvádění.

Systém je kvůli své povaze vhodný pro investory, ale není vhodný pro nové, začínající kryptoměny a není zatím bezpečný tolik, jako Proof of Work, protože ještě neprošel zatěžkávací fází a může se tak objevit díra v systému. Za výhodu se dá považovat, jak je možné vidět z principu fungování, odrazování útoků ekonomickou silou.

Kryptoměny používající tento systém jsou například chystané Ethereum 2.0 (ETH2), Polkadot (DOT) nebo třeba Solana (SOL).

Nespornou výhodou systému Proof of Stake je fakt, že proces není tolik energeticky náročný, jako Proof of Work, od čehož se odvíjí množství spotřebované elektřiny a není k tomu nutný drahý a výkonný hardware. Může se tedy jednat o jednu z ekologičtějších variant těžby kryptoměn. To může mít za následek zvýšení popularity kryptoměn běžících na Proof of Stake systému a tím i zvýšení jejich hodnoty.

Nevýhodou pro validátory jsou odměny pouze ve výši poplatku za potvrzení transakce, které musí být malé, protože by se jinak nevyplatilo provádět transakce v dané kryptoměně.

Příklad transakce: *Alena se rozhodla poslat Bořkovi 10 SOL, přičemž poplatek za ověření platby je 0,001 SOL. Transakci je třeba ověřit, a tak systém vybere validátora Cyrila, protože ten v tu danou chvíli ručí svými 2000 SOL, což je zrovna nejvíce ze všech validátorů. Cyrilův počítač následně ověří blok plateb, ve kterém je obsažena i platba ve výši 10 SOL od Aleny pro Bořka. Blok plateb je v pořádku, Cyrilův počítač uzavře blok transakcí a zapíše jej do blockchainu. Bořek dostane na účet od Aleny 10 SOL a Cyril dostal za validaci 0,001 SOL.*

1.10 Farmaření – systém Proof of Space and Time

Po třech letech vývoje přišla v květnu 2021 na svět kryptoměna jménem Chia Network (XCH), u které si její vývojáři v čele s Bramem Cohenem [16] kladou za cíl konkurovat síti Bitcoin, avšak mnohem ekologičtějším způsobem.

Od toho se odvinul nový pojem, kdy místo pojmu „těžba kryptoměn“ je využíván pojem „farmaření kryptoměn“, stejně jako samotný název kryptoměny, Chia, který odkazuje na současně velmi oblíbená semínka pouštní rostliny *Salvia Hispanica*, která se nazývají stejně a jsou v současnosti velkým trendem.

Vývojáři taktéž přišli s algoritmem pro farmaření, nazývaným POST – Proof Of Space And Time.

POST algoritmus se skládá ze dvou funkcí:

Proof of Space funkce je využívání prázdného místa (minimálně však 100 GB), primárně na pevném Hard Disk Drive (HDD), nebo případně polovodičovém Solid State Drive (SSD) disku, kam se zapisují velké datové soubory, takzvané záhony neboli parcely, anglicky *„plot“*, které obsahují „imaginární chia semínka“ (jiný název pro hashe).

Proof Of Time funkce zajišťuje bezpečnost a zamezuje falšování výpočtů v Proof of Space. Taktéž zajišťuje ekologičnost procesu, že není třeba paralelního zvětšování výpočetního výkonu.

Princip farmaření: Uživatel, zvaný farmář, anglicky *„farmer“*, si určí maximální velikost záhonů obsahujících imaginární chia semínka a dá svolení k jejich generování a ukládání na disk. Záhon s imaginárními chia semínky je vlastně již předdefinovaný výpočet pro blockchain. Při vytváření záhonu – souboru o velikosti 100 GB, je potřeba pro jeho vytvoření zapsat na disk až 1 200 GB dat, ze kterých se poté propočítá záhon o finální velikosti 100 GB. Tímto způsobem připraví farmář svůj záhon. Program následně každých 18 sekund odesílá farmářovi výzvy, které obsahují transakci převodu a na každou výzvu farmář (respektive jeho kryptofarma) prohledá své „záhony“ za účelem nalezení hashe – imaginárního chia semínka odpovídajícího požadovanému bloku transakcí. V případě že uživatel má k dispozici dané imaginární chia semínko, tak poté obdrží určitou částku (současně 2 XCH) a blok plateb se odešle do blockchainu. Z principu je zřejmé, že se pravděpodobnost získání odměny zvyšuje s větším počtem záhonů. Zde vzniká problém, že pokud se Chia Network stane populární měnou, může způsobit nedostatek SSD či HDD disků.

Vzhledem k tomu, že u POST algoritmu jde o velké množství dat, tak se využívají SSD disky, které provádějí vstupně/výstupní operace mnohem rychleji než HDD disky. Bohužel, standardní SSD disky mají životnost okolo 300-600 TB zápisu, tedy SSD pevný disk vydrží vytvořit cca 600 záhonů (to odpovídá 60 TB imaginárních chia semínek/záhonů uložených na disku). K farmaření se tak používají i HDD disky, které sice vstupně/výstupní operace provádějí pomaleji, ale za stejnou pořizovací cenu má farmář několikanásobné větší množství paměti než v případě pořizování SSD disku, tudíž může vytvořit více záhonů.

Od druhé poloviny roku 2021 je k dispozici nová metoda plotování, která snižuje množství vstupních a výstupních operací zápisu ze zhruba 1200 GB na cca 300 GB pro 100 GB záhon, přičemž zbytek jejich zbytek probíhá v paměti RAM. Výsledný plot je možné mít uložený na standardním HDD disku.

Příklad transakce: *Alena chce poslat Bořkovi 100 XCH. Transakce je zapracována do bloku a ten je třeba ověřit. Systém pošle všem farmářům, nejdéle po 18 sekundách požadavek a počítače farmářů začnou prohledávat své záhony, zda mají ve svých záhonech imaginární chia semínko, které je stejné, jako v bloku transakcí. Kryptofarma farmáře Cyrila zjistí, že zrovna v jednom z jeho záhonů je odpovídající chia semínko. Blok je tím pádem ověřen, zapsán do blockchainu a Bořkovi se na účtě objeví 100 XCH od Aleny a Cyril dostane odměnu 2 XCH za ověření platby/bloku.*

1.11 Kryptoměnové útoky

1.11.1 Cryptojacking

Dle společnosti ESET [17] existují dvě varianty. V první si oběť do počítače nainstaluje spustitelný program – malware, který se následně zmocní výpočetního výkonu počítače oběti a útočník skrz něj začne těžit kryptoměny.

Druhou variantou je úryvek kódu psaného primárně v jazyce JavaScript. Ten je vložený do webové stránky, která může být napadena buď bez vědomí majitele, anebo napadený skript majitel omylem sám vloží místo skriptu s reklamou. Počítač je tedy napaden dočasně prostřednictvím internetového prohlížeče.

Tyto útoky společnost ESET detekovala na mobilních zařízeních s operačním systémem Android, a i všech populárních počítačových platformách, přičemž byly většinou klasifikovány jako potenciálně nechtěné aplikace, ale některé z detekovaných útoků byly zařazeny do více nebezpečné kategorie trojských koní.

