

**EKONOMICKÁ UNIVERZITA V BRATISLAVE
NÁRODOHOSPODÁRSKA FAKULTA**

Evidenčné číslo: 101007/B/2022/ 36122163602994948

**TECHNOLÓGIA BLOCKCHAIN A
ŤAŽBA KRYPTOMIEN**
Bakalárska práca

EKONOMICKÁ UNIVERZITA V BRATISLAVE NÁRODOHOSPODÁRSKA FAKULTA

Evidenčné číslo: 101007/B/2022/36122163602994948

TECHNOLÓGIA BLOCKCHAIN A ŤAŽBA KRYPTOMIEN Bakalárska práca

Študijný program: Financie, bankovníctvo a investovanie

Študijný odbor: Ekonómia a manažment

Školiace pracovisko: Katedra bankovníctva a medzinárodných financií

Vedúca záverečnej práce: doc. Ing. J. Kotlebová, PhD.

Pod'akovanie

Moje pod'akovanie patrí doc. Ing. Jane Kotlebovej, PhD. za jej rady, pripomienky a odbornú pomoc, ktoré mi poskytla pri spracovaní bakalárskej práce.

ABSTRAKT

KLEIN, Jakub: *Technológia blockchain a ťažba kryptomien*. – Ekonomická univerzita v Bratislave. Národohospodárska fakulta, Katedra bankovníctva a medzinárodných financií. – Vedúca záverečnej práce: doc. Ing. J. Kotlebová, PhD. – Bratislava: NHF, 2022, 41 strán

Záverečná práca je vypracovaná na tému Technológia blockchain a ťažba kryptomien. Cieľom záverečnej práce bolo vymedziť silné a slabé stránky technológie blockchain ako aj výhody a nevýhody ťažby kryptomien v dnešnom medzinárodnom finančnom prostredí. Jednotlivé časti záverečnej práce boli zamerané na vymedzenie a objasnenie fungovania technológie blockchain, charakteristiku transakcií a vymedzenie silných a slabých stránok technológie blockchain. Charakterizovanie a definovanie ťažby kryptomien, výhody, nevýhody a problémy spojené s ťažbou a jej praktická aplikácia na medzinárodnom finančnom trhu.

Kľúčové slová: kryptoaktívum, blockchain, technológia, kryptomeny, bitcoin, ťažba bitcoinu, výhody a riziká

ABSTRACT

KLEIN, Jakub: *Blockchain technology and cryptocurrency mining*. – The University of Economics in Bratislava. Faculty of National Economy, Departure of Banking and International Finance. – Supervisor of thesis: doc. Ing. J. Kotlebová, PhD. – Bratislava: NHF, 2022, 41 pages

The thesis of the work is blockchain technology and cryptocurrency mining. The aim of the thesis was to define the strengths and weaknesses of blockchain technology as well as the advantages and disadvantages of cryptocurrency mining in today's international financial environment. The different parts of the thesis were focused on defining and clarifying functionality of blockchain technology, characterizing transactions and defining strengths and weaknesses of blockchain technology. Characterizing and defining cryptocurrency mining, benefits, risks and problems associated with mining and its practical application on the international financial market.

Key words: crypto asset, blockchain, technology, cryptocurrency, bitcoin, bitcoin mining, benefits and risks

Obsah

Úvod.....	8
1. Súčasný stav riešenia problematiky doma a v zahraničí.....	9
1.1. Vznik trhu s kryptoaktívami	9
1.1.1. Ethereum (ETH)	14
1.1.2. XRP.....	15
1.1.3. Paris Saint-Germain Fan token (PSG).....	15
1.2. Kryptografia v blockchain-e	16
1.3. Blockchain	20
1.4. Ťažba kryptomien	21
1.5. Empirický výskum.....	24
2. Cieľ, metodika a metódy práce	27
3. Výsledky práce a diskusia.....	28
3.1. Faktory vplývajúce na efektivitu ťažby bitcoinu	28
3.2. Rozhodnutie investora medzi obchodovaním a ťažbou bitcoinu.....	37
Záver	39
Zoznam použitej literatúry.....	40

Úvod

V modernej dobe 21. storočia investori hľadajú na finančnom trhu stále nové investičné príležitosti. Nie je za tým len primárny cieľ zisku, mnohí majú záujem investovať do firiem alebo projektov s perspektívou do budúcnosti a s pridanou hodnotou pre spoločnosť. Stále ešte len rozvíjajúci sa trh s kryptoaktívami ponúka takéto možnosti investovať do firiem alebo projektov, ktoré sa zaoberajú rôznymi svetovými problémami a ich riešeniami. Cieľom práce je vymedziť silné a slabé stránky fungovania technológie blockchain a preskúmať výhody, nevýhody a riziká spojené s ťažbou kryptomien v medzinárodnom finančnom prostredí. Kryptoaktíva môžeme charakterizovať ako rizikové digitálne aktíva, ktoré však môžu výborne dopĺňať investičné portfólio. Investície do kryptoaktív však nemusia vždy byť také rizikové ako sa na prvý pohľad zdá. Investícia do ťažby kryptomien je jedna z možností ako minimalizovať riziká straty finančných prostriedkov a zároveň investovať do rozvoja trhu s kryptoaktívami. Preto budeme skúmať a popisovať oblasť trhu kryptoaktív a chceme objasniť problematiku spojenú s ťažbou bitcoinu.

Prvá kapitola bude charakterizovať trh s kryptoaktívami a dôvody jeho vzniku, vznik bitcoinu, bude popisovať fungovanie transakcií a charakterizovať rôzne typy kryptoaktív.

V ďalších častiach popisujeme sieť blockchain a charakterizujeme vnútorné princípy a podmienky jej fungovania, vymedzíme dôležitosť ťažby pre fungovanie siete blockchain a prinesieme prehľad empirického výskumu v danej oblasti.

Druhá kapitola bližšie charakterizuje hlavný cieľ práce, pracovné postupy a spôsoby získavania a spracovania údajov.

Budeme porovnávať investovanie do ťažby bitcoinu a obchodovanie s bitcoinom, porovnáme ťažiarne zariadenia, objasníme proces prípravy na ťažbu bitcoinu a vymedzíme faktory, ktoré môžu ovplyvniť efektivitu ťažby v praxi. V ďalšej časti porovnáme spotrebu a produkciu elektrickej energie vo vybraných štátoch, využitie rôznych typov energií pri ťažbe bitcoinu a urobíme prehľad zastúpenia jednotlivých štátov v ťažbe bitcoinu. V závere tejto časti porovnáme rentabilitu ťažby bitcoinu v rôznych podmienkach a popíšeme rozhodovanie investora medzi ťažením bitcoinu a jeho obchodovaním.

1. Súčasný stav riešenia problematiky doma a v zahraničí

Mnohí tvrdia, že kryptomeny budú hlavným finančným aktívom v budúcnosti. V dnešnej dobe existuje veľa jednotlivcov, ktorí poznajú kryptomeny, využívajú ich ako investičné aktívum, alebo s nimi obchodujú. Stále však existuje značný počet ľudí, ktorí nevedia čo to je, a ako z nich môžu ťažiť.

Okrem súkromného sektora, vládnych agentúr, finančných inštitúcií a niektorých spoločností len málo ľudí dobre vie, čo to je. V dnešnej dobe väčšina týchto agentúr skutočne investovala a naďalej vynakladá investície do výskumu kryptomien. To len ukazuje, aké dôležité sú tieto virtuálne peniaze v našej modernej spoločnosti.

Kryptomena je séria digitálnych peňazí, ktoré možno použiť na platenie či iné online transakcie. Názov „kryptomena“ vznikol kombináciou slov „kryptografia“ a „mena“. Rovnako ako tradičné finančné nástroje, aj kryptomeny môžu byť držané ako investičné aktívum alebo obchodované za účelom zisku. Atraktivitu kryptomien pre investorov vyvoláva najmä skutočnosť, že nepodliehajú regulácií úradov, bánk alebo iných vládnych subjektov. Fakt, že kryptomeny nie sú regulované zapríčiňuje to, že investície do nich sú častokrát veľmi rizikové. Kryptomeny v skutočnosti nie sú samy o sebe virtuálne peniaze, ale ide skôr o sústavu riadkov kódu v databáze. Zmena riadkov kódu nie je jednoduchá, pretože existujú podmienky, ktoré je potrebné splniť pred udelením prístupu na úpravy.

Rovnaký koncept platí aj pre tradičnú menu, papierové peniaze či mince. V tomto prípade je databázou váš bankový účet a peniaze uložené vo vnútri tvoria záznamy.

1.1. Vznik trhu s kryptoaktívami

Kryptomeny vznikli preto, že ľudia hľadali porovnateľný produkt ku digitálnym aktívam na uskutočňovanie bezhotovostných operácií. Bitcoin bola prvá vytvorená kryptomena, ktorú v roku 2009 vytvoril a založil Satoshi Nakamoto. Objem bitcoinov na trhu sa neustále zvyšuje vzhľadom na to, že odmena pre ťažiarov je aktuálne 6,25 bitcoinu za vytiažený blok. Všetky existujúce bitcoiny boli vytvorené rovnakou formou. Bitcoinový protokol určuje, že odmena pre ťažiarov sa každých 210 000 vytiažených blokov zníži o polovicu. Tento protokol zabraňuje vzniku inflácie na bitcoine. Maximálny celkový počet tokenov, ktorý v budúcnosti bude v obehu bol vopred stanovený na 21 miliónov bitcoinov. Predpokladá sa, že tento objem by sme mali dosiahnuť v roku 2140¹.

¹STROUKAL, Dominik – SKALICKÝ, Jan. *BITCOIN Peníze budoucnosti*. Praha: Ludwig von Mises Institut CZ&SK, 2015. s. 35. ISBN 978-80-87733-26-4.

Satoshi bol autor dokumentu o bitcoine, ktorý sa stal známy v roku 2008. Bol aktívny na fórach, kde rovnako zmýšľajúci ľudia diskutovali o spôsoboch ako získať späť svoje súkromie v elektronickej dobe. Po zverejnení pôvodného dokumentu sa Satoshi naďalej zúčastňoval na fórach o bitcoinoch až do roku 2013. Krátko na to zmizol.

Satoshi Nakamoto vlastní, resp. kontroluje značný počet bitcoinov, ktoré v roku 2013 odhadol konzultant pre bezpečnosť kryptomien Sergio Lerner na približne 1 milión bitcoinov. To predstavuje necelých 5% z celkového počtu 21 miliónov bitcoinov, ktoré budú v budúcnosti vytvorené, ak sa pravidlá protokolu nezmenia.

Na identite Satoshiho Nakamota v skutočnosti nezáleží, pretože ak by sa odhalila skutočná identita tejto osoby alebo skupiny ľudí, ich názory a správanie by mohli ovplyvniť bitcoin a aj samotnú spoločnosť. Tejto centralizácií sa však Satoshi snaží vyhnúť.

Bolo zverejnených niekoľko článkov v rôznych časopisoch ukazujúcich na reálnych ľuďoch, ktorí by potenciálne mohli byť Satoshi, no realita je taká, že Satoshi Nakamoto zostáva stále iba ako pseudonym.²

Predtým, ako vznikol koncept kryptomien bola elektronická hotovosť prístupná len prostredníctvom depozitov z debetných kariet alebo depozitov z bankových účtov na online platobné platformy. Problémom digitálnej hotovosti však bolo, že nebola navrhnutá dostatočne dobre na to, aby zabraňovala problému dvojitého míňania.

Dr. Julian Hosp definuje: „*Dvojité míňanie znamená, že niečo možno minúť dvakrát, a do roku 2008 sa za jediné jeho riešenie považovala prítomnosť centrálnej inštitúcie.*“³

Problém dvojitého míňania sa dá veľmi dobre pochopiť na príklade obrázku v telefóne. Keď nahrám kópiu tohoto obrázka na sociálne siete (Facebook, Instagram, Twitter a pod.), tak v podstate vytvorím len jeho kópiu bez toho, aby ma to niečo stálo. To znamená, že som svoj obrázok použil niekoľkokrát. Nemalo to na nikoho negatívny vplyv, takže to nikto nekontroloval a nikoho nezaujímal, či svoj obrázok použijem päťkrát alebo stokrát.

