

EKONOMICKÁ UNIVERZITA V BRATISLAVE
FAKULTA HOSPODÁRSKEJ INFOMATIKY

Evidenčné číslo: 103004/B/2023/36124048428437508

BITCOIN A OSTATNÉ KRYPTOMENY AKO
INVESTIČNÉ AKTÍVUM, ICH VÝVOJ
A PROGNÓZY DO BUDÚCNOSTI

Bakalárska práca

EKONOMICKÁ UNIVERZITA V BRATISLAVE
FAKULTA HOSPODÁRSKEJ INFOMATIKY

BITCOIN A OSTATNÉ KRYPTOMENY AKO
INVESTIČNÉ AKTÍVUM, ICH VÝVOJ
A PROGNÓZY DO BUDÚCNOSTI

Bakalárska práca

Študijný program: Hospodárska informatika

Študijný odbor: Ekonómia a manažment

Školiace pracovisko: Katedra aplikovanej informatiky

Vedúci záverečnej práce: Ing. Pavol Sojka, PhD.

Bratislava 2023

Jozef Mikuš



Ekonomická univerzita v
Bratislave Fakulta hospodárskej
informatiky

ZADANIE ZÁVEREČNEJ PRÁCE

Meno a priezvisko študenta: Jozef Mikuš
Študijný program: hospodárska informatika (Jednoodborové štúdium, bakalársky I. stupeň, denná forma)
Študijný odbor: ekonómia a manažment
Typ záverečnej práce: Bakalárska záverečná práca
Jazyk záverečnej práce: slovenský
Sekundárny jazyk: anglický

Názov: Bitcoin a ostatné kryptomeny ako investičné aktívum, ich vývoj a prognózy do budúcnosti.
Anotácia: Študent vytvorí v práci porovnávacie kritériá pre komparáciu kryptomien a odporučí najvhodnejšiu pre ten ktorý účel. Referenčnou menou pre porovnanie bude Bitcoin, kde študent popíše jeho negatíva aj pozitíva a zároveň na negatívach Bitcoinu zdôrazní lepšie vlastnosti porovnávaných kryptomien.

Vedúci: Ing. Pavol Sojka, PhD.
Katedra: KAI FHI - Katedra aplikovanej informatiky
Vedúci katedry: Ing. Mgr. Peter Schmidt, PhD.
Dátum zadania: 24.03.2022

Dátum schválenia: 17.04.2023

doc. Ing. Martin Mišút, CSc.
osoba zodpovedná za realizáciu študijného programu

Čestné vyhlásenie

Čestne prehlasujem, že záverečnú prácu som vypracoval samostatne, a že všetku použitú literatúru a ďalšie podkladové materiály, ktoré som použil, uvádzam v zozname použitých zdrojov.

Dátum:

.....

(podpis študenta)

Pod'akovanie

Touto cestou by som sa chcel pod'akovať vedúcemu mojej bakalárskej práce, Ing. Pavlovi Sojkovi, PhD., za rýchle reagovanie, dôležité rady a tiež odborné konzultácie, počas písania práce.

Abstrakt

MIKUŠ, Jozef: *Bitcoin a ostatné kryptomeny ako investičné aktívum, ich vývoj a prognózy do budúcnosti*. – Ekonomická univerzita v Bratislave. Fakulta hospodárskej informatiky; Katedra aplikovanej informatiky. – Vedúci záverečnej práce: Ing. Pavol Sojka, PhD. – Bratislava: FHI EU, 2023, 45 s.

Záverečná práca je vypracovaná na tému bitcoin a ostatné kryptomeny ako investičné aktívum, ich vývoj a prognózy do budúcnosti. Cieľom záverečnej práce bolo identifikovať kryptomenu, ktorá má najväčší potenciál sa stať kvalifikovanou menou na základe detailnej analýzy. Budú porovnávané tri známe kryptomeny z dvoch hľadísk. Cieľom prvého porovnania je vybrať jednu, ktorá má najväčší potenciál stať sa budúcou menou, resp. finančným aktívom. Na základe druhého porovnania sa vyberie kryptomena s najväčším investičným potenciálom do budúcnosti. Porovnania budú uskutočnené na základe rôznych faktorov. Práca je rozdelená do troch kapitol. Jednotlivé časti záverečnej práce boli zamerané na vymedzenie problematiky kryptomien z teoretického hľadiska a ich následne porovnanie. Prvá kapitola je zameraná na teoretické vymedzenie skúmanej problematiky. Sú v nej vysvetlené základné pojmy a technológie kryptomien. V rámci druhej kapitoly je definovaný hlavný cieľ práce a tiež k nemu prislúchajúce parciálne ciele. V kapitole sú tiež opísané metódy k dosiahnutiu cieľa práce. V tretej kapitole sú v tabuľkách zhrnuté závery porovnania jednotlivých kryptomien z daného hľadiska na základe vopred definovaných faktorov. Výsledkom riešenia danej problematiky je výsledné porovnanie interpretované slovne. Je vybraná kryptomena s najväčším celkovým potenciálom do budúcnosti.