Tato nelegální těžba kryptoměn funguje na bázi vysoké aktivity procesoru se znatelnými vedlejšími účinky. Mezi tyto účinky můžeme zařadit viditelné snížení výkonu zařízení, jeho přehřívání, a také zvýšenou aktivitu ventilátoru projevující se hlukem, spojenou se zmíněnou vysokou aktivitou procesoru. Uvádí se, že u zařízení s operačním systémem Android dále může vést zvýšená aktivita procesoru ke kratší životnosti baterie, zvýšené teplotě zařízení, nižší výkonnosti nebo dokonce

k takzvanému „nafouknutí“ baterie, což zapříčiňuje fyzické poškození nebo úplné zničení zařízení.

Někdy ovšem problémy s výkonem způsobují obecné potíže, ať už s hardwarem nebo softwarem. Společnost ESET dále uvádí, že škodlivý Cryptojacking lze poznat podle toho, když se zvýšená zátěž zařízení začne projevovat až poté, co je navštívena nakažená webová stránka obsahující JavaScript kód pro skrytou nelegální těžbu kryptoměn.

Jako prevenci před nelegální těžbou doporučuje společnost ESET použít spolehlivé a vícevrstvé bezpečnostní řešení nebo antivirovou ochranu, která blokuje nežádoucí aktivity spojené s malwarem pro nelegální těžbu kryptoměn a dále počítačové viry. Pokud člověk při návštěvě určité webové stránky zjistí výrazně vyšší využití procesoru, pak se doporučuje zavřít webový prohlížeč.

Dále doporučuje ještě restartovat počítač, kvůli zavření skrytých oken prohlížeče, která teoreticky mohou pokračovat s těžbou na pozadí.

1.11.2 51% útok

Neboli „útok většiny“ je dle portálu Binance Academy [18] definován jako *„potenciální útok na blockchainovou síť, kdy jeden subjekt ovládá většinu hashovacího výkonu, což může potenciálně způsobit organizace narušení sítě.“* Jinými slovy, tento portál uvádí, že by útočník měl dostatek těžařského výkonu k tomu, aby měl nadpoloviční výkonovou nadvládu nad kryptoměnovou sítí. Také by mohl zvrátit transakce, které provedl, když měl nad blockchainem kontrolu – což by mělo za následek vznik problému dvojí útraty.

Úspěšný útok většiny by měl za následek takzvaný těžařský monopol. Umožnil by tak útočníkovi například zabránit v potvrzení některých, nebo všech transakcí (odepření transakcí) a dále zabránit některým nebo všem těžařům v těžbě. Naproti tomu útok většiny neumožňuje například zabránit odesílání transakcí jiných uživatelů. Za teoreticky nemožnou se taktéž pokládá změna výše odměny za blok transakcí, tvorba nových mincí dané kryptoměny nebo jejich krádež.

Dále portál Binance Academy uvádí, že vzhledem k velikostem kryptoměnových sítí je nadpoloviční útok u velkých kryptoměnových sítí poměrně nepravděpodobný,

protože pravděpodobnost ovládnutí 51 % těžebního výkonu nad ostatními uživateli je, při současných technických dispozicích, velmi malá. Navíc, čím větší blockchain je, tím hůře se zpětně upravuje díky kryptografickým důkazům. Pokud by se útok, například na síť Bitcoin, vydařil, tak by útočník dokázal upravit transakce pouze v posledních blocích, a to jen na krátkou chvíli. Díky tomu je tento útok v praxi možný pouze na malých a nových kryptoměnách, většinou odvozených, kde není takový problém získat více jak 51 % výkonu celé sítě.

1.11.3 Investiční podvody

O současném problému investičních podvodů pojednává článek z portálu iROZHLAS.cz. [19] Jde o to, že podvodníci využívají, vzhledem k obecné rozšířenosti kryptoměn, neznalosti uživatelů a metod na bázi sociálního inženýrství, kdy se snaží z oběti vylákat peníze pomocí cílené reklamy na sociálních sítích.

Reklama se tváří jako výhodná investiční nabídka, navíc vypadá důvěryhodně, zpravidla jakoby zastřešená velkou firmou, popřípadě vlivnou osobností. Člověk (oběť) se zaregistruje na webových stránkách (pochybné) investiční platformy, kde jé poté telefonicky kontaktován podvodníky vydávajícími se za brokery. Tito podvodníci posléze pomáhají oběti s převáděním peněz na investiční účet. Avšak místo toho, aby se peníze objevily na investiční platformě, končí v kapsách podvodníků.

Dle tohoto článku je celková škoda uváděna 1,5 miliardy CZK.

1.12 Vliv kryptoměn na ekologii

Kvůli potřebě velkého příkonu za sebou výše zmíněná zařízení, konkrétně grafické karty a ASIC-minery zanechávají poměrně velkou uhlíkovou stopu. Dle studie Alexe de Vriese [20] v roce 2018 celosvětová těžba spotřebovala celkově okolo 18,8 GW elektrické energie, což odpovídá spotřebě státu o velikosti Polska.

Skupina vědců z týmu Christiana Stolla [21] dospěla k výsledku, že na jednu Bitcoinovou transakci připadá 271 kg CO_2 a celá Bitcoinová síť má na svědomí roční emise 22-22,9 milionů tun CO_2 a spotřebu 25.8 TWh.

V důsledku rychlé amortizace počítačů, komponent a jiných specializovaných zařízení využívaných pro těžbu, kdy například průměrná životnost čipu ve

specializovaném ASIC mineru (které nemají jiné využití než těžbu) činí okolo 12-16 měsíců, je další hrozbou vznik elektroodpadu. Těžaři totiž dle výše zmíněné studie C. Stolla a jeho týmu celosvětově vyprodukují 30 700 tun odpadu a na jednu transakci průměrně připadá 272 gramů elektroodpadu.

Podle průzkumů CBECI (Cambridge Bitcoin Electricity Consumption index) univerzity v Cambridge [22] se během roku 2021 podařilo snížit použití elektrické energie z uhlí ze 47 % na 37 % a z fosilních paliv z 65 % na 62%, avšak na druhou stranu míra elektrické energie z plynu vzrostla ze 16 % na 25 %. Poměr elektrické energie z udržitelných zdrojů, kam je zařazena jaderná, solární, větrná a vodní energie, vzrostl nepatrně, a to z 35 % na 38 %.

Ekologičnost kryptoměn by se dala, jak logicky vyplývá, zvýšit například ještě větším využitím obnovitelných zdrojů elektrické energie. Zároveň by bylo potřeba přijít se systémem ověřování kryptoměnových plateb takovým, aby nebyl potřeba velký elektrický příkon, a zároveň by nezpůsoboval amortizaci elektrických zařízení k tomu určených.

2 Praktická část

Pro potvrzení, zdali je ekologičtější těžba kryptoměn pomocí systému Proof of Work nebo jejich farmaření pomocí systému Proof of Space and Time, bude využita metoda domácího experimentu.

K němu bude sloužit těžební stroj, který bude těžit kryptoměnu Ethereum pomocí výkonných herních grafických karet a jedna kryptofarma farmařící kryptoměnu Chia pomocí 3,5“ HDD disků, která se jeví jako potenciální ekologičtější varianta těžby kryptoměn. Experiment se bude dále sestávat z výpočtů, převodů a vzájemného porovnávání.