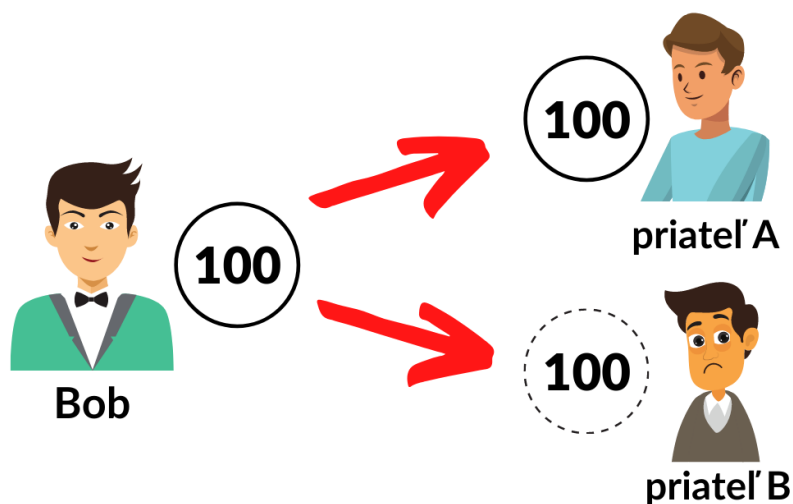
Predstavme si, že existuje digitálna mena Jakub-coin. Povedzme, že Bob vlastní sto Jakub-coinov a chce ich poslať priateľovi A. Následne urobí to isté čo s obrázkom, skopíruje sto Jakub-coinov a pošle ich inému priateľovi. Urobil presne to isté čo s obrázkom, pričom vtedy to nikoho nezaujímal. V tomto prípade to však bude spoločnosť zaujímať, pretože peniaze sú formou hodnoty a dôvery. Za bežných okolností dvojitému míňaniu zabraňuje banka alebo iná dozerajúca inštitúcia. Ak však chceme mať decentralizované riešenie,

²LEWIS, Anthony. *The Basics of Bitcoins and Blockchains*. Mango Media, 2018. ISBN 978-1-63353-800-9.

³HOSP, Julian. *Krypto Meny*. Bratislava: TATRAN, 2018. s. 38. ISBN 978-80-222-0945-8.

musíme nájsť spôsob ako sa dvojitému míňaniu vyhnúť aj bez dozerania kontrolného orgánu. Problematiku dvojitého míňania popísal J. Hosp.⁴

Obrázok č. 1 Dvojité míňanie



Zdroj: vlastné spracovanie na základe Hosp, J. (2018)

Riešenie na problém dvojitého míňania bolo predstavené v roku 2008. Toto riešenie v podobe bitcoinu nevyžadovalo centralizovanú sieť serverov, regulácie ani iné oprávnenia.

A. Heston uvádza: „*Táto kryptomena sa spoliehala na sieť P2P ako prostriedok na zabezpečenie jednoduchého míňania. Musíme poznamenať, že predošlé pokusy o podobné riešenie zlyhali, preto bol vynález bitcoinu skutočne revolučný.*“⁵

Okrem problému s dvojitým míňaním možno identifikovať aj ďalší problém, ktorý podnietil vznik kryptomien. Zlyhanie niekoľkých platobných kanálov tretích strán, ktoré mali poskytnúť bezpečný systém, pomocou ktorého by ľudia mohli platiť za veci online.

Ako odpoveď na zlyhanie platobných kanálov, ktoré sú vysoko regulované a majú centralizovaný charakter bol bitcoin vytvorený tak, aby nebol závislý od akéhokoľvek centrálného regulačného systému a aby namiesto toho pracoval na princípe dôveryhodnosti P2P siete. Výhoda kryptomien je v tom, že neexistuje žiadny serverový systém, ktorý by si vyžadoval starostlivosť, pretože pracuje s decentralizovanou sieťou. Vďaka fungujúcej sieti P2P má každý aktualizovaný zoznam transakcií ktoré sleduje, monitoruje a kontroluje, či nedochádza k problémom.

⁴HOSP, Julian. *Krypto Meny*. Bratislava: TATRAN, 2018. ISBN 978-80-222-0945-8.

⁵HESTON, Anthony. *Cryptocurrencies: How to safely create stable and long-term passive income by investing in Cryptocurrencies*. CreateSpace Independent Publishing Platform, 2017. s. 9. ISBN 1975623703.

Transakcie prebiehajú medzi jednotlivcami, a preto existuje osobný záujem na správnosti zápisu každej transakcie v uchovávaných záznamoch. Práve tento systém umožňuje elimináciu problémov ako dvojité míňanie. Vo väčšine prípadov môžeme očakávať, že všetci účastníci dosiahnu absolútny konsenzus o legitimitě obchodov. Vznik kryptomien a trhu s nimi popísal A. Heston.⁶

Bitcoin je označovaný ako digitálna mena, virtuálna mena alebo kryptomena, ale môžeme ho považovať aj za elektronické aktívum. Keď sa ľudia snažia porozumieť bitcoinu, často ich nadchne slovo mena. Snažia sa porozumieť aspektom konvenčných mien, ktoré sa však bitcoinu netýkajú, napríklad čím je krytý, alebo kto udáva úrokové miery. Pojem bitcoin je tiež niekedy popisovaný ako digitálny token, ale to nie je úplne jednoznačná definícia.

Bitcoiny sú digitálne aktíva, ktorých celkový počet je 21 milióna a v obehu je vyše 18,77 milióna bitcoinov (júl 2021). Ich vlastníctvo je zaznamenané v elektronickej účtovnej knihe, ktorá je takmer neustále aktualizovaná tisíckami nezávisle ovládanými počítačmi, ktoré sú prepojené rovnakým softvérom, vďaka ktorému sa dokážu vzájomne spájať a komunikovať. Tieto počítače sú rozmiestnené po celom svete, takže sú decentralizované. Tento systém sa nazýva bitcoinový blockchain.

Transakcie, ktoré zaznamenávajú prevod vlastníctva týchto virtuálnych peňazí sa vytvoria a overia podľa protokolu – zoznamu pravidiel, ktorý definuje ako prevody fungujú a ako sa následne zapisujú a aktualizujú do účtovnej knihy. Protokol je implementovaný softvérom – aplikáciou, ktorú účastníci používajú na svojich počítačoch. Stroje, na ktorých sú aplikácie spustené sa nazývajú „uzly“ siete. Každý uzol nezávisle overuje všetky čakajúce transakcie bez ohľadu na to kde vzniknú a následne aktualizuje svoj vlastný záznam o knihe pomocou overených blokov potvrdených transakcií. Centrá s výpočtovou technikou sú budovy, kde sa nachádza množstvo grafických kariet, ktoré zabezpečujú výpočtový výkon. Nazývame ich ťažiarne centrá, ktoré spájajú platné transakcie do blokov a distribuujú ich do uzlov v blockchain sieti.

Ktokoľvek na svete môže bitcoiny nakupovať, vlastniť ich a posilať ich iným ľuďom. Každá bitcoinová transakcia je zaznamenaná a verejne zdieľaná v bitcoinovom blockchaine. Bitcoinový blockchain nie je šifrovaný, takže každý môže vidieť všetky detaily všetkých transakcií. Teoreticky si každý dokáže „vytvoriť“ svoje bitcoiny v rámci procesu vytvárania a overovania blokov. Tento proces vytvárania blokov sa nazýva „ťažba“ bitcoinu.

⁶HESTON, Anthony. *Cryptocurrencies: How to safely create stable and long-term passive income by investing in Cryptocurrencies*. CreateSpace Independent Publishing Platform, 2017. ISBN 1975623703.

Transakcie spojené s kryptomenami možno opísať v niekoľkých krokoch:

1. Na uskutočnenie transakcie je potrebné pripojenie peňaženky na burzu. Môže ísť o nákup, predaj, odoslanie alebo príjem kryptomeny.
2. Po zadaní transakcie je požiadavka odoslaná do P2P siete. Namiesto serverov sa využívajú počítačové systémy, ktoré označujeme ako uzly.
3. Použitím algoritmov počítače v sieti overia transakciu a identitu žiadateľa.
4. Transakcia sa overí a následne je prijatá alebo zamietnutá.
5. Overené a schválené žiadosti sú následne zapísané do digitálnej databázy blockchain.
6. Nová transakcia je pridaná k už existujúcemu radu uložených riadkov kódu, ktoré nemožno meniť ani vymazať.
7. Transakcia sa následne označí ako dokončená.

Aj keď sa transakcie s kryptomenami zdajú byť zložité, dokončenie týchto procesov v skutočnosti trvá veľmi krátky čas v podobe minúty alebo dvoch. Práve vďaka rýchlosti transakcií sú obchody s kryptomenami považované za vysoko efektívne a pohodlné v porovnaní s inými formami mien.

Transakcie s kryptomenami nepodliehajú žiadnym regulačným procesom tretích strán, ktoré by sa vzťahovali na ich nákup, predaj, odosielanie alebo prijímanie. Treba však podotknúť, že aj napriek tomu majú všetky transakcie, ktoré sú uskutočnené určité vlastnosti, ktoré musia byť splnené. Fungovanie kryptotransakcií popísal A. Lewis.⁷

Hlavné vlastnosti, ktoré spĺňajú všetky transakcie s kryptomenami:

1. Transakcie sú anonymné

Okrem toho, že samotné transakcie sú anonymné, tak aj účty medzi ktorými transakcia prebieha sú anonymné. Je to možné vďaka tomu, že transakcia je zašifrovaná pod kódom - „hashom“ a účty sú taktiež zapísané ako kód zložený z číslíc a písmen.

2. Transakcie sú nevratné

To znamená, že akonáhle je platba odoslaná, alebo sú digitálne peniaze prevedené na iný účet, už ich nie je možné vrátiť späť na pôvodný účet. Pri procese potvrdzovania transakcií,

⁷LEWIS, Anthony. *The Basics of Bitcoins and Blockchains*. Mango Media, 2018. ISBN 978-1-63353-800-9.

ktorý prebieha veľmi rýchlo, neexistuje žiadna záchranná sieť, ktorá by mohla asistovať. To je dôvod prečo treba vždy postupovať veľmi opatrne a obozretne.

3. Transakcie sú bezpečné

Aj keď sú nevratné, tak všetky transakcie sú bezpečné, pretože kryptomeny využívajú na ochranu kryptografiu. Na prístup k účtu je potrebný špeciálny kľúč. Pokiaľ existuje tento kľúč, nie je nutné sa obávať o finančné prostriedky uložené na účte.

4. Transakcie sú vysoko prístupné

Ak je záujem realizovať transakcie spojené s kryptomenami, nie je nutné žiadať o povolenie. Stačí stiahnuť potrebný softvér alebo založiť online účet a tým je získaný priamy prístup k digitálnym finančným nástrojom.

5. Systém transakcií prebieha globálne

Transakcie v kryptomene sa uskutočňujú prostredníctvom počítačových systémov a sietí P2P. To znamená, že transakcie je možné ľahko vykonávať na medzinárodných trhoch z pohodlia domova alebo z kancelárie. Vlastnosti kryptotransakcií popísal vo svojej knihe A. Heston.⁸

Okrem samostatnej kryptomeny bitcoin však poznáme aj spoločnosti, ktoré na svoje financovanie vytvorili kryptoaktíva. Ich predaj v podstate nahrádza predaj akcií danej spoločnosti.

V súčasnosti existujú viac než stovky rôznych digitálnych mincí, ktoré sú voľne obchodovateľné, alebo reprezentujú akcie spoločností, pôsobiacich v oblastiach od gamingu, virtuálneho umenia a reality cez oblasti športu alebo hudby až po poisťovníctvo, turizmus a energetiku. Každá minca reprezentuje konkrétnu spoločnosť s konkrétnym podnikateľským zámerom. Spoločnosti často využívajú formu digitálnych aktív s cieľom vyzbierať kapitál pre expandovanie, rozšírenie výroby alebo začatie nového projektu. Tieto digitálne aktíva spája fakt, že všetky fungujú na základe technológie blockchain.

1.1.1. Ethereum (ETH)

Ethereum je platforma založená na decentralizovanej báze, využívajúca blockchain. Kryptoaktívum, ktoré využíva na financovanie a rozvoj sa volá ether a má skratku ETH.

Prioritným cieľom zakladateľa nebolo vytvoriť menu ako takú, ale vytvoriť zdieľanú výpočtovú platformu, ktorá by umožňovala využiť technológiu blockchain na prevádzku

⁸HESTON, Anthony. *Cryptocurrencies: How to safely create stable and long-term passive income by investing in Cryptocurrencies*. CreateSpace Independent Publishing Platform, 2017. ISBN 1975623703.

decentralizovaných aplikácií. Vďaka vnútornej hodnote, ktorú ether drží, sú tieto aplikácie využívané na prenos hodnoty etheru od užívateľa k ďalšiemu užívateľovi.