Experiment bude trvat 1 rok (pro každý stroj). Cílem je v obou případech zjistit spotřebu elektřiny a roční výdělek. Naměřené hodnoty se poté budou porovnávat.

Míra ekologičnosti způsobu ověřování plateb se bude odvíjet od ročního množství spotřebované elektrické energie obou strojů, a to tak, že pokud bude mít některý stroj menší roční výdělek, tak bude teoreticky zvětšen a přepočítán, aby měly oba stroje stejnou hodnotu ročního výdělku.

Mezi možné nástrahy experimentu můžeme zařadit volatilitu měnových kurzů, přičemž je obecně známo, že volatilita kryptoměn je ještě vyšší než u normálních měn. Dále pohyby cen elektřiny (CZK/1 kWh), fyzikální proměnné a dále postupná opotřebovanost elektronických zařízení.

Ve výpočtech a převodech je používáno zaokrouhlování na celá čísla nebo na dvě desetinná místa. České koruny jsou zaokrouhlovány na celá čísla.

Pro zjednodušení výpočtů není v experimentech započítáváno zdanění sazbou 15 % ze zisku z každé směny nebo prodeje (nebo 23 % v případě přijmu vyššího než 48násobek průměrné mzdy).

2.1 Stroj těžící Ethereum

K těžbě kryptoměny Ethereum použijeme těžební stroj sestavený z:

- Základní deska ASUS
- Dvoujádrový procesor Intel Core 2 Duo

- Operační paměť RAM Mustang 2 GB DDR3
- 2x počítačový zdroj Zalman 1000 W
- 5x grafická karta AMD Sapphire Radeon R9 390

Základní deska, procesor a paměť RAM byly použity ze starého, již vyřazeného PC.

Těžební stroj byl sestaven na začátku roku 2021, kdy byly k dispozici ještě grafické karty za poměrně přijatelné ceny. V rámci experimentu se podařilo na internetových bazarech nakoupit grafické karty AMD Sapphire Radeon R9 390 za průměrnou cenu 6 000 CZK za kus (leden 2021).

Parametry grafických karet AMD Sapphire Radeon R9 390:

- Typ grafické paměti: DDR5
- Velikost grafické paměti: 8 192 MB
- Rychlost grafického čipu: 1 010 MH/s (H = hashrate, udává těžební výkon grafické karty)
- Doporučený minimální výkon zdroje: 750 W
- Sběrnice: PCI-express 3.0

Pro samotný těžební stroj bylo nutné, vzhledem ke spotřebě elektřiny v případě grafických karet, dokoupit ještě 2x počítačový zdroj Zalman o výkonu 1 000 W (1 000 CZK za kus), dále PCI-express 3.0 adaptér pro 4 grafické karty (1 000 CZK za kus) a počítačovou skříň (600 CZK), ve které je těžební stroj umístěn.

Po sečtení nákladů cena těžebního stroje činila 33 600 CZK.

Software:

Jako operační systém byl v těžebním stroji použit, vzhledem k použité základní desce, OS Linux, konkrétně v jeho distribucích CentOS 6.0 a OS Hiveon.

Pro těžení kryptoměny Ethereum bylo využito napojení na mining pool. Pro experiment bylo vybráno prostředí nanopool.org

Průběh těžby:

V prvním čtvrtletí roku 2021 byl použit těžební program PhoenixMiner ve verzích 5.3 až 5.5b. Toto období bylo ve znamení různých zkoušek a optimalizací, kdy se

zkoušely různé varianty nastavení systému a grafických karet. Byly zkoušeny i jiné těžební programy, konkrétně Nanominer a LolMiner.

Během tohoto období s použitím OS Centos 6.0 a PhoenixMiner dosahovala spotřeba elektřiny u těžebního stroje cca 1 000 W, přičemž hlavním problémem zde byla nemožnost řídit otáčky ventilátorů u grafických karet – jejich výkon byl konstantně nastaven na 90 %, což zapříčiňovalo zvyšování spotřeby elektrické energie. Během toho dosahovaly grafické karty průměrné teploty 48 °C. Výpočetní výkon jedné grafické karty činil 25 977 MH/s.

Během března 2021 byl nahrazen OS Centos za řešení OS Hiveon, který je určený primárně pro těžbu kryptoměn. To umožnilo provést aktualizaci firmwaru grafických karet, konkrétně byl nahrán firmware optimalizovaný pro matematické výpočty blockchainu kryptoměny Ethereum. Nespornou výhodou tohoto řešení byla například možnost již řídit otáčky ventilátorů chlazení na základě teploty grafické karty. Díky tomu se úspěšně podařilo snížit otáčky ventilátorů grafických karet na zhruba 40 %. Teplota grafických karet se pohybovala v rozmezí 55-60 °C.

Došlo sice k ponížení výkonu grafických karet na cca 23 000 MH/s z původních 25 977 MH/s za kartu, ale celkový potřebný příkon stroje poklesl z 1000 W na 800 W.

Vedlejší výhodou, která je ovšem většinou považována za nevýhodu, bylo i velké vytváření tepla při těžbě (laickým odhadem 400 W tepelného výkonu). Stroj byl totiž umístěn ve vlhkém, větratelném, chladném sklepě, kde se teplota pohybovala okolo 15 °C. Pomocí těžebního stroje se podařilo vytopit sklep na 23 °C za zhruba týden, což pomohlo následně i snížení vlhkosti.

Nevýhodou tohoto těžebního stroje byla hlučnost dána chlazením grafických karet, proto byl umístěn ve sklepě.

2.2 Těžba kryptoměny Ethereum

Jako rozhodné období pro stanovení výhodnosti těžby bylo vybráno období od druhého čtvrtletí roku 2021 do prvního čtvrtletí roku 2022. Pro účely experimentu použit již odladěný a plně optimalizovaný těžební stroj.

Poznámka: *V tomto experimentu nebereme v úvahu amortizaci těžebního stroje, primárně grafických karet obsažených v něm, vzhledem k plánovanému přechodu kryptoměny Ethereum z těžebního systému Proof of Work na modernější Ethereum 2.0 (ETH2) pracující na jiném systému – Proof of Stake. (V době psaní této práce již existují testovací verze ETH2.)*

Během daného období stroj těžil kryptoměnu Ethereum, která byla po každém čtvrtletí směněna ve směnárně na měnu euro. Ve směněné hodnotě mezi měnou euro a kryptoměnou Ethereum jsou započítány i poplatky směnárny. Měna euro je dále převedena ještě na české koruny, konkrétně podle průměrného kurzu devizového trhu v daných čtvrtletích dle dat České národní banky [23].

Tabulka 1: Počet vytěžené kryptoměny Ethereum a směnné kurzy. (Písmeno Q v tabulce označuje kvartál (čtvrtletí) a číslo za písmenem Q pořadí kvartálu v daném roce.)

Období	**Vytěženo ETH**	**Kurz 1 ETH = EUR**	**Směněno na EUR**	**Kurz 1 EUR = CZK**	**Částka v CZK**
2Q 2021	0,4	2342,5	937	25,64	24 025
3Q 2021	0,4	2055	822	25,50	20 961
4Q 2021	0,4	2755	1 102	25,38	27 969
1Q 2022	0,4	3150	1 260	24,65	31 059

Obrázek č. 1: Graf vývoje ceny kryptoměny Ethereum vůči měně euro v době experimentu. (Zdroj: Kurzy.cz [24])

Obrázek č. 2: Graf vývoje ceny kryptoměny Ethereum vůči české koruně v době experimentu. (Zdroj: Kurzy.cz [24])

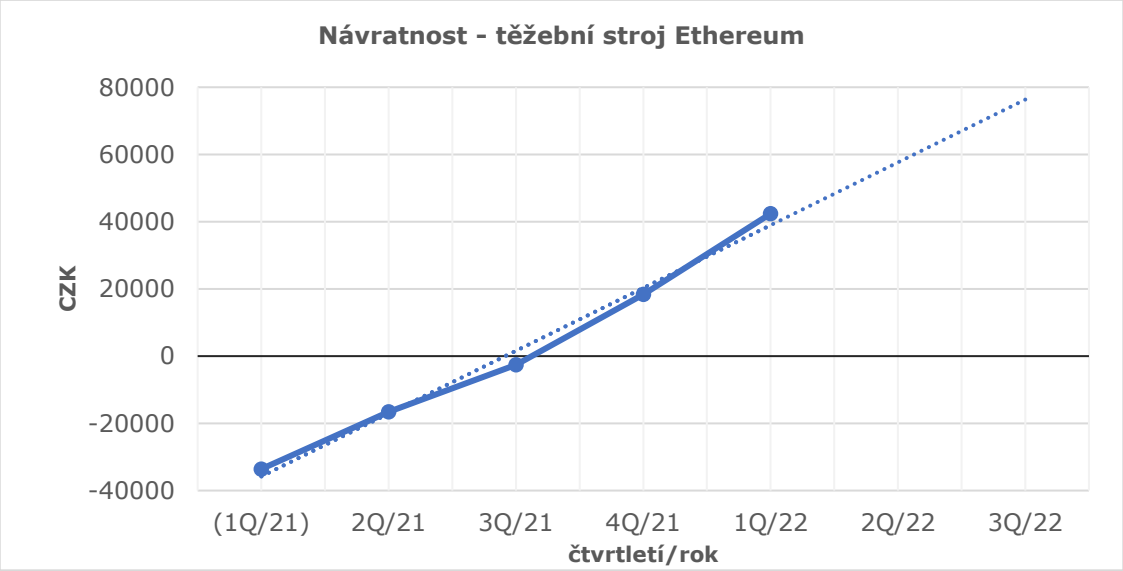
Celkem bylo v období experimentu vytěženo **1,6 ETH**, směněných na **4 121 EUR**, což odpovídá ekvivalentu **104 014 CZK**.

Cena elektřiny byla během doby provádění experimentu zafixována na ceně **4 CZK/kWh**.

Průměrná hodinová spotřeba elektřiny u těžebního stroje činila **800 W/h**, což se rovná spotřebě 19,2 kW za den provozu (76,8 CZK/den) a **1752 kW** za čtvrtletí. Čtvrtletní náklady na elektřinu tak činí **7008 CZK**. Celková spotřeba elektřiny u těžebního stroje během experimentu, který trval 365 dní, tak činila **7 008 kW**, což při ceně 4 CZK/kWh odpovídá **28 032,- Kč.**

Pokud odečteme od vytěžených 104 014 CZK náklady na pořízení těžebního stroje, které činily 33 600 CZK a náklady na elektřinu v hodnotě 28 032 CZK, tak se dostáváme na částku **42 382 CZK ročního výdělku**, což odpovídá **průměrnému výdělku 3 532 CZK/měsíc**.

Návratnost investice, kterou označujeme roční poměr výnosu k investovaným penězům, vypočítáme z čistého ročního výdělku 42 382 CZK a nákladů na nákup těžebního stroje a elektřiny, které dohromady činí 61 632 CZK. Z toho dostaneme výsledek poměru, 0,688, který následně vynásobíme 100 za účelem získání procentuální hodnoty. **Návratnost investice tak činí 68 % po prvním roce.**



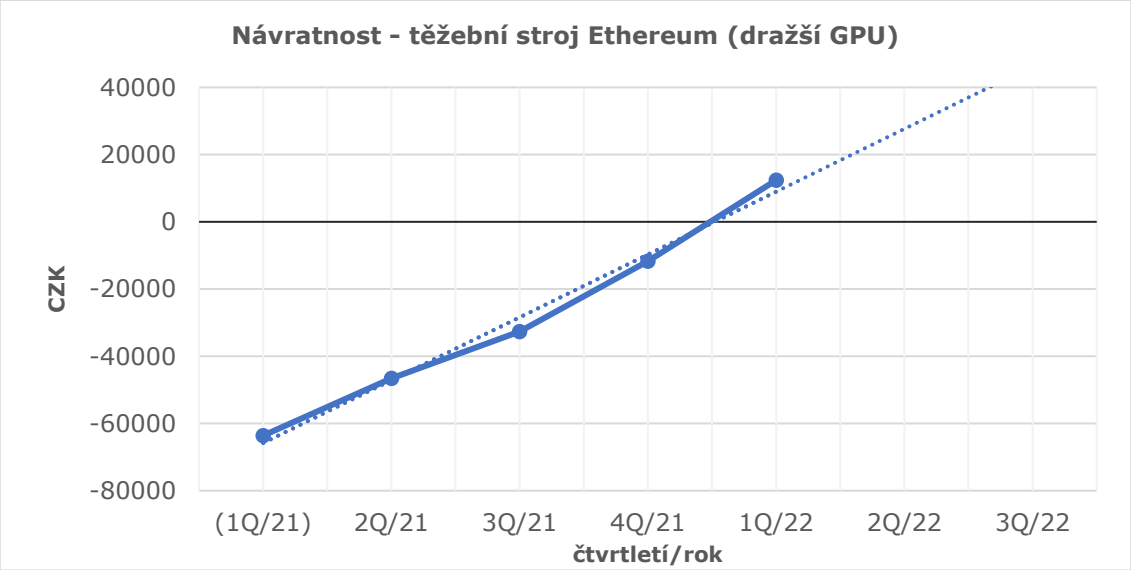
Obrázek č. 3: Graf návratnosti investice do těžebního stroje těžícího kryptoměnu Ethereum. (Zdroj: autor)

Z grafu uvedeného výše je patrné, že se náklady na těžební stroj zaplatily již po 2 čtvrtletích těžby. Odchylky od vývoje trendu jsou způsobeny pohyby měnových kurzů.

Varianta 2: *Je obecně známo, že se v průběhu roku 2021 tržní cena grafických karet, kvůli velké poptávce a nedostatku čipů, zhruba zdvojnásobila. Pokud bychom vzali v úvahu tuto dvojnásobnou pořizovací cenu grafických karet, což je navýšení z původních 6 000 CZK/kus na 12 000 CZK/kus, pořizovací cena těžebního stroje by vyšla v našem případě na 63 600 CZK (po započtení dvou počítačových zdrojů a PCI-express adaptéru v celkové hodnotě 3 600 CZK).*

V tomto případě, kdy bychom od vytěžených 104 014 CZK odečetli náklady na pořízení těžebního stroje v hodnotě 63 600 CZK a náklady na elektřinu činící 28 032 CZK, dostali bychom se na částku 12 382 CZK ročního výdělku, což odpovídá průměrnému výdělku 1 031 CZK/měsíc.