Hlavná výhoda etheru je využitie inteligentných (smart) kontraktov a ich rozšírenie do praxe pre širokú verejnosť. Myšlienka "smart kontraktov" zaujala používateľov, vývojárov a spoločnosti na celom svete, vďaka čomu ethereum získalo veľkú pozornosť. Mohli by sme tak nahradiť a svojím spôsobom decentralizovať rôzne vzťahy, zmluvy alebo dohody.

V súčasnosti sa sieť ethereum využíva pri obchodovaní s NFT (not-fungible token) – nezameniteľnými tokenmi, ktoré v podstate prenášajú umenie do virtuálneho sveta. Fungovanie smart kontraktov je pre chod celej siete úplne zásadné a práve tým sa ether výrazne odlišuje od bitcoinu. Ether patrí svojim charakterom do kryptomien novej, druhej generácie, ktoré bývajú často označované aj ako Bitcoin 2.0. Trhová kapitalizácia etheru je viac ako 365 miliárd dolárov (2022).⁹

1.1.2. XRP

XRP je označenie pre decentralizovanú mincu, ktorá sa využíva primárne pre medzištátne prevody z a do fiat mien, ale je aj voľne obchodovateľná na burze. XRP bol navrhnutý a naprogramovaný v roku 2012 spoločnosťou Ripple tak, aby rýchlosť transakcií neprekračovala pár sekúnd a aby jeho transakcie boli energeticky a cenovo výhodné.

Myšlienkou nebolo vytvorenie coinu na voľné obchodovanie, ale vytvorenie systému pre P2P infraštruktúru na presun finančných prostriedkov bez potreby zúčtovacieho centra alebo iného orgánu vo veľmi rýchlom čase s vysokou efektivitou. Tým, že táto platforma overuje transakcie decentralizovaným konsenzom členov v XRP sieti sa odlišuje od ostatných platforiem, ktoré pracujú s overovaním transakcií pomocou ťažby.

Vďaka týmto vlastnostiam začali so spoločnosťou Ripple spolupracovať viaceré svetové banky, ktoré hľadajú spôsob ako využiť jeho potenciál a uplatnenie v praxi. Momentálna trhová kapitalizácia je viac ako 34 miliárd dolárov (2022).¹⁰

1.1.3. Paris Saint-Germain Fan token (PSG)

Športový klub Paris Saint-Germain vytvoril vlastné krypto aktívum, v podobe fanúšikovskej mince, ktorú možno získať nákupom na burze. Vedenie týmto krokom

⁹CoinMarketCap. Trhová kapitalizácia etheru. [2022-04-08]. Dostupné na: <https://coinmarketcap.com/sk/currencies/ethereum/>

¹⁰CoinMarketCap. Trhová kapitalizácia XRP. [2022-04-08]. Dostupné na: <https://coinmarketcap.com/sk/currencies/xrp/>

vyzberalo kapitál potrebný na ďalšie rozširovanie klubu, využilo digitálne aktívum na marketingovú stratégiu a poskytlo fanúšikom možnosť podieľať sa na vlastníctve ich obľúbeného klubu. Do obehu dali 20 miliónov tokenov, pričom momentálna trhovú kapitalizácia mierne presahuje 42 miliónov dolárov.¹¹

1.2. Kryptografia v blockchain-e

Na to, aby sme skutočne porozumeli fungovaniu bitcoinu a kryptoaktív v sieti blockchain, musíme podrobnejšie rozobrať oblasť kryptografie, ktorá sa výraznou mierou stará o funkčnosť týchto digitálnych mien. „*Blockchainy nie sú vo všeobecnosti šifrované, ale chápanie šifrovania poskytuje dobré základy pre kryptografiu, ktorá sa v blockchainoch vo veľkej miere používa.*“¹² Kryptografia je okrem iného o odosielaní tajných správ, ktoré môže čítať iba zamýšľaný príjemca. Pracuje s pojmi ako šifrovanie a dešifrovanie (kódovanie a dekódovanie správ), hashovanie (premena údajov na šifrované kódy) a digitálne podpisy (dôkazy o tom, že sa správa vytvorila a schválila).

Kryptografia sa vo veľkej miere používa na ochranu údajov, ktoré zdieľame cez internet. „S“ v skratke „https“ znamená bezpečné (secure).

To znamená, že sa používa kryptografia, aby sa zaručilo, že webová stránka, o ktorej si myslíte že ju navštevujete, je v skutočnosti skutočnou overenou webovou stránkou. Znamená to tiež, že posielené údaje medzi vami a touto webovou stránkou sú šifrované, takže hackeri nedokážu ľahko prečítať komunikáciu medzi vašim zariadením a webovou stránkou, na ktorú prístupujete.

Kryptografia sa používa na oveľa viac účelov, ako je len šifrovanie a dešifrovanie správ. Šifrovanie je najznámejším využitím kryptografie v praxi. Blockchainy nie sú spravidla šifrované, ale porozumenie šifrovaniu poskytuje dobré zázemie pre kryptografiu, ktorá je v blockchainoch veľmi využívaná.

Šifrovanie je proces premeny obyčajnej (čitateľnej) ľudskej správy na šifrovaný text (mix znakov). Takže ak je zachytená šifrovaná správa, hacker jej nemôže porozumieť. Dešifrovanie je proces, ktorý premieňa šifrovaný text späť na čitateľný, obyčajný text. „Prelomenie“ šifrovaného textu znamená zistiť, ako dešifrovať šifrovaný text bez zadania „kľúča“.

¹¹CoinMarketCap. Trhová kapitalizácia XRP. [2022-04-09]. Dostupné na: <https://coinmarketcap.com/sk/currencies/paris-saint-germain-fan-token/>

¹²LEWIS, Anthony. *The Basics of Bitcoins and Blockchains*. Mango Media, 2018. s. 155. ISBN 978-1-63353-800-9.

Máme dve osoby, Alica a Bob. Povedzme, že Alica chce Bobovi poslať správu, aby si ju mohol prečítať iba Bob. Alica a Bob sa najprv dohodnú na schéme. Použijeme veľmi jednoduchú schému, kde zašifrujeme text posunutím každého písmena o určitý počet miest ďalej v abecede. Obaja súhlasia s tým, že ako kľúč budú používať „+1“, čo znamená, že každé písmeno sa v abecede posunie o jedno miesto ďalej. Takže A sa stane B, B sa stane C, C sa stane D a tak ďalej. Táto schéma sa nazýva Caesarova šifra.

Obrázok č. 2 Príklad šifrovania



Zdroj: vlastné spracovanie na základe Lewis A. (2018)

1. Alica napíše textovú správu „Stretnime sa Bob“.
2. Alica zašifruje správu posunutím každého písmena o jedno ďalej: „Tusfuojnf tb Cpc“.
3. Alica pošle Bobovi šifrovaný text.
4. Bob dešifruje text posunutím každého písmena o jedno dozadu a následne dostane obyčajný text: „Stretnime sa Bob“.

Tento typ šifrovania patrí medzi symetrické šifrovania, pretože ten istý „kľúč“ (+1 v tomto prípade) sa používa vo fáze šifrovania aj vo fáze dešifrovania. Tento spôsob sa v dnešnej dobe už nevyužíva, pretože je príliš jednoduchý a aj preto, lebo Bob a Alica sa najskôr museli stretnúť, aby sa dohodli, aký kľúč v schéme použijú.

Vo svete, kde zariadenia neustále nadväzujú spojenie s novými webovými stránkami je akékoľvek stretnutie a dohodnutie, pri ktorom sa dohodne a zdieľa symetrický kľúč medzi zariadením a webovou stránkou slabé miesto a každý odpočúvajúci, ktorý sleduje túto počiatočnú výmenu, môže dešifrovať tajné správy pre zvyšok konverzácie. Práve preto bola vynájdená asymetrická kryptografia, oveľa bežnejšie používaná forma šifrovania.

V skutočnosti šifrovanie pre blockchain nie je veľmi relevantné. Mnoho ľudí hovorí o šifrovaných blockchainoch, ale zamieňajú si šifrované údaje, ktoré sa nepoužívajú v blockchainoch s kryptografiou, ktorá je v blockchainoch vysoko využívaná na hashovanie a digitálne podpisy. V základe nič v bitcoinovej sieti nie je šifrované. Ide o to, že údaje o transakciách vo forme obyčajného textu sa replikujú v sieti, aby ich mohol ktokoľvek prečítať a overiť.

V bitcoinovej sieti sa využívajú iné kryptografické schémy, ako sú schémy verejných kľúčov alebo kryptografické hash-e. Vyššie spomenutá Caesarova šifra je známa ako symetrická šifra, pretože na šifrovanie a dešifrovanie správ sa používa rovnaký kľúč.

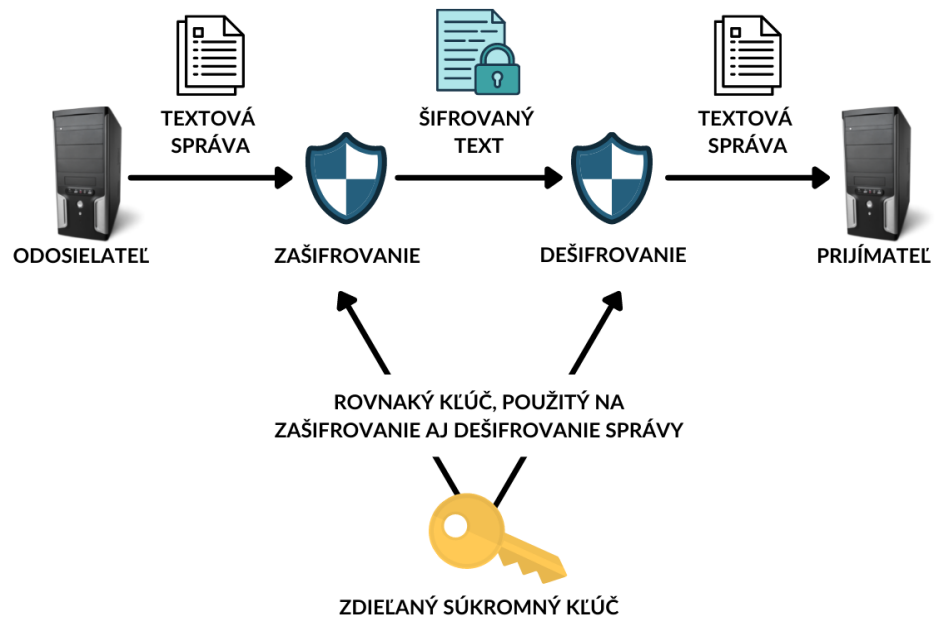
V kryptografii verejných kľúčov je kľúč použitý na dešifrovanie správy odlišný od kľúča na šifrovanie správy. Kryptografia verejného kľúča je asymetrická schéma. Vďaka tomu je oveľa bezpečnejšia.

Ak by sme chceli prijímať šifrované správy pomocou asymetrickej kryptografie, musíme si vytvoriť dva matematicky prepojené kľúče: verejný a súkromný kľúč. Spoločne tvoria kľúčový pár. Svoj verejný kľúč môžeme zdieľať so svetom a ktokoľvek ho môže použiť na šifrovanie správ na nás. Na dešifrovanie týchto správ používame náš súkromný kľúč, ktorý poznáme iba my. Každý, kto nám zašle šifrované správy pomocou nášho verejného kľúča vie, že ich môžeme dešifrovať iba my, našim súkromným kľúčom.

Ako môžeme vidieť na obrázkoch nižšie, jedným z najväčších problémov symetrickej kryptografie je spôsob, ako zdieľajú kľúč odosielateľ a prijímateľ správy. Tento systém je veľmi jednoduchý a príliš ľahko napadnuteľný. Vďaka asymetrickej kryptografii s verejným kľúčom, môžeme zdieľať verejný kľúč všetkým, bez akýchkoľvek obáv alebo problémov. Odosielateľ pošle zašifrovanú správu. Jediný, kto môže túto správu dešifrovať je samotný prijímateľ a to tak, že použije svoj súkromný kľúč, ktorý má iba on. Tento systém fungovania (asymetrická kryptografia) je vo výraznej miere využívaný v blockchaine a rovnako aj pri transakciách s kryptomenami.¹³

¹³LEWIS, Anthony. *The Basics of Bitcoins and Blockchains*. Mango Media, 2018. ISBN 978-1-63353-800-9.