Návratnost investice by tak činila 13,51 % po prvním roce.



Obrázek č. 4: Graf návratnosti investice do těžebního stroje těžícího kryptoměnu Ethereum v případě dvojnásobně dražších grafických karet. (Zdroj: autor)

Z grafu uvedeného výše je patrné, že by se náklady na těžební stroj zaplatily po 3 čtvrtletích těžby. Odchylky od vývoje trendu jsou způsobeny pohyby měnových kurzů.

2.3 Chia kryptofarma

Kryptofarma, která farmaří kryptoměnu Chia byla sestavena z:

- Základní deska B450M Pro4-F
- Procesor AMD Ryzen 5 3600
- Operační paměť RAM Kingston o velikosti 32 GB
- 10x 3,5“ HDD harddisk Toshiba Enterprise o kapacitě 14 TB

Celková kapacita harddisků sloužících k plotování činí 140 TB.

Parametry harddisků Toshiba:

- Kapacita 14 000 GB
- Rychlost: 7 200 otáček/min
- Rozhraní SATA III (6 Gbit/s)
- Cache vyrovnávací paměť o velikosti 512 MB

Potřebné harddisky byly nakoupeny na internetových bazarech za průměrnou cenu 8 000 CZK za kus.

Základní deska, procesor a operační paměť RAM byly použity v domácnosti již dříve, jako NAS server (chytré datové úložiště), a to s distribucí operačního systému Linux OS Debian.

Pro samotnou kryptofarmu bylo nutné dokoupit jeden SSD disk s rozhraním NVME o kapacitě 1 TB, určený pro vytváření plotů (2 800 CZK) a PCI-express adaptér pro 10 SATA III připojení (1 000 CZK za kus). Konstrukce pro harddisky byla sestavena ze stavebnice, která se nacházela v domácnosti.

Investice do kryptofarmy činila 83 800 CZK.

Kryptofarma byla sestavena v průběhu druhého pololetí roku 2021, kdy byla kryptoměna Chia již zavedena, a zároveň existovala její dostatečná podpora pro softwarové vybavení.

Původní spotřeba elektrické energie celého NAS datového úložiště činila 70 W. Přidáním harddisků byla spotřeba zvýšena o 50 W, tedy během experimentu byla spotřeba elektrické energie 120 W.

Software:

Jako operační systém byl použit již fungující, výše zmíněný OS Debian. Pro samotné farmaření byl nainstalován z GIT oficiální program pro měnu Chia v Linux Ubuntu/Debian variantě.

Před samotným plotováním (plněním disků) bylo nutné rozhodnout, jestli farmaření bude prováděno jako samostatný stroj nebo jestli bude farmaření prováděno pomocí napojení na farming pool (obdoba mining pool).

Pro odhad, kdy je shoda v plotech nalezena, je možné využít oficiální Chia kalkulátor, který lze nalézt na webových stránkách https://www.chiacalculator.com/. Ten při cca 1 400 plotech (odpovídajících úložišti o velikosti 140 TB) odhadoval nalezení shody do 1 měsíce. Tedy ziskovost by měla být zhruba 2 XCH za měsíc, avšak nalezení shody není nikdy zaručeno.

Při samostatném farmaření kryptoměna Chia je výhodou, že v případě nalezení shody je zaslána odměna 2 XCH. Pro farmaření bylo nakonec použito napojení na farming pool (samotné výsledky jsou uvedeny níže). V rámci farmaření ve farming poolu je výhodou, stejně jako u mining poolů, že uživatel dostává "podíl" za farmaření i od ostatních farmářů. Nevýhodou farmaření ve farming poolu je, že v případě nalezení shody je odměna rozdělena na 0,25 XCH jako odměna konkrétnímu farmáři a 1,75 XCH je zasláno farming poolu pro přerozdělení zisku ostatním farmářům.

Pro samotné farmaření bylo nutné nejdříve vytvořit ploty pro farming pool. Pro jejich vytvoření byl použit softwarový nástroj od "madMAx43v3r", nalezený na GitHub. Ten narozdíl od originálního Chia plotovacího nástroje snižuje náročnost generování plotů pomocí využití operační paměti RAM.

V rámci generování jednoho plotu (souboru hashů o velikosti 100 GB) je nutné, jak je uvedeno v teoretické části, provést různé přepočty, které dosahují cca 1 TB zápisu na disk, ze kterých je následně propočítán jeden plot. Proto byl pro plotování použit rychlejší SSD disk s NVME konektivitou. Díky tomu se povedlo zrychlit plotování na cca 75 minut/plot z původních 120 minut/plot. Po naplotování již nebyl SSD disk s NVME konektivitou používán.

Pro zaplnění všech HDD harddisků bylo vytvořeno 1412 plotů. Časová náročnost plotování činila 105 900 min, což odpovídá 73 dnům.

Pokud by byl v rámci experimentu při plotování použit originální Chia plotovací nástroj, tak by tento proces trval 169 440 min, což odpovídá 117 dnům.

Jako výhoda tohoto procesu se ukázalo, že míra vznikajícího odpadního tepla byla zanedbatelná, nebylo třeba používat aktivní chlazení pro harddisky (např. větrákem).

2.4 Farmaření kryptoměny Chia

Jako rozhodné období pro stanovení výhodnosti vezmeme období farmaření kryptoměny Chia od začátku ledna do konce prosince roku 2022, kdy byla k experimentu použita naplotovaná, odladěná, stabilní kryptofarma.

Poznámka: V tomto experimentu nebereme v úvahu amortizaci kryptofarmy, primárně harddisků obsažených v ní.

Během experimentu s kryptofarmou bylo za celou dobu jeho trvání nalezeno 7 shod a vyfarmařeno **20,2 XCH**, což odpovídá průměrnému měsíčnímu výdělku **1,69 XCH**.

Vyfarmařená částka 20,2 XCH byla směněna na kryptoměnu Ethereum v hodnotě **0,48 ETH**, a to jednorázově na konci experimentu v prosinci 2022, přes burzu okx.com při kurzu 1 ETH = 41,67 XCH.