Obrázok č. 3 Symetrická kryptografia



Zdroj: vlastné spracovanie na základe Lewis, A. (2018)

Obrázok č. 4 Asymetrická kryptografia



Zdroj: vlastné spracovanie na základe Lewis, A. (2018)

1.3. Blockchain

Dr. J. Hosp definuje blockchain takto: „*Blockchain je kompletná a nemenná história všetkých transakcií decentralizovanej komunity, s ktorou súhlasí každý, kto je súčasťou tejto komunity.*“¹⁴ História transakcií je pravidelne aktualizovaná. Každý účastník ju akceptuje a ukladá si ju do svojho počítača a tým zabezpečuje, aby nedošlo k dvojitému míňaniu v rozpore s blockchain protokolom.

Technológia blockchain je základom pre existenciu decentralizovaných digitálnych mien. Je to však len jedno z mnohých využití blockchainu. V praxi túto technológiu môžeme využiť pri riešení otázok vlastníctva, komunikácie, identifikácie atď., kde je existencia tretej centrálnej strany nežiadúca. To je jedna z jeho silných stránok. Ďalšími sú decentralizovaná sieť, transparentnosť, dôveryhodnosť a nemenná technológia. V teórii si blockchain môžeme predstaviť ako puzzle, ktoré do seba zapadajú a nadväzujú na seba ďalšie dieliky, alebo ako sieť blokov pospájaných do reťazcov.

Skutočnosť je však taká, že blockchain tvorí len samotná kryptografia, čiže nič iné ako písmená a číslice. Súkromný kľúč definujeme ako postupnosť písmen a číslic. Tento súkromný kľúč podpisuje inú postupnosť zloženú z nových písmen a číslic.

Výsledkom tohto podpisu je Tx-ID – úplne nová, jedinečná postupnosť písmen a číslic. Toto zodpovedá dieliku puzzle. Ťažiar tieto Tx-ID príjmu a overia ich s verejnou adresou, z ktorej boli informácie odoslané. Toto všetko je kryptografia, zložená z písmen a číslic. Potom sa ťažiar snažia nájsť blok, pokúšajú sa hashovať hash, postupnosť znakov starého bloku so všetkými Tx-ID aktuálneho bloku a nájsť Merkleov strom (Merkles root) s určitým počtom núl. Zodpovedá to skladaniu puzzle a vytváraniu obrazca, pričom sa kontroluje náročnosť ťažby. Úpravou postupnosti znakov vznikne vždy nový hash, čo zodpovedá ďalšej, novej postupnosti.

Blok teda môžeme charakterizovať ako postupnosť znakov, do ktorej je integrované množstvo iných postupností znakov. Ak by sme tieto prvky zmenili, výsledná postupnosť znakov by vyzerala odlišne a kryptograficky by to nesesedelo.

Ak si niekto „stiahne blockchain“, stiahne si v skutočnosti celú postupnosť písmen a číslic, ktorá zobrazuje všetky transakcie, ktoré sa v ňom uskutočnili. Ide o obrovské množstvo dát. Medzi slabé stránky blockchainu patrí vysoká energetická závislosť, náročný proces integrácie a vysoké náklady na implementáciu do praxe. Technológiu blockchainu popísal vo svojej knihe Dr. J Hosp.¹⁵

¹⁴HOSP, Julian. *Krypto Meny*. Bratislava: TATRAN, 2018. s. 38. ISBN 978-80-222-0945-8.

¹⁵HOSP, Julian. *Krypto Meny*. Bratislava: TATRAN, 2018. ISBN 978-80-222-0945-8.

1.4. Ťažba kryptomien

Na to, aby sme udržali aktívny chod krypto-siete a zároveň udržali záujem ľudí o digitálne mince, musíme hovoriť aj o ťažbe kryptomien, ktorá má rôzne podoby, akým spôsobom sa ťažba vykonáva a akým spôsobom ťažba funguje. „*Keď porovnáme ťaženie kryptomien s ťažbou zlata je jasné, prečo sa tento proces nazýva ťažba kryptomien. V oboch formách ťažby baníci vynakladajú úsilie a odmenou im je aktívum, ktoré ešte nie je v obehu.*“¹⁶

Pri klasickej ťažbe sa ťaží zlato, ktoré sa prirodzene nachádza v prírode. Novovyťažené zlato, ktoré bolo mimo obehu a stáva sa súčasťou zlata, ktoré je v trhovom obehu a je možné ho obchodovať. Pri ťažbe kryptomien sa vykonáva proces, ktorý sa končí uvoľnením nových digitálnych mincí do obehu a ich pridaním na trh. V oboch prípadoch ťažiar po získaní svojej odmeny - vyťažného zlata alebo uvoľnených mincí - zvyčajne predávajú verejnosti, aby si zabezpečili zisk. Týmto uvedú uvoľnené mince do obehu.

Poznáme rôzne podoby a spôsoby ťažby, ktoré súvisia s technológiou, na ktorej daná digitálna minca funguje. Základná a primárna je však ťažba bitcoinu, ktorej sa budeme venovať. Pri ťažbe kryptomeny bitcoin ťažiar rieši matematickú šifru, ktorú mu vygeneruje sieť, aby sa rozšifrovaním dokázalo, že sa daná transakcia uskutočnila. Vďaka spôsobu akým blockchain funguje, má každý užívateľ v sieti prístup ku kódu transakcie, vďaka ktorému môže vidieť, či účastník transakcie získal bitcoin legitímne alebo nie. Ťažba môže byť vykonávaná na každom počítači, ktorý má pripojenie na blockchain sieť. To je jedna z výhod, ktoré ťažba má. Keď by sme chceli nastaviť počítač na vykonávanie ťažby, museli by sme zvoliť hardvér vo vnútri počítača, ktorý bude ťažbu vykonávať. Dnes už ťaženie na notebookoch alebo počítačoch však nie je také efektívne.¹⁷

Blockchain sieť posudzuje aký výkonný je používateľom poskytnutý hardvér a zároveň sleduje, aký má aktuálny výpočtový výkon vo vnútri siete. Keď sieť nadobudne všeobecnú predstavu o tom, aký výkonný je poskytovaný hardvér, náhodne vyberie uzly v blockchaine a priradí matematickú šifru, ktorej rozlúštením sa overí platnosť zapísanej transakcie. Tento proces overovania transakcií je známy ako Proof of Work koncept. Hardvér, ktorý rozlúšti matematickú šifru a preukáže správnosť riešenia je následne odmenený za vykonanú prácu digitálnou mincou, ktorej transakcie overoval. Celý proces ťažby od rozšifrovania matematickej šifry až po získanie odmeny prebieha v čase, kedy sú

¹⁶KENT, Peter – BAIN, Tyler. *Cryptocurrency mining for dummies*. New Jersey: John Wiley & Sons Inc., 2019. s. 30. ISBN 978-1-119-57929-8.

¹⁷KENT, Peter – BAIN, Tyler. *Cryptocurrency mining for dummies*. New Jersey: John Wiley & Sons Inc., 2019. ISBN 978-1-119-57929-8.

overené transakcie zapisované do blockchainu. Znamená to, že rýchlosť siete je závislá výlučne od toho, aký výkonný hardvér je momentálne napojený na sieť a pripravený pracovať na overovaní transakcií.

S ťažbou kryptomien je spojených množstvo benefitov, ale nesie aj značnú mieru neistoty a rizika. Pred samotným procesom ťažby je dôležité, poznať a zanalyzovať si možné riziká a benefity. Hlavným benefitom je, že ťažiar sa stáva aktívnym “kontrolórom“ procesu overovania a tým zabezpečuje bezpečnosť blockchainu. Riešením matematických šifrier ochraňuje zakódovanú informáciu, ktorá prechádza sieťou. Celý proces napomáha budovať bezpečnosť a dôveru blockchainovej siete. Bez tejto pomoci ťažiarov by pravdepodobne krypto aktíva v súčasnosti nevzbudzovali toľko pozornosti a dôvery. Ďalší benefit ťažby je, že práca ťažiarov je odmeňovaná. Keď je práca ťažiarov hotová, sú odmenení malým množstvom digitálnych mincí, daného aktíva. Odmeňovanie uvoľňuje ďalšie digitálne mince do obehu, až pokiaľ sa celkové limitované množstvo daného krypto aktíva nenaplní. Nepochybne výhodou ťažby je minimalizácia rizika straty investovaných prostriedkov z dlhodobého hľadiska a pri vhodných podmienkach celkom rýchla návratnosť.

Napriek tomu, že ťažba mincí prináša mnoho výhod je nutné dodať, že ťažiar musí čeliť aj rôznym rizikám. Hlavným a zároveň najväčším rizikom je, že ťažba bude nákladnejšia, ako samotný profit z odmeny a následného predaja vytŕažených mincí. Nároky na ťažbu sa neustále zvyšujú a v súčasnosti si ťažba digitálnych mincí vyžaduje množstvo zariadení výpočtovej techniky rovnako ako veľké množstvo spotrebovanej elektrickej energie. Tieto podmienky môžu vytvoriť ťažiarovi vysoké náklady, ktoré nie je následne schopný získať späť. Je na stratégii investora, aby správne rozhodol, či mu daná minca prinesie dostatočný výnos nielen na pokrytie nákladov, ale aj zisk.¹⁸ „Skutočná otázka, ktorú si treba položiť, znie: pri akej cene bitcoinu by som mal prestať ťažiť? Po zistení tohto ukazovateľa môžem ďalej analyzovať, aké zmeny je nutné vykonať, aby som zostal vo finančnej komfortnej zóne.“¹⁹ Vo všeobecnosti platí, že staršie ťažobné zariadenia v kombinácii s veľmi lacnou elektrickou energiou boli vždy najvýhodnejším spôsobom ťažby, pretože maximalizujú celkový hashpower za relatívne nízke množstvo kapitálu. Keď variabilné náklady (náklady na elektrickú energiu) stúpajú v porovnaní s nákladmi ostatných

¹⁸ SINEK, Robert. *DETAILS OF CRYPTOCURRENCY MINING: THE ULTIMATE GUIDE ABOUT BLOCKCHAIN, MINING, TRADING, ICO, ETHEREUM PLATFORM, EXCHANGES*, Independently published, 2018. ISBN 9781386771234.

¹⁹ HASHIMOTO, Hal. *The economics of Crypto-currency mining*. Independently published. 2021. s.22. ISBN 9798717952729.

ťažiarov, staršie zariadenia rýchlo strácajú svoju príťažlivosť a svoju ziskovosť. Je to preto veľmi dynamický biznis.²⁰

Ziskovosť ťažby pri zachovaní všetkých ostatných podmienok má tendenciu klesať. Veľkú úlohu v celkovej odmene ťažiarov zohrávajú aj sieťové poplatky. Keď sieťové poplatky dlhšie obdobie zostanú na vysokých hodnotách a zvyšuje sa hashrate, tieto podmienky môžu spôsobiť rapídny pokles ziskovosti.

„Vezmime si do úvahy otázku, ktorú si položí každý nový ťažiar : "Je ťažba zisková?". Odpoveď, ktorá sa objaví, či už sme v roku 2013 alebo 2020, je vždy "Ťažba nie je zisková".“²¹

Je to zaujímavá odpoveď vzhľadom na nárast zložitosti, a teda aj hashovacej kapacity od začiatku ťažby. Časť odpovede vychádza zo skutočnosti, že všetci ťažiar zdieľajú rovnakú odmenu, ktorá sa medzi nich delí. Ak povzbudíte nových ťažiarov, aby začali ťažiť, bude to tak na vaše vlastné náklady, pretože vyplácaná odmena sa rozdelí na väčšiu časť. Je to však nesprávny argument. Noví ťažiar sa automaticky stávajú aktívnymi používateľmi siete, hľadajú odbyt pre svoje mince a privádzajú aj ďalších nových používateľov. Rast počtu nových ťažiarov znamená rast celého krypto ekosystému, rast dopytu, čo následne vedie k rastu ceny. Keďže ponuka bitcoinu má v čase klesajúci charakter a bitcoiny sa strácajú alebo hromadia, jeho trhovú cenu bude za predpokladu minimálneho konštantného dopytu dlhodobo rásť, čo samozrejme zvýši aj ziskovosť ťažby. To, čo škodí ziskovosti je stále vyvíjajúci sa hardvér, služby a softvér, ktorý je špeciálne navrhnutý pre ťažobné farmy.²²

„Skutočná odpoveď na otázku "je ťažba výnosná ?" je "samozrejme"“²³

Ťažiar, ktorí sa rozhodnú ťažiť v domácich priestoroch s malým množstvom hardvéru si dokážu každý deň zarobiť niekoľko dolárov. Ak ťažiar zvolí kryptoaktívum, ktoré bude schopný ťažiť za čo najnižšie náklady, môže získať späť veľkú časť vstupných nákladov približne do obdobia jedného roka.

²⁰HASHIMOTO, Hal. *The economics of Crypto-currency mining*. Independently published. 2021. ISBN 9798717952729.