Výše zmíněných 0,48 ETH bylo následně směněno na 792 EUR (kurz 1 ETH = 1 650 EUR), což odpovídá ekvivalentu **19 221 CZK za rok farmaření** (dle měsíčního průměru pro prosinec 2022 – kurz devizového trhu České národní banky [23], který byl 1 EUR = 24,27 CZK). Kryptofarma tedy vyfarmařila **průměrně 1 602 CZK měsíčně**, což lze převést na **4 805 CZK za čtvrtletí.**

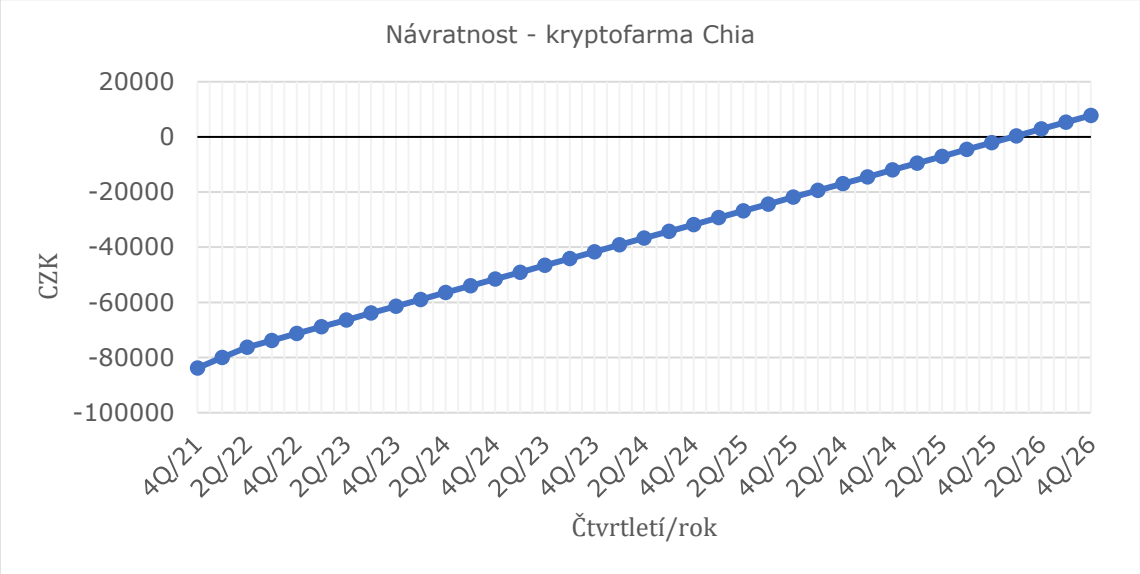
Průměrná hodinová spotřeba elektřiny u kryptofarmy činila **120 W/h**, což odpovídá spotřebě elektřiny 2,88 kWh/den. Roční spotřeba tak odpovídá **1 051,2 kW**.

První půlrok byla cena elektřiny fixována na ceně 4 CZK/kWh. První půlrok kryptofarma spotřebovala elektřinu v hodnotě 2 073 CZK. Druhý půlrok byla cena elektřiny tržní a činila 9 CZK/kWh, tedy druhý půlrok byla spotřebována elektřina

v hodnotě 4 666 CZK. Za dobu experimentu (1 rok) tak činily náklady na elektřinu **6 739 CZK**.

Pokud odečteme od vyfarmařených 19 221 CZK náklady na pořízení kryptofarmy, které činily 83 800 CZK a náklady na elektřinu v hodnotě 6739 CZK, tak se bohužel dostáváme na částku **-71 318 CZK čistého průdělku po prvním roce**, což odpovídá **průdělku 5943 CZK/měsíc**.

Investice tak činí **ztrátovost 78,78 % po prvním roce**.



Obrázek č. 5: Graf návratnosti investice do Chia kryptofarmy. (Zdroj: autor)

Z grafu uvedeného výše je patrné, že by se náklady na kryptofarmu teoreticky zaplatily po 4 letech, konkrétně v prvním čtvrtletí roku 2026.

Pokud bychom odhadli životnost harddisků na 5 let, což nemusí být pravděpodobné, vzhledem k bazarovému původu, tak by při zachování cenového kurzu a ceně elektřiny 9 CZK/kWh teoretický výdělek činil 7 784 CZK za jejich životnost.

Díky tomu můžeme prohlásit, že se za současných podmínek farmaření kryptoměny Chia prakticky nevyplatí. Buďto by bylo třeba pořídit harddisky nové, nebo cena této kryptoměny by se musela několikanásobně zvětšit, nebo by se musely zlevnit elektronické součástky, aby se její farmaření finančně vyplatilo.

Obrázek č. 6: Graf vývoje ceny kryptoměny Chia Network vůči měně euro v době experimentu. (Zdroj: Kurzy.cz [25])

Obrázek č. 7: Graf vývoje ceny kryptoměny Chia Network vůči české koruně v době experimentu (Zdroj: Kurzy.cz [25])

2.5 Porovnání procesů z hlediska ekologičnosti

Abychom mohli porovnat ekologičnost obou procesů, je nutné přepočítat některé parametry. Nebereme přitom v úvahu původ elektřiny, jestli je z fosilních paliv nebo z obnovitelných zdrojů.

Stroj těžící kryptoměnu Ethereum v experimentu pracoval při spotřebě 800 W/h, přičemž za rok vytěžil 104 014 CZK.

Za tímto účelem teoreticky zvětšíme v experimentu využitou Chia kryptofarmu. A to konkrétně 5,41krát, aby byl roční výdělek stejný, jako v případě stroje těžícího kryptoměnu Ethereum. Tudíž z původních 140 TB teoreticky zvětšíme kapacitu HDD disků na 757 TB, což by znamenalo přidání dalších 44 kusů 14 TB harddisků Toshiba. Pokud by se je podařilo obstarat za stejnou cenu, jako v kryptofarmě použité disky (8 000 CZK/kus), tak by cena přikoupených HDD harddisků činila 352 000 CZK. Dále by bylo potřeba zakoupit 5 SATA připojení (každé pro 10 HDD harddisků), což jsou další náklady v hodnotě 5 000 CZK. Vzhledem k tomu, že SSD disk s NVME konektivitou sloužící pro plotování má životnost okolo 4 000 plotů, bylo by potřeba přikoupit ještě 1 disk s NVME konektivitou, jelikož by bylo potřeba propočítat 7 570 plotů. Tímto ještě musíme připočíst 2 800 CZK. Celková pořizovací ceny této kryptofarmy by tak, místo původních 83 800 CZK činila **443 600 CZK**, což je **5,3x více**.

Pro zaplnění všech HDD harddisků by bylo vytvořeno výše zmíněných 7570 plotů. Časová náročnost plotování za použití softwarového nástroje “madMAx43v3r”, umožňujícího zkrácení doby plotování ze 120 min/plot na 75 min/plot, by činila 567 750 min, což odpovídá přibližně 394 dnům. Pokud by byl při plotování použit v rámci experimentu originální Chia plotovací nástroj, tak by tento proces trval 908 400 min, což odpovídá skoro 631 dnům.

Co se týče spotřeby elektrické energie, tak při uvažování spotřeby 1 HDD harddisku 5 W/h, by se z původní spotřeby celé kryptofarmy činící 120 W, přidáním dalších 44 harddisků, spotřeba navýšila o 220 W/h na průměrných 340 W/h. To odpovídá spotřebě 8,16 kW za den a 2978,4 kW za rok.

v případě experimentu s těžebním strojem těžící kryptoměnu Ethereum jsme došli k roční spotřebě elektřiny 7 008 kW a v případě experimentu s Chia kryptofarmou 1 051,2 kW. Pokud porovnáme průměrnou spotřebu elektrické energie obou strojů, přičemž teoreticky zvětšíme Chia kryptofarmu, aby měla stejný roční výdělek, jako Ethereum těžební stroj, tak nám vychází roční spotřeba 2978,4 kW. Ve výsledku je tedy **farmařit kryptoměnu Chia 2,4x méně energeticky náročné** než těžit kryptoměnu Ethereum pomocí těžebního stroje.