²¹HASHIMOTO, Hal. *The economics of Crypto-currency mining*. Independently published. 2021. s.27. ISBN 9798717952729.

²²HASHIMOTO, Hal. *The economics of Crypto-currency mining*. Independently published. 2021. ISBN 9798717952729.

²³HASHIMOTO, Hal. *The economics of Crypto-currency mining*. Independently published. 2021. s.28. ISBN 9798717952729.

„Ak by sme chceli dosiahnuť obstojný zisk, museli by sme byť schopní investovať okolo 5000 USD do hardvéru ešte pred samotným začiatkom. Ak sme toho schopní, môžeme zarobiť viac ako 50 dolárov denne.“²⁴

Veľa začínajúcich ťažiarov však nie je ochotných zaplatiť tieto náklady vopred, aby mohli začať, takže ťažba kryptoaktív v malom množstve nie je dobrá voľba pre väčšinu ľudí.²⁵

1.5. Empirický výskum

Chu a Wang²⁶ k otázke decentralizácie blockchainu analyzovali v roku 2018 problémy decentralizácie blockchainu. Na základe analýzy kvantitatívnej miery blockchainovej decentralizácie v súvislosti s jej dopadmi na rôzne modely dôvery a konsenzuálne algoritmy systému dospeli k záveru, že kľúčovými problémami v oblasti decentralizácie blockchainu sú: skreslené rozloženie ťažobného výkonu, inherentný rozpor medzi decentralizáciou a škálovateľnosťou (dokázali prvú hornú hranicu priepustnosti transakcií decentralizovaných blockchainových systémov), plne replikované a jednovláknové vykonávanie činností a sekvenčný programovací model zabraňujúci vykonávaniu škálovania inteligentných kontraktov. Analyzovali bitcoin, ethereum, škálovateľnosť smart kontraktov, PoS (Proof of Stake) a DPoS (Delegated Proof of Stake).

Zhang, Qin, Yuan a Wang²⁷ k zložitosti a technike ťažby analyzovali v roku 2018 princípy na úpravu zložitosti ťažby v blockchain sieti pri ťažbe bitcoinu. Na základe analýzy procesu výpočtu zložitosti ťažby a faktorov, ktoré ju môžu ovplyvniť dospeli k záveru, že zložitosť ťažby je dôležitý faktor podieľajúci sa na bezpečnosti blockchain siete, od ktorého závisí ako rýchlo sú ťažiaroch schopní nájsť nový platný blok v systéme. V bitcoin sieti sa zložitosť upravuje každých 2016 vytŕažených blokov tak, aby sa čas na nájdenie nového bloku udržal na úrovni približne 10 minút. Príčinu vidia v tom, že zložitosť ťažby má zásadný vplyv na udržanie stability bitcoin siete. Analyzovali sieť bitcoin, procesy výpočtu zložitosti na vytvorenie nových blokov, faktory, ktoré tento proces ovplyvňujú (množstvo

²⁴BENSON, Jared. *Cryptocurrency mining*. CreateSpace Independent Publishing Platform, 2018. s.15. ISBN 9781985790070.

²⁵BENSON, Jared. *Cryptocurrency mining*. CreateSpace Independent Publishing Platform, 2018. ISBN 9781985790070.

²⁶CHU, Shumo – WANG, Sophia. The Courses of Blockchain Decentralization [elektronický zdroj]. Washington, [2018], online. 7 s. [cit. 2022-03-22]. Dostupné na: <https://arxiv.org/pdf/1810.02937.pdf>

²⁷ZHANG, Xiaojing – QIN, Rui – YUAN, Yong – WANG, Fei-Yue. *An analysis of Blockchain-based Bitcoin mining difficulty: Techniques and Principles* [elektronický zdroj]. Beijing, [2018], online. 6 s. [cit. 2022-03-26]. Dostupné na: <https://ieeexplore.ieee.org/document/8623140>

voľného výpočtového výkonu, množstvo aktuálnych transakcií etc.), zložitosť ťažby a jej historický vývoj.

Kumar²⁸ k zefektívneniu ťažby bitcoinu analyzoval v roku 2021 potenciál využitia geotermálnej energie pri ťažbe bitcoinu. Na základe analýzy spotreby elektrickej energie, analýzy nákladov spojených s ťažbou a dlhodobej udržateľnosti nízkych nákladov dospel k záveru, že využitie geotermálnej energie je efektívnejšie, ako využitie klasickej elektrickej energie. Príčinu vidí v tom, že geotermálna energia je ekologickejšia a zároveň viac nákladovo efektívna alternatíva v porovnaní s elektrickou energiou. Geotermálna energia však nie je úplne bezchybná. Z dlhodobého hľadiska môže spôsobovať určité geoseizmické problémy, no v konečnom dôsledku je to výhodná možnosť. Analyzoval zdroje geotermálnej energie v Amerike, náklady na elektrickú energiu spojené s ťažbou, výnosnosť investície do ťažby, dlhodobú udržateľnosť nákladov a medzery v predošlom výskume tejto oblasti, pričom odporučil ďalší, podrobnejší výskum.

Dilek a Furuncu²⁹ k negatívnym dopadom kryptomien na spoločnosť analyzovali v rokoch 2018 a 2019 vplyv ťažby bitcoinu na životné prostredie. Na základe analýzy porovnania historických údajov spotreby elektrickej energie pri ťažbe so súčasnými, a porovnania vyprodukovaného CO₂ prepočítaného na transakciu dospeli k záveru, že vzhľadom na zvyšujúce sa požiadavky kvality a množstva hardvéru potrebného na ťažbu je obrovské množstvo spotreby elektrickej energie dlhodobo neudržateľné. Je známe, že v snahe vyhnúť sa vysokým nákladom na energiu ťažiarne firmy vykonávajú tieto operácie v krajinách, kde je energia lacná. Neustály rast spotreby elektrickej energie v dôsledku zvyšujúcich sa nárokov na ťažbu bitcoinu bude mať environmentálne aj sociálne dôsledky, ako napríklad globálne otepľovanie alebo zmenu klímy. Analyzovali údaje nárastu spotreby energie, údaje o spotrebe energie na transakcie, údaje o znečistení v jednotlivých krajinách, produkciu CO₂ ťažbou a jej vplyv na znečistenie životného prostredia.

²⁸KUMAR, Sumit. *Review of geothermal energy as an alternate energy source for Bitcoin mining* [elektronický zdroj]. [2018], online. 13 s. [cit. 2022-03-28]. Dostupné na: https://www.researchgate.net/profile/Sumit-Kumar-185/publication/358249180_REVIEW_OF_GEOTHERMAL_ENERGY_AS_AN_ALTERNATE_ENERGY_SOURCE_FOR_BITCOIN_MINING/links/61f877a0aad5781d41c273f2/REVIEW-OF-GEOTHERMAL-ENERGY-AS-AN-ALTERNATE-ENERGY-SOURCE-FOR-BITCOIN-MINING.pdf

²⁹DİLEK, Şerif – FURUNCU, Yunus. *Bitcoin mining and its environmental effects* [elektronický zdroj]. [2018], online. 15 s. [cit. 2022-04-01]. Dostupné na: <https://dergipark.org.tr/en/download/article-file/641972>

Guo a Liang³⁰ k praktickému využitiu systému blockchain analyzovali v roku 2016 potenciál jeho uplatnenia v bankovom sektore v Číne. Na základe analýzy výdavkov spojených s využívaním tradičných bankových systémov a blockchainu, výnosnosti a návratnosti aktív komerčných bánk a porovnaní tradičných bankových systémov s blockchainom dospeli k záveru, že systém blockchain by mohol priniesť modernizáciu a transformáciu v platobných zúčtovacích a úverových systémov v bankách. Príčinu vidia v tom, že online finančný sektor ponúka nové možnosti a scenáre fungovania tak, aby prilákal ešte viac zákazníkov a používateľov. Keďže sféra internetového finančníctva sa ešte len vyvíja, časom bude každodennou súčasťou využívanou spotrebiteľmi, čo predstavuje významnú hrozbu pre dominantné postavenie bánk v budúcnosti. Cezhraničné transakcie vykonané cez blockchain sú výrazne lacnejšie ako klasické transakcie a zároveň sú oveľa rýchlejšie a efektívnejšie. Ďalší dôležitý faktor je, že blockchain je oveľa bezpečnejší ako klasické bankové systémy. Implementácia systému blockchain však bude vyžadovať vyriešenie problémov ako decentralizácia, regulácia a samospráva blockchainu. Analyzovali návratnosť aktív komerčných bánk, skúsenosti zákazníkov bánk s jednotlivými systémami, cenovú nákladovosť, efektivitu a bezpečnosť systémov, výšku poplatkov za cezhraničné platby a typy blockchainov najvhodnejšie pre využitie v bankovom sektore.

³⁰GUO, Ye – LIANG Chen. *Blockchain application and outlook in the banking industry* [elektronický zdroj]. Xiamen, [2016], online. 12 s. [cit. 2022-04-05]. Dostupné na: <https://link.springer.com/content/pdf/10.1186/s40854-016-0034-9.pdf>

2. Cieľ, metodika a metódy práce

Cieľom bakalárskej práce je vymedziť slabé a silné stránky technológie blockchain ako aj výhody a nevýhody ťažby kryptomien v dnešnom medzinárodnom finančnom prostredí. Keďže sa v slovenskej literatúre nevenuje veľa pozornosti fungovaniu siete blockchain, ani ťažbe bitcoinu, rozhodli sme sa, priblížiť túto problematiku.

Pre naplnenie hlavného cieľa bakalárskej práce, sme si vytýčili nasledujúce čiastkové ciele:

- Vymedzenie trhu s kryptoaktívami, popísanie jeho fungovania, determinovanie výhod a nevýhod kryptoaktív
- Charakteristika a priblíženie funkcionality blockchain siete, zhodnotenie silných a slabých stránok
- Charakteristika procesu ťažby bitcoinu, vymedzenie faktorov, ktoré ju ovplyvňujú, identifikácia rizík a benefitov spojených s ťažbou
- Objasnenie praktického postupu prípravy investora pred realizáciou ťažby, stanovenie faktorov, ktoré ovplyvňujú rentabilitu ťažby bitcoinu, prehľad ťažby vo svete a posúdenie rentability ťažby v štátoch s rôznymi vstupnými faktormi
- Porovnanie efektívnosti ťažby a obchodovania s bitcoinom

Pri spracovaní zdrojov boli použité logické metódy: štúdium domácej a zahraničnej literatúry, zber dát (eurostat, university of cambridge, forbes), úprava dát (microsoft excel), grafické spracovanie (canva), indukcia, analýza, komparácia a syntéza.

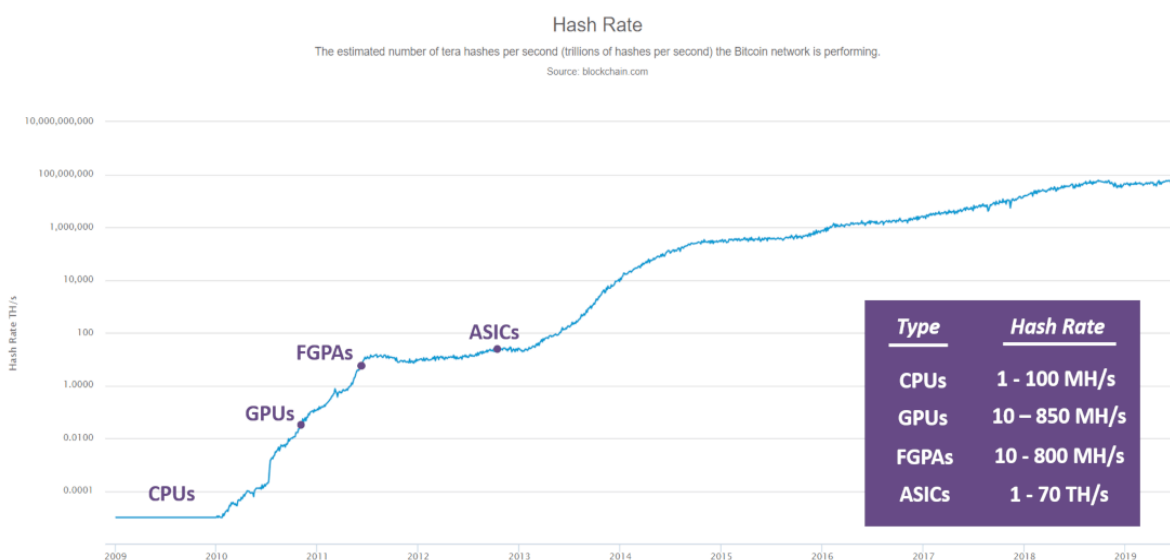
3. Výsledky práce a diskusia

3.1. Faktory vplyvajúce na efektivitu ťažby bitcoinu

Existuje mnoho faktorov ktoré určujú, či bude ťažba bitcoinu zisková. Samotný proces je v praxi spojený s prípravou a mnohými zásadnými rozhodnutiami, ktoré je potrebné urobiť ešte pred samotným začatím. Je nutné naplánovať business stratégiu a musia byť vytýčené ciele, vybrať lokalita s blízkym zdrojom lacnej elektrickej energie a štát s vyhovujúcou legislatívou pre podnikanie v oblasti kryptoaktív.

Výber správneho zariadenia na ťažbu patrí medzi dôležitú časť plánovania procesu. V začiatkoch bitcoinu (r. 2010) bolo možné efektívne ťažiť s bežným procesorom (CPU). Do obyčajného notebooku alebo stolového počítača bolo len potrebné stiahnuť softvér a mohlo sa začať ťažiť. Akonáhle sa začalo k sieti pripájať viac ťažiarov, začal prudko stúpať aj celkový hashrate a dopyt po ťažbe. To začalo novú éru grafických kariet. Jednotky GPU (grafické výpočtové jednotky) sú špecializovanejšie ako bežne používané procesory, to znamená, že sú účinnejšie a výkonnejšie pri nepretržitom vykonávaní výpočtov spojených s ťažbou. Ťažba bitcoinu pomocou GPU však dlho nevydržala, najmä kvôli zvyšujúcej sa náročnosti ťažby. V súčasnosti dominujú celému odvetviu špecializované zariadenia zvané ASIC (application-specific integrated circuit). ASIC je špeciálne navrhnutý integrovaný obvod, ktorý je vhodný na vykonávanie jedinej špecifickej úlohy – v tomto prípade výpočtu matematických šifri pri ťažení bitcoinu. Práve rýchlosť riešenia týchto šifri ho najviac zvýhodňuje v porovnaní s procesormi.

Graf č. 1 Výkonnosť siete pri používaní rôznych zariadení na ťažbu



Zdroj: vlastné spracovanie na základe <https://www.blockchain.com/charts/hash-rate>

Z analýzy grafu hashratu vidíme, že pri ťažbe kryptomien špecializácia a technologický vývoj vytvára veľké rozdiely medzi procesormi, na ktorých sa dá vykonávať ťažba. V súčasnosti je rozdiel taký veľký, že od roku 2013 sa oplatí ťažiť bitcoin jedine na ASIC procesoroch. Výška nákladov spojená s používaním CPU alebo GPU pri ťažbe bitcoinu je oveľa vyššia, ako výška potenciálnych príjmov pri maximálnej efektívite ťažby.

Pre čo najefektívnejší výber sme v tabuľke porovnali procesory ASIC určené na ťažbu bitcoinu, momentálne dostupné na trhu.

Tabuľka č.1 Porovnanie procesorov ASIC

Spoločnosť	Názov	Cena (USD)	Výkon (Th/s)	Spotreba (W)
Bitmain (Čína)	Antminer S17	3000	56	2520
MicroBT (Čína)	Whatsminer M20S	2700	68	3360
Canaan (Čína)	Avalonminer 1066	1800	50	3250
Ebang (Čína)	EBIT E11 ++	2400	44	1980
Innosilicon (Čína)	T3 +	2150	52	2200

Zdroj: vlastné spracovanie

Zistili sme, že ponuka trhu je výrazne obmedzená kvôli nízkemu počtu výrobcov. Po ASIC procesoroch je však mimoriadne vysoký dopyt vzhľadom na ich výkonnosť a efektívnosť pri ťažbe bitcoinu. V prípade, že nemáme veľkú halu so stovkami procesorov, alebo nie sme v ťažiarstvom odvetví dlhšiu dobu, ktorá by zabezpečila nadviazanie osobných kontaktov s výrobcami procesorov, nájdenie dostatočného počtu voľného hardvéru typu ASIC na trhu je veľmi ťažká úloha.

Ďalším kľúčovým faktorom je doba dodania strojov z Číny, ktorá vyrába všetky typy procesorov ASIC. Pri vysokom dopyte po týchto zariadeniach sa čakacia doba na dodanie odhaduje na pol roka až rok. Ďalší problém, ktorý sme identifikovali môže nastať pri samotnej platbe za stroje. Výrobcovia zväčša prijímajú platby iba v kryptomenach, takže by sme museli prostredníctvom burzy kúpiť veľké množstvo bitcoinu, aby sme mohli za vybrané procesory zaplatiť.

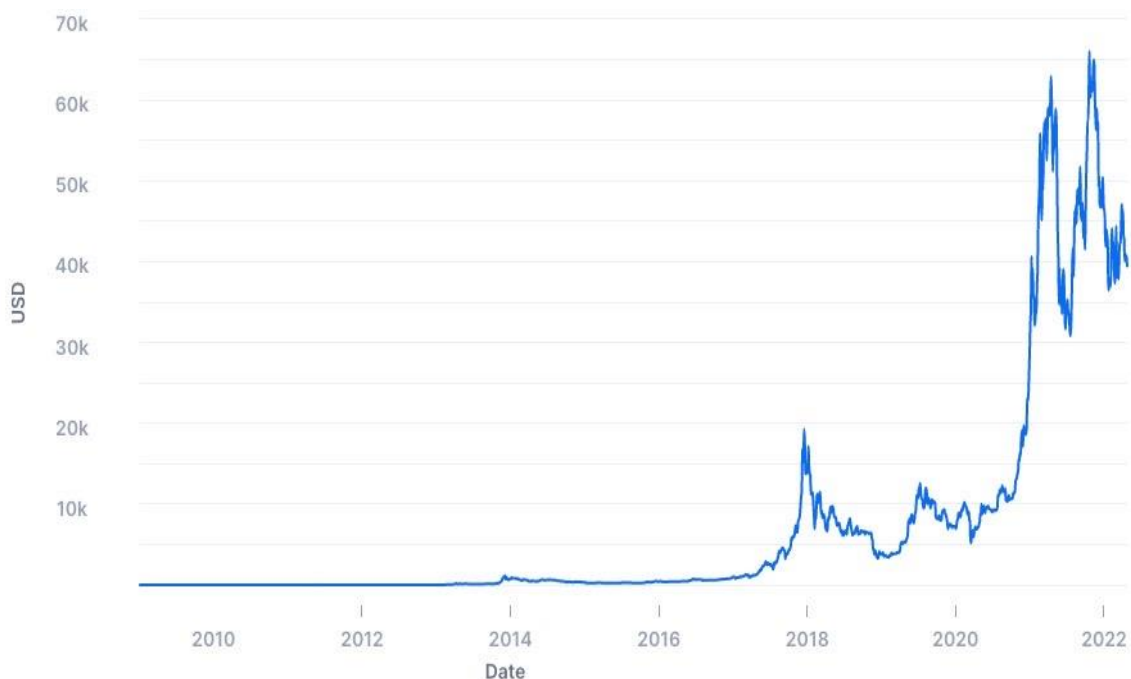
Zaobstaranie hardvéru na ťaženie je prvý nevyhnutný krok na to, aby sa mohol ťažiť bitcoin. Nie je to však jediný faktor na zachovanie dlhodobej ziskovosti. Ďalšie dôležité faktory pri ťažbe bitcoinu sme zhrnuli do 3 ďalších bodov.

- Cena bitcoinu
- Náročnosť ťažby
- Náklady na energie

Jeden z najviditeľnejších faktorov je samotná trhovacia cena bitcoinu, ktorá má zásadný vplyv na výšku budúceho príjmu.

Bitcoin sa pohybuje v určitých cykloch, preto je potrebné ho analyzovať a rozhodovať sa, či bude efektívnejšie vyťažený bitcoin predat' za aktuálnu cenu na burze, alebo počkať na rast ceny v budúcnosti.

Graf č. 2 Cena bitcoinu (USD)

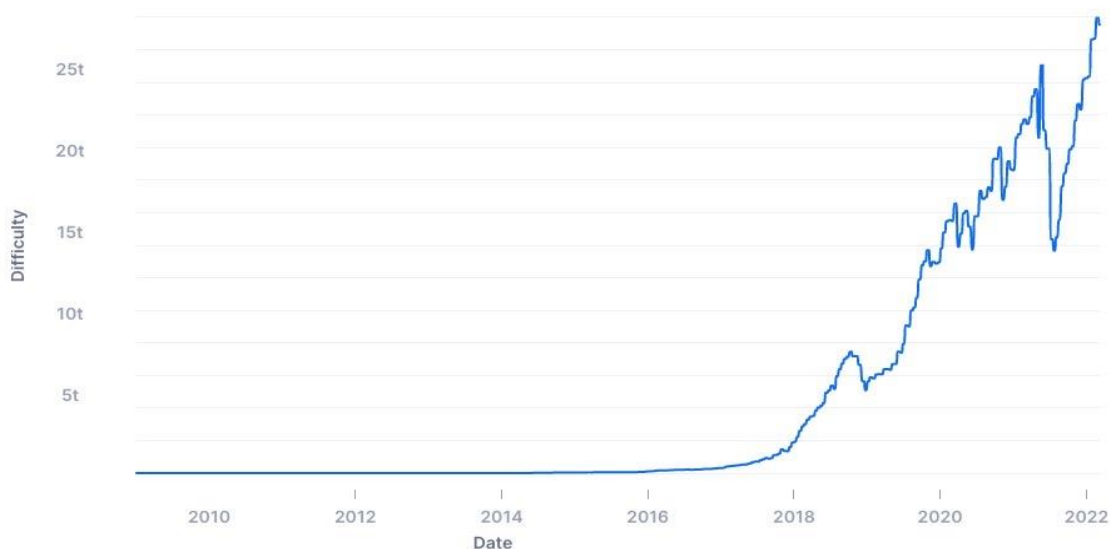


Zdroj: <https://www.blockchain.com/charts/market-price>

Ďalší z faktorov, ktorý je potrebné brať na vedomie je ťažba a jej zložitosť. Zložitosť ťažby vyjadrujeme v čase, ktorý je potrebný na rozšifrovanie matematickej šifry. Rozšifrovaním šifry sa vytvára nový blok v blockchaine.

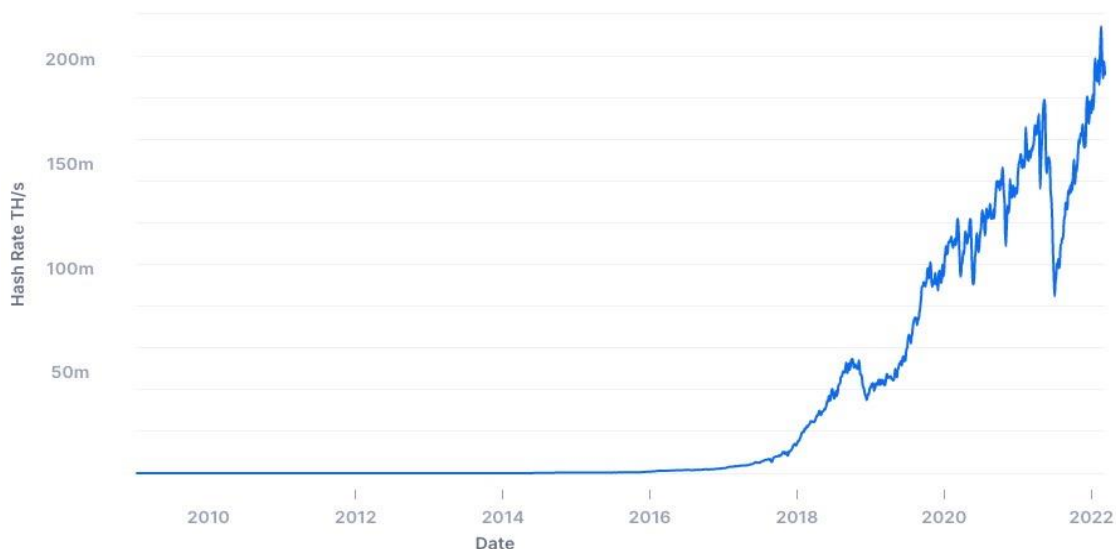
Náročnosť nájdenia nového bloku je priamo úmerná celkovému výkonu ťažobnej siete, čo znamená, že čím väčší je ťažobný výkon, tým ťažšie je nájsť nasledujúci blok.