Ani u teoreticky zvětšené Chia kryptofarmy by nemělo docházet k potřebě aktivního chlazení, vzhledem k principu ověřování plateb.

Pro ještě větší ekologičnost by bylo vhodné zajistit alespoň částečné napojení Ethereum těžebního stroje a Chia kryptofarmy na nějaký zdroj obnovitelné elektrické energie, například na fotovoltaickou nebo vodní elektrárnu.

Zatímco stroj těžící kryptoměnu Ethereum produkoval značné množství odpadního tepla (jak bylo zmíněno, laickým odhadem 400 W tepelného výkonu), tak u kryptofarmy nebylo třeba jejího aktivního chlazení.

2.6 Obecné porovnání

Investice do vybavení činila u těžebního stroje na kryptoměny Ethereum 33 600 CZK a u Chia kryptofarmy šlo o investici v hodnotě 83 800 CZK, což je zaokrouhleně 2,5krát více.

Aby Chia kryptofarma poskytovala stejný roční výdělek, jako Ethereum těžební stroj, bylo by potřeba dokoupit komponenty v hodnotě 359 800 CZK, přičemž celková cena kryptofarmy by tak činila 443 600 CZK, což je 13,2krát více.

Roční výdělek bez odečtení nákladů na pořízení stroje a elektřiny u těžebního stroje na Ethereum činil 104 014 CZK za rok a u Chia kryptofarmy činil 19 221 CZK. Výdělek byl u těžebního stroje na Ethereum 5,41krát vyšší.

Jak bylo zmíněno v minulé podkapitole, pokud porovnáme průměrnou spotřebu elektrické energie obou strojů, přičemž bereme v úvahu teoreticky zvětšenou Chia kryptofarmu, tak je ve výsledku **farmaření kryptoměny Chia 2,4x méně energeticky náročné** než těžba kryptoměny Ethereum pomocí těžebního stroje.

2.7 Praktické klady a zápory systémů ověřování plateb

Těžba kryptoměny Ethereum: Značným kladem těžby kryptoměny Ethereum je poměrně rychlá návratnost investovaných prostředků (v našem případě cca 6 měsíců).

Dalším kladem je nižší vstupní investice do potřebného hardware.

Za nevýhodu musíme považovat vysokou spotřebu elektrické energie, která je, kromě výpočetního výkonu, dále převedena na odpadní teplo (odpadní teplo může být i výhodou, pokud lze uplatnit těžební stroj jako zdroj tepla).

Farmaření kryptoměny Chia: Zde za největší výhodu můžeme považovat několikanásobně (2,3x) menší spotřebu elektrické energie. Dále, že zde nevzniká skoro žádné, resp. Zanedbatelné množství odpadního tepla (v našem experimentu postačilo pasivní chlazení, a i tak nedocházelo k přehřívání harddisků.)

Nevýhodou je časově delší návratnost investovaných prostředků pohybující se v řádu let.

Dále jako nevýhodu můžeme považovat znatelně menší výnosnost, ke které patří ještě finančně náročnější vstupní investice.

Nelze také opomenout čas strávený plotováním disků, který může být v řádech měsíců i let, než jsou HDD harddisky připraveny k samotnému farmaření. Dále je limitující životnost harddisků, která je u nových odhadována na 5 let.

Jak bylo zmíněno, za našich podmínek se farmaření kryptoměny Chia prakticky nevyplatilo.

3 Kryptoměnový slovník

Vzhledem k množství pojmů používaných ve světě kryptoměn tato práce přináší jejich základní souhrnný přehled. Pojmy jsou uváděny v následujícím formátu:

(anglický) výraz = *český překlad* – vysvětlení

- **51 % attack** = *51 % útok* – útok, při kterém těžař ovládá nadpoloviční většinu výkonu celé sítě
- **Bitcoin** = *bitová mince* – nejznámější kryptoměna, založena Satoshi Nakamoto
- **Blockchain** = *řetězec bloků* – virtuální „účetní kniha"
- **Cryptocurrency** = *kryptoměna* – digitální, virtuální měna, nehmotná movitá věc
- **Crypto wallet** = *kryptopeněženka* – slouží k uchovávání kryptoměn, obdoba bankovního účtu
- **Cryptojacking** = *krypto „nabourání se"* – kyberútok, kdy útočník zneužívá internetový prohlížeč a výpočetní výkon počítače oběti k nelegální těžbě kryptoměn
- **Farmers** = *farmáři* – ověřovatelé plateb pracující pomocí algoritmu Proof of Space and Time
- **Hash** = *(nelze přeložit)* – matematický algoritmus, podstata blockchainu, vyniká výpočetní složitostí
- **Hashrate =** *množství hashů* – výpočetní výkon zařízení při tvorbě hashů, jednotka H, udávaná za konkrétní čas
- **Miners =** *těžaři* – ověřovatelé plateb pracující pomocí algoritmu Proof of Work
- **Proof of Space** = *důkaz o místě* – část algoritmu Proof of Space and Time, algoritmus sloužící k ověřování plateb, farmaření
- **Proof of Stake =** *důkaz o vkladu/podílu* – algoritmus sloužící k ověřování plateb, kdy je ručeno vkladem, validace
- **Proof of Time** = *důkaz o čase* – část algoritmu Proof of Space and Time, algoritmus sloužící k ověřování plateb, farmaření
- **Proof of Work** = *důkaz o vykonané práci* – algoritmus sloužící k ověřování plateb pomocí jejich těžby
- **Validators** = *validátoři* – ověřovatelé plateb pracující pomocí algoritmu Proof of Stake

Závěr

Cílem této bakalářské práce bylo v teoretické části seznámení čtenáře s obecným popisem fungování kryptoměn, jejich historií, s riziky, úskalími, nynějšími trendy a s technologií blockchain. Dále se čtenář seznámil se současnými principy ověřování transakcí, a to s těžbou kryptoměn pomocí systému Proof of Work, dále pomocí systému pro farmaření kryptoměn Proof of Space and Time a validováním kryptoměn pomocí systému Proof of Stake.

V praktické části se práce zaměřovala na to, zda může být farmaření kryptoměn pomocí systému Proof of Space and Time (kryptoměna Chia) opravdu ekologičtější než jejich těžba pomocí systému Proof of Work (kryptoměna Ethereum).

Podařilo se nám úspěšně potvrdit, že farmaření kryptoměn je opravdu ekologičtější než jejich těžba. V rámci experimentu bylo nakonec potřeba teoreticky 5,41x zvětšit Chia kryptofarmu, aby produkovala stejný roční výdělek jako Ethereum těžební stroj. Porovnání probíhalo na základě průměrné roční spotřeby elektrické energie, která byla u teoreticky zvětšené Chia kryptofarmy (kterou by nebylo potřeba ani aktivně chladit) 2798,4 kW, což je 2,4x méně než v případě stroje těžícího kryptoměnu Ethereum, kde spotřeba elektrické energie činila 7008 kW a vznikalo zde ještě velké množství odpadního tepla (odhadem 400 W).