Graf č. 3 Bitcoin - náročnosť ťažby



Zdroj: <https://www.blockchain.com/charts/difficulty>

Graf č. 4 Bitcoin - výpočtový výkon siete



Zdroj: <https://www.blockchain.com/charts/hash-rate>

Poznámka: TH/s - Tera HASH za sekundu. Jeden bilión hashov vypočítaných za jednu sekundu.

Vysoká zložitosť znamená, že na vytáženie rovnakého počtu blokov je potrebný väčší výpočtový výkon. Čím väčší je však výpočtový výkon siete (hashrate), tým je sieť bezpečnejšia a odolnejšia voči útokom. Na grafoch náročnosti ťažby a výkonnosti siete vidíme koreláciu. Náročnosť ťažby je pri bitcoine upravovaná každých približne 2016 blokov (približne každé 2 týždne) tak, aby priemerný čas medzi jednotlivými blokmi zostal

okolo 10 minút. Náročnosť vyplýva priamo z údajov o potvrdených blokoch v sieti blockchain.

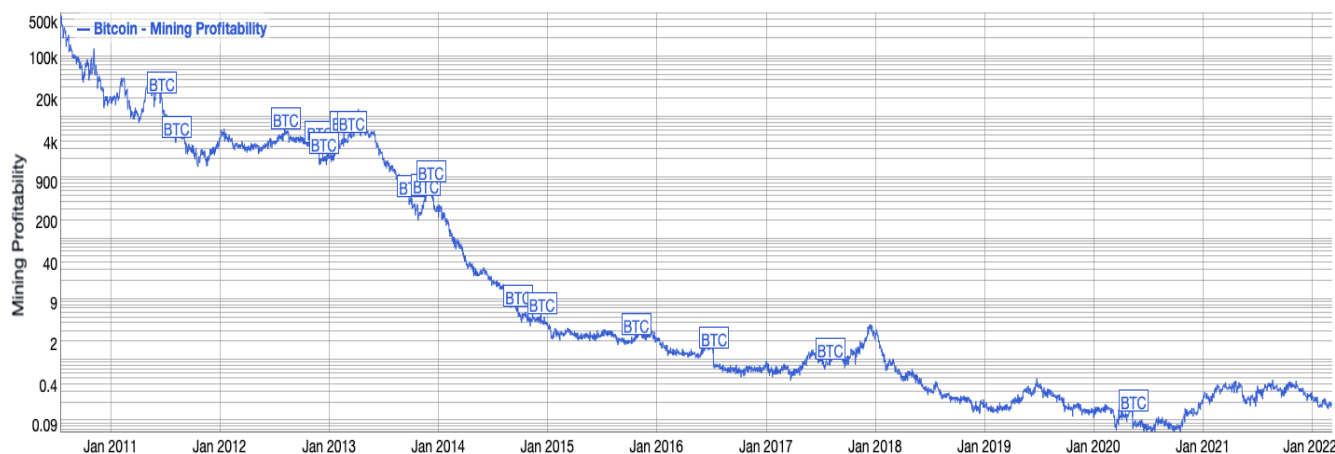
S rastom výpočtového výkonu má graf výnosnosti ťažby v prepočte na 1 TeraHash klesajúci charakter. Na výpočet výnosnosti ťažby používame pomer medzi ťažiarskym výkonom siete a cenou bitcoinu. Pri používaní a ťažení bitcoinu sa stretávame s opatrením – halving. Je to protiinflačné opatrenie, ktorým sa spomaľuje uvoľňovanie nových jednotiek bitcoinu do obehu. Ide o periodickú udalosť, ktorá sa opakuje každé štyri roky, pričom odmena pre ťažiarov sa vždy znižuje o polovicu za vyťažovaný blok.

Tabuľka č. 2 Halving

Halving	Dátum halvingu	Číslo bloku	Odmena za vyťaženie bloku (BTC)
0.	---	0	50
1.	2012	210 000	25
2.	2016	420 000	12,5
3.	2020	630 000	6,25
4.	2024	840 000	3,125
5.	2028	1 050 000	1,5625

Zdroj: vlastné spracovanie

Graf č. 5 Výnosnosť ťažby bitcoinu v USD za 1 THash/s



Zdroj: https://bitinfocharts.com/comparison/bitcoin-mining_profitability.html#log&alltime

Graf výnosnosti reaguje na graf ceny, pretože trvá nejaký čas, kým ťažiarci zvýšia výkon siete a kým sa prispôbi zložitosť ťažby. Ziskovosť bitcoinu na jednotku hashpower klesá v dôsledku pribúdajúcich, stále lepších a výkonnejších procesorov. Celková ziskovosť sa však neodvíja len od prepočtu na hashpower, ale predovšetkým od ceny bitcoinu.

Posledný faktor, ktorý má najzásadnejší vplyv na ziskovosť ťažby sú náklady na energie. Väčšina denných prevádzkových nákladov je tvorená najmä spotrebou elektrickej energie ťažiarских zariadení, ktoré pracujú 24 hodín denne 7 dní v týždni. Najvýhodnejšou alternatívou je teda prebytočná energia vyrobená z obnoviteľných zdrojov, ako sú hydroelektrárne, solárne panely alebo veterné farmy. Práve energia z týchto zdrojov je vo svete najčastejšie používaná na ťažbu bitcoinu. Ročná spotreba elektrickej energie sieťou bitcoin sa odhaduje na 129 TWh (TeraWatt hodín). V tabuľke sme porovnali spotrebu siete bitcoin so spotrebou iných štátov a firiem.

Tabuľka č. 3 Porovnanie spotreby elektrickej energie (2021)

Názov	Počet obyvateľov	Ročná spotreba elektrickej energie (TWh)	Ročná produkcia elektrickej energie (TWh)
Čína	1,4 miliardy	6 543	8 112
USA	331 miliónov	3 989	4 116
Sieť bitcoin	-	129	-
Nórsko	5,4 milióna	124	156
Slovensko	5,5 milióna	26,6	31
Bangladéš	165 miliónov	70	89
Google	-	12	-
Facebook	-	5	-

Zdroj: Cambridge Centre for Alternative Finance, Science Mag, New York ISO, Forbes, Eurostat

Poznámka: 1 Terawathodina (TWh) reprezentuje elektrickú hodnotu 1 miliarda wattov spotrebovaných za 1 hodinu

Vybrané štáty produkujú viac energie ako spotrebujú, to znamená že v prípade väčšieho rozvoja ťažby bitcoinu v týchto štátoch nebudú vznikať pre štát dodatočné náklady na kupovanie elektrickej energie zo zahraničia. Spotreba pre chod siete bitcoinu jemne presahuje ročnú spotrebu elektrickej energie Nórska v roku 2021. V porovnaní so spotrebou

spoločnosti Google je viac ako 10 násobne vyššia, čo predstavuje zaujímavé výsledky, no v porovnaní so štátmi ako USA a Čína je však táto spotreba stále relatívne malá.

Čo sa týka ťažby bitcoinu sme zistili, že krajiny, kde sa bitcoin najviac ťaží využívajú hlavne energiu vyrábanú z uhlia, zemného plynu a z vody. Zvýšenie využitia energie produkovanej obnoviteľnými zdrojmi by určite dopomohlo znížiť dopad ťažby bitcoinu na životné prostredie.

Tabuľka č. 4 Využitie rôznych typov energií pri ťažbe bitcoinu (2021)

Zdroje energie	Ázia	Európa	Južná a Stredná Amerika	Severná Amerika
Vodná energia	65%	60%	67%	61%
Zemný plyn	38%	33%	17%	44%
Uhlie	65%	2%	0%	28%
Veterná energia	23%	7%	0%	22%
Ropa	12%	7%	33%	22%
Jadrová energia	12%	7%	0%	22%
Slnečná energia	12%	13%	17%	17%
Geotermálna energia	8%	0%	0%	6%

Zdroj: University of Cambridge (2021)

Poznámka: Údaje v jednotlivých stĺpcoch sa nesčítavajú do 100

V tabuľke sme analyzovali podiel využívanej energie rôznych typov pri ťažbe bitcoinu v jednotlivých svetových regiónoch. „Obnoviteľné zdroje energie³¹ predstavujú len 39% celkovej spotreby energie pri ťažbe bitcoinu.“³² V tejto oblasti vidíme výzvu na zlepšenie, využívať vo väčšej miere obnoviteľné zdroje, ktoré šetria životné prostredie. Očakávame, že v najbližších rokoch vysoká spotreba energie vyrábanej z uhlia v Ázii výrazne klesne vzhľadom na vládne obmedzenia voči kryptoaktívam v Číne, ktorá je najväčším producentom energie z uhlia, čo výrazne zlepší aj dopad na životné prostredie.

³¹geotermálna energia, vodná energia, slnečná energia, veterná energia

³²SCHMIDT, John. *Why does bitcoin use so much energy?* [elektronický zdroj]. [2022], online. [cit. 2022-04-06]. Dostupné na: <https://www.forbes.com/advisor/investing/cryptocurrency/bitcoins-energy-usage-explained/>

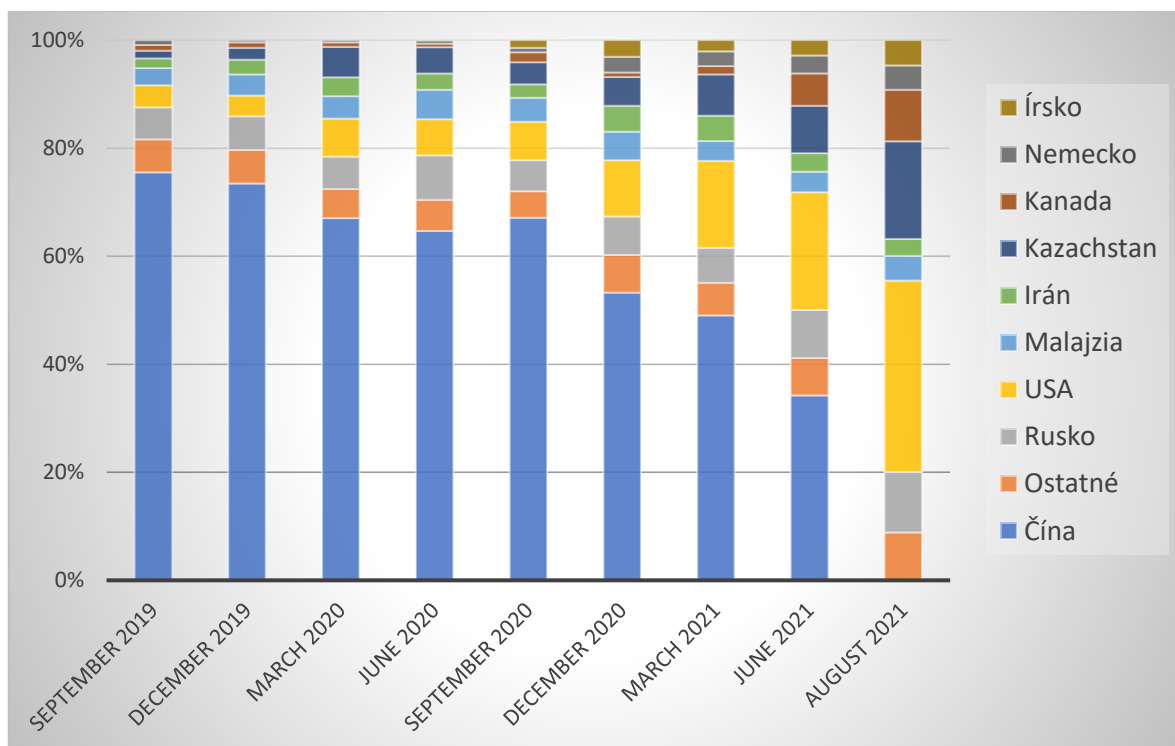
Vlády a regulačné orgány štátov by mali venovať väčšiu pozornosť uhlíkovej stope zanechávanej týmto odvetvím.

Vládne opatrenia a regulácie kryptotrhu je nutné si predom naštudovať a brať ich do úvahy pri výbere krajiny, v ktorej by sme chceli realizovať ťažbu. V mnohých štátoch nie je otázka regulácie trhu s kryptoaktívami vyriešená. Ťažba sa v posledných mesiacoch presunula zo štátov ako Čína, kde boli kryptoaktíva zakázané a ťažiari vyhostení do štátov, kde je kryptotrh bez regulácií.

Tu vidíme systémové zlyhanie, pretože zo strany niektorých štátov nebol zaujatý jednoznačný postoj voči trhu s bitcoinom a inými kryptoaktívami. Niektoré štáty si ho adoptovali ako menu, iné ho naopak zakázali, a iné sa danou otázkou zatiaľ nezaoberali. Preto odporúčame riadiacim orgánom jednotlivých štátov, aby vytvorili legislatívu pre trh s kryptoaktívami a aby kládli dôraz na využívanie energie z obnoviteľných zdrojov.