Vzhledem k nízké ceně kryptoměny Chia a dalším faktorům se farmaření kryptoměny Chia vyplatí pouze po nákupu velmi levného, avšak kvalitního hardware, přičemž pořizovací cena velké kryptofarmy se může i tak pohybovat v rámci statisíců českých korun, narozdíl od Ethereum těžebního stroje, kde investice do finančně vynášejícího hardware šplhají do řádu desítek tisíc českých korun. U farmaření je třeba také počítat s časově delší návratností investovaných prostředků, a to několik let, narozdíl od několika měsíců v případě Ethereum těžebního stroje, a se samotným plotováním harddisků, které může trvat i roky. Náklady za elektřinu lze omezit napojením těžebního stroje či kryptofarmy na obnovitelný zdroj elektrické energie (například solární panely či vodní elektrárnu), avšak zde následně vznikají další investiční náklady.

K dalšímu ekologickému pokroku může dojít rozšířením systému Proof of Stake.

Seznam použité literatury

[1] BINANCE ACADEMY. Co je Proof of Stake (PoS)? *Binance Academy* [online]. Dostupné z: https://academy.binance.com/cs/articles/proof-of-stake-explained

[2] FERGUSON, Niels a Bruce SCHNEIER. *Practical cryptography*. New York: Wiley, 2003. ISBN 978-0-471-22894-3.

[3] FINEX MEDIA S.R.O. Kryptoměny ▶ Jak fungují a jak na nich vydělat? Vysvětlení, seznam a kurzy kryptoměn. *finex.cz* [online]. Dostupné z: https://finex.cz/rubrika/kryptomeny/#co-jsou-kryptomeny

[4] MEUNIER, Sebastien. Blockchain 101. In: *Transforming Climate Finance and Green Investment with Blockchains* [online]. B.m.: Elsevier, 2018 [vid. 2021-12-01], s. 23–34. ISBN 978-0-12-814447-3. Dostupné z: doi:10.1016/B978-0-12-814447-3.00003-3

[5] NIAN, Lam Pak a David LEE Kuo CHUEN. Introduction to Bitcoin. In: *Handbook of Digital Currency* [online]. B.m.: Elsevier, 2015 [vid. 2021-12-01], s. 5–30. ISBN 978-0-12-802117-0. Dostupné z: doi:10.1016/B978-0-12-802117-0.00001-1

[6] PER PARTES CONSULTING S.R.O. Blockchain. *Per Partes Consulting* [online]. Dostupné z: https://perpartes.cz/kontakt

[7] PŘISPĚVATELÉ BITCOIN WIKI. *Bitcoin* [online]. B.m.: Přispěvatelé Bitcoin Wiki, nedatováno. Dostupné z: https://en.bitcoin.it/wiki/Bitcoin

[8] PŘISPĚVATELÉ BITCOIN WIKI. *Bitcoin FAQ* [online]. B.m.: Přispěvatelé Bitcoin Wiki, nedatováno. Dostupné z: https://en.bitcoin.it/wiki/Help:FAQ

[9] PŘISPĚVATELÉ WIKIPEDIE. *Kryptoměna* [online]. 2023. Dostupné z: https://cs.wikipedia.org/wiki/Kryptoměna

[10] STROUKAL, Dominik a Jan SKALICKÝ. *Bitcoin: peníze budoucnosti : historie a ekonomie kryptoměn, stručná příručka pro úplné začátečníky*. Praha: Ludwig von Mises Institut CZ & SK, 2015. ISBN 978-80-87733-26-4.

[11] OPLUŠTILOVÁ, Lenka. *Informace k daňovému posouzení transakcí s kryptoměnami (např. bitcoin)* [online]. B.m.: Generální finanční ředitelství. 30. březen 2022. Dostupné z: https://www.financnisprava.cz/assets/cs/prilohy/d-seznam-dani/Info_kryptomeny_GFR.pdf

[12] CHEZ, Brandon. CoinMarketCap.com. *CoinMarketCap* [online]. Dostupné z: https://coinmarketcap.com/cs/

[13] ŠEVČÍK, Jan. Historie, současnost a budoucnost kryptoměn. *forbino.com* [online]. Dostupné z: https://forbino.com/kryptomeny/historie-soucasnost-a-budoucnost-kryptomen/

[14] NAKAMOTO, SATOSHI. *Bitcoin: A peer-to-peer electronic cash system* [online]. 21260. B.m.: Decentralized business review. 2008. Dostupné z: https://bitcoin.org/bitcoin.pdf

[15] RADA EVROPSKÉ UNIE. *Digitální finance: Rada přijala nová pravidla pro trhy kryptoaktiv (MiCA)* [online]. B.m.: Rada EU. 2023. Dostupné z: https://www.consilium.europa.eu/cs/press/press-releases/2023/05/16/digital-finance-council-adopts-new-rules-on-markets-in-crypto-assets-mica/

[16] COHEN, Bram. Introduction to Chia. *Chia network, Inc.* [online]. Dostupné z: https://docs.chia.net/introduction

[17] ESET SOFTWARE SPOL. S R. O. Slovník pojmů: Cryptojacking. *ESET software spol. s r.o.* [online]. Dostupné z: https://www.eset.com/cz/cryptojacking-nelegalni-tezba-kryptomen/

[18] BINANCE ACADEMY. Co je to 51% útok? *Binance Academy* [online]. Dostupné z: https://academy.binance.com/cs/articles/what-is-a-51-percent-attack

[19] PIKA, Tomáš. Podvedení přicházejí zhruba o 1,5 miliardy ročně. Šejdíři lákají na investice do kryptoměn. *iROZHLAS.CZ* [online]. 2022. Dostupné z: https://www.irozhlas.cz/zpravy-domov/kryptomeny-podvody-investice-varovani-policie-vysetrovani-ceska-bankovni_2206100500_pik

[20] DE VRIES, Alex. Bitcoin's Growing Energy Problem. *Joule* [online]. 2018, **2**(5), 801–805. ISSN 25424351. Dostupné z: doi:10.1016/j.joule.2018.04.016

[21] STOLL, Christian, Lena KLAASSEN a Ulrich GALLERSDÖRFER. The Carbon Footprint of Bitcoin. *Joule* [online]. 2019, **3**(7), 1647–1661. ISSN 25424351. Dostupné z: doi:10.1016/j.joule.2019.05.012

[22] CAMBRIDGE CENTRE FOR ALTERNATIVE FINANCE. Cambridge Bitcoin Electricity Consumption Index. *University of Cambridge - Judge Business School* [online]. Dostupné z: https://ccaf.io/cbnsi/cbeci

[23] ČESKÁ NÁRODNÍ BANKA. Kurzy devizového trhu. *Česká národní banka* [online]. Dostupné z: https://www.cnb.cz/cs/financni-trhy/devizovy-trh/kurzy-devizoveho-trhu/kurzy-devizoveho-trhu/

[24] KURZY.CZ. Ethereum - ETH/ kurz. *Kurzy.cz* [online]. Dostupné z: https://www.kurzy.cz/kryptomeny/ethereum/

[25] KURZY.CZ. *Chia Network - XCH/ kurz* [online]. Dostupné z: https://www.kurzy.cz/kryptomeny/chia-network/

Seznam příloh