V súčasnosti je zložité z pozície ťažiara nájsť vhodný štát s jednoznačnou legislatívou a zároveň štát, kde by bol schopný ťažiť pri čo najnižších nákladoch na energiu. Aktuálny podiel jednotlivých štátov na ťažbe bitconu sme premietli v nasledujúcom grafe. Osobitnou otázkou je aj oblasť zdaňovania kryptoaktív, tou sa ale v tejto práci nezaobráme.

Graf č. 6 Podiel jednotlivých štátov na ťažbe bitcoinu



Zdroj: vlastné spracovanie na základe https://ccaf.io/cbeci/mining_map

Pre porovnanie rentability ťažby sme pripravili modelovú situáciu, vďaka ktorej vieme ďalej analyzovať a porovnávať rentabilitu ťažby bitcoinu v rôznych podmienkach a štátoch. Vybrali sme štát, ktorý reprezentuje naše podmienky – Slovensko a štát reprezentujúci zahraničné podmienky vyššej životnej úrovne – USA, štát Texas a štát reprezentujúci zahraničné podmienky nižšej životnej úrovne – Kazachstan. Zistené údaje sme zapísali do tabuliek a následne porovnali.

Počítame so vstupným kapitálom 30 000\$, za ktorý by sme nakúpili najnovšie procesory ASIC Antminer S17 od spoločnosti Bitmain (Čína). Ťažba by prebiehala 24 hodín denne 7 dní v týždni. Náklady na prenájom priestoru sme zo situácie vynechali, pretože sme sa zamerali na náklady spojené s energiami. Pri situácii sme počítali s konštantnou cenou 31 000\$ za jeden bitcoin.

S kapitálom 30 000\$ sme schopní kúpiť 10 zariadení Antminer S17 od spoločnosti Bitmain, čo pre nás predstavuje ťažobný výkon o sile 560 Th/s a spotrebu energie 25 200 w.

Tabuľka č. 5 Informácie ku modelovanej situácii

Ťažobný výkon	560 Th/S
Spotreba energie	25200 w/h
Cena energie Slovensko (KWh)	0,17\$
Cena energie Texas (KWh)	0,089\$
Cena energie Kazachstan (KWh)	0,056\$

Zdroj: vlastné spracovanie

Zo získaných dát sme zistili, že pri konštantnej cene bitcoinu sme dosiahli najvyššiu rentabilitu v štáte s najnižšou životnou úrovňou a najlacnejšou energiou (Kazachstan). Potvrďuje to aj jeho zastúpenie v grafe porovnania štátov, v ktorých sa uskutočňuje ťažba. Vďaka podmienkam lacnej energie a nízkej regulácie sa do tohto štátu presunula väčšina ťažiarskych centier z Číny, kde im bolo zakázané fungovať. Ďalej sme zo získaných dát zistili, že v našich podmienkach je cena energií príliš vysoká, čo zapríčiňuje nerentabilitu ťažby.

Tabuľka č. 6 Rentabilita ťažby vo vybraných štátoch

Štát	Týždenný profit (\$)	Týždenný profit (BTC)	Mesačný profit (\$)	Mesačný profit (BTC)	Ročný profit (\$)	Ročný profit (BTC)
Slovensko	-206	0,01709	-883	0,07323	-10 740	0,891
Texas (USA)	154	0,01709	659	0,07323	8 023	0,891
Kazachstan	294	0,01709	1 258	0,07323	15 310	0,891

Zdroj: vlastné spracovanie

Poznámka: pre výpočet údajov bola použitá bitcoin kalkulačka³³

Predpokladáme, že krajiny s nižšou životnou úrovňou sú vhodnejšie na ťažbu v prípade, že si využívanú energiu kupujeme lacno. Alternatíva riešenia problému drahej energie je jej samostatné vyrábanie solárnymi panelmi, hydroelektrárnami alebo veternými elektrárnami. Toto riešenie by mohlo byť efektívne z dlhodobého horizontu, no vyžadovalo by si podrobnejšiu analýzu. S určitosťou však vieme povedať, že možnosť samovýroby elektrickej energie by si však vyžadovala ďalšiu vysokú investíciu, tým pádom by sa nám návratnosť investícií výrazne predĺžila, čo nepovažujeme za efektívne.

3.2.Rozhodnutie investora medzi obchodovaním a ťažbou bitcoinu

Investor má okrem ťaženia bitcoinu možnosť generovať zisk aj iným spôsobom – online obchodovaním bitcoinu na burze. Oba spôsoby investovania majú svoje výhody aj nevýhody a zahŕňajú riziká.

Môžeme však povedať, že online obchodovanie je určite prístupnejšie, pretože existuje obrovské množstvo obchodných platforiem, ktoré sú k dispozícii používateľom. Na obchodovanie investorovi stačí nižšia počiatočná investícia, no na druhej strane ak chce byť investor dlhodobo úspešný potrebuje skúsenosti, dobrý money management a obchodnú stratégiu.

S investovaním sa spája oveľa väčšia miera rizika straty finančných prostriedkov pri vysokej volatilitate na trhu. Na druhej strane ťažba bitcoinov je lepšou voľbou pre investora,

³³Bitcoin mining calculator [elektronický zdroj]. online. Dostupné na: <https://www.cryptocompare.com/mining/calculator/btc?HashingPower=768&HashingUnit=TH%2Fs&PowerConsumption=34560&CostPerkWh=0.15&MiningPoolFee=0>

ktorý vyhladáva dlhodobú investíciu do blockchainovej siete a má k dispozícii väčšie množstvo voľných finančných prostriedkov.

Zásadná otázka je, čo investor preferuje z klasického investičného trojuholníka. Pri preferencii likvidity, je pre investora lepšia voľba obchodovanie, pri výnose a riziku závisí od dĺžky investície, z krátkodobého hľadiska je lepšia voľba obchodovanie, z dlhodobého hľadiska je lepšia voľba investícia do ťažby.

Záver

Trh s kryptoaktívami nepochybne v súčasnosti zastáva významné miesto na finančnom trhu. Jeho postavenie výrazne ovplyvňuje dianie aj na ostatných segmentoch finančného trhu, preto je veľmi dôležité aby sa tento trh ďalej analyzoval a aby mu bola venovaná dostatočná pozornosť.

V úvodnej časti sme popísali trh s kryptoaktívami a jeho fungovanie. Taktiež sme priblížili fungovanie siete blockchain, vymedzili sme jej silné stránky, ktorými sú decentralizovaná sieť, transparentnosť, dôveryhodnosť a nemenná technológia. Za slabé stránky blockchainu sme identifikovali vysokú energetickú závislosť, náročný proces integrácie a vysoké náklady na implementáciu do praxe. V ďalšej časti sme popísali transakcie, ktoré v sieti blockchain prebiehajú, venovali sme pozornosť podstate a dôležitosti ťažby kryptomien pre ich celkové fungovanie a determinovali sme výhody a nevýhody ťažby. Hlavné výhody sú, že ťažiar je aktívne zapojený do práce pre blockchain a tým vytvára vyššiu bezpečnosť a dôveryhodnosť siete, odmeňovanie za ťažbu a minimalizácia rizika z dlhodobého hľadiska. Nevýhody ťažby sú, že ťažba nebude rentabilná kvôli vysokým výdavkom, vysoké vstupné náklady a technologický pokrok, ktorý môže zapríčiniť zníženie efektivity.

V praktickej časti sme sa zamerali na postup prípravy investora pred realizáciou ťažby a na faktory a dôvody, ktoré ovplyvňujú rentabilitu ťažby bitcoinu. Následne sme uviedli množstvo celkovej spotreby a celkovej produkcie elektrickej energie vybraných štátov a súčasne sme porovnali spotrebu elektrickej energie pri ťažbe bitcoinu. Vybrané štáty produkujú viac energie ako spotrebujú, to znamená, že v prípade väčšieho rozvoja ťažby bitcoinu v týchto štátoch nebudú vznikať pre štát dodatočné náklady na kupovanie elektrickej energie zo zahraničia. V ďalšej časti sme na modelovej situácii skúmali rentabilitu ťažby vo vybraných štátoch s rôznymi podmienkami. Zistili sme, že v krajinách s nižšou životnou úrovňou je predpoklad lacnejšej energie, čo zvyšuje rentabilitu ťažby bitcoinu v týchto štátoch.

Na záver konštatujeme, že rozhodnutie medzi investovaním do ťažby alebo obchodovaním závisí od rizikového profilu investora, veľkosti kapitálu a doby investovania. Zásadná otázkou pre investora je, čo preferuje z klasického investičného trojuholníka. Pri preferencii likvidity, by mal obchodovať, ak preferuje výnos a riziko, rozhodujúci faktor je doba investície.

Zoznam použitej literatúry

Knižné zdroje:

1. BENSON, Jared. 2018. *Cryptocurrency mining*. CreateSpace Independent Publishing Platform, United States, 64s. 2018. ISBN 9781985790070.
2. HASHIMOTO, Hal. 2021. *The economics of Crypto-currency mining*. Independently published, 2021. 29s. ISBN 9798717952729.
3. HESTON, Anthony. 2017. *Cryptocurrencies: How to safely create stable and long-term passive income by investing in Cryptocurrencies*. CreateSpace Independent Publishing Platform, United States, 2017. 95 s. ISBN 1975623703.
4. HOSP, Julian. 2018. *Krypto Meny*. Bratislava: TATRAN, 2018. 172 s. ISBN 978-80-222-0945-8.
5. KENT, Peter - BAIN, Tyler. 2019. *Cryptocurrency mining for dummies*. Nw Jersey: JohnWile & Sons Inc., 2019. 368s. ISBN 978-1-119-57929-8.
6. LEWIS, Antony. 2018. *The Basics of Bitcoins and Blockchains*. Mango Media, United States, 2018. 483 s. ISBN 978-1-63353-800-9.
7. SINEK, Robert. 2018. *DETAILS OF CRYPTOCURRENCY MINING: THE ULTIMATE GUIDE ABOUT BLOCKCHAIN, MINING, TRADING, ICO, ETHEREUM PLATFORM, EXCHANGES*. Independently published, 2018. 97s. ISBN 9781386771234.
8. STROUKAL, Dominik - SKALICKÝ, Jan. 2015. *BITCOIN Peníze budoucnosti*. Praha: Ludwig won Mises Institut CZ&SK, 2015. 167s. ISBN 978-80-87733-26-4.

Ostatné zdroje:

1. DÍLEK, Şerif – FURUNCU, Yunus. *Bitcoin mining and its environmental effects* [elektronický zdroj]. [2018], online. 15 s. [cit. 2022-04-01]. Dostupné na: <https://dergipark.org.tr/en/download/article-file/641972>
2. GUO, Ye – LIANG Chen. *Blockchian application and outlook in the banking industry* [elektronický zdroj]. Xiamen, [2016], online. 12 s. [cit. 2022-04-05]. Dostupné na: <https://link.springer.com/content/pdf/10.1186/s40854-016-0034-9.pdf>
3. CHU, Shumo – WANG, Sophia. *The Courses of Blockchain Decentralization* [elektronický zdroj]. Washington, [2018], online. 7 s. [cit. 2022-03-22]. Dostupné na: <https://arxiv.org/pdf/1810.02937.pdf>

4. KUMAR, Sumit. *Review of geothermal energy as an alternate energy source for Bitcoin mining* [elektronický zdroj]. [2018], online. 13 s. [cit. 2022-03-28]. Dostupné na: https://www.researchgate.net/profile/Sumit-Kumar-185/publication/358249180_REVIEW_OF_GEO_THERMAL_ENERGY_AS_AN_ALTERNATE_ENERGY_SOURCE_FOR_BITCOIN_MINING/links/61f877a0aad5781d41c273f2/REVIEW-OF-GEO_THERMAL-ENERGY-AS-AN-ALTERNATE-ENERGY-SOURCE-FOR-BITCOIN-MINING.pdf
5. SCHMIDT, John. *Why does bitcoin use so much energy?* [elektronický zdroj]. [2022], online. [cit. 2022-04-06]. Dostupné na: <https://www.forbes.com/advisor/investing/cryptocurrency/bitcoins-energy-usage-explained/>
6. ZHANG, Xiaojing – QIN, Rui – YUAN, Yong – WANG, Fei-Yue. *An analysis of Blockchain-based Bitcoin mining difficulty: Techniques and Principles* [elektronický zdroj]. Beijing, [2018], online. 6 s. [cit. 2022-03-26]. Dostupné na: <https://ieeexplore.ieee.org/document/8623140>