Kľúčové slová:

Kryptomena, bitcoin, cardano, ethereum, blockchain

Abstract

MIKUŠ, Jozef: *Bitcoin and other cryptocurrencies as an investment asset, their development and forecasts for the future.* – University of Economics in Bratislava. Faculty of Economic Informatics; Department of Applied Informatics. – Advisor: Ing. Pavol Sojka, PhD. – Bratislava: FHI EU, 2023, 45 p.

The final thesis is prepared on the subject of bitcoin and other cryptocurrencies as an investment asset, their development and future forecasts. The goal of the final thesis was to identify the cryptocurrency that has the greatest potential to become a qualified currency based on a detailed analysis. Three well-known cryptocurrencies will be compared from two points of view. The goal of the first comparison is to choose the one that has the greatest potential to become the future currency, or a financial asset. Based on the second comparison, the cryptocurrency with the greatest future investment potential is selected. Comparisons will be made based on various factors. The work is divided into three chapters. Individual parts of the final thesis were aimed at defining the issue of cryptocurrencies from a theoretical point of view and then comparing them. The first chapter is focused on the theoretical definition of the investigated issue. It explains the basic concepts and technologies of cryptocurrencies. Within the second chapter, the main goal of the work is defined, as well as the related partial goals. The chapter also describes methods to achieve the goal of the work. In the third chapter, the conclusions of the comparison of individual cryptocurrencies from a given point of view based on predefined factors are summarized in tables. The result of solving the given problem is the resulting comparison interpreted verbally. The cryptocurrency with the greatest overall future potential is selected.

Key words:

Cryptocurrency, bitcoin, cardano, ethereum, blockchain

Obsah

Úvod	10
1 Teoretické vymedzenie problematiky	12
1.1 Blockchain	12
1.2 Vysvetlenie transakcií vo všeobecnosti	12
1.3 Pojmy	12
1.4 Výhody a nevýhody kryptomien	14
1.5 Cardano	14
1.5.1 Konkurencia	14
1.5.2 Smart kontrakty	15
1.5.3 Spustenie siete	15
1.5.4 Transakcie digitálnych aktív.....	15
1.5.5 Veľká základňa aktívnych používateľov.....	16
1.5.6 Riadenie a financovanie	16
1.5.7 Vývoj.....	16
1.5.8 Výhody	17
1.5.9 Potenciálne riziká.....	17
1.6 Bitcoin.....	18
1.6.1 Porovnanie s dnešným bankovým systémom.....	18
1.6.2 Zhrnutie	19
1.6.3 Ako sa bitcoiny ukladajú?	19
1.6.4 Čo sa stane, keď uskutočním platbu bitcoinom?	20
1.7 Ethereum	20
1.7.1 Decentralizované aplikácie Etherea	21
1.7.2 Ako ethereum funguje?	21
1.7.3 Gas	21
1.7.4 Porovnanie s bitcoinom.....	22
2 Cieľ práce a metódy spracovania	23
3 Porovnania kryptomien a výsledky práce	24
3.1 Porovnanie kryptomien z hľadiska potenciálu finančného aktíva.....	24
3.1.1 Cardano	24
3.1.2 Bitcoin	26
3.1.3 Ethereum	30

3.1.4 Záverečné porovnanie	33
3.2 Porovnanie kryptomien z hľadiska investičného potenciálu.....	33
3.2.1 Cardano	33
3.2.2 Bitcoin	35
3.2.3 Ethereum	37
3.2.4 Záverečné porovnanie	40
Záver	41
Zoznam použitej literatúry.....	42

Úvod

Kryptomenami nazývame digitálne meny, ktoré využívajú ako systém šifrovania kryptografiu. Kryptografia je typ šifrovania, ktorý znemožňuje subjektu čítať údaje, ku ktorým nemá heslo. Bezpečnosť kryptomien závisí od viacerých faktorov. Práve kryptografia ich vytvára takmer nesfalšovateľnými.

Svet zaznamenal mnoho pokusov o vytvorenie digitálnych mien už pred bitcoinom. Žiadna z nich ale nezaujala do takej miery, aby sa daná mena presadila či už na finančných alebo investičných trhoch. Prvá stránka, ktorá je do dnes domovskou stránkou bitcoinu - známa ako bitcoin.org vznikla v roku 2008. Dňa 31. októbra 2008 bola uverejnená práca, ktorá objasnila koncept technológie s názvom blockchain a tiež opísala fungovanie bitcoinu. Práca bola uverejnená autorom, ktorý je do dnes považovaný za zakladateľa bitcoinu, je známy pod falošným menom Satoshi Nakamoto. Nie je známe, kto sa pod týmto menom skrýva.

Prvá kryptomena s názvom bitcoin bola sprístupnená začiatkom roka 2009. Satoshi Nakamoto spustil ťažbu kryptomeny vytážením prvých 50 bitcoinov. V tomto období o bitcoine vedelo iba pár ľudí.

Zo začiatku nebolo možné kryptomene udávať hodnotu. Prvou uskutočnenou transakciou si softvérový vývojár László Hanyecz kúpil 2 pizze za 10 000 bitcoinov. Práve táto transakcia bola veľmi dôležitým momentom pri zrode kryptografického ekosystému.

Koncom roka 2010 bola uverejnená posledná správa týkajúca sa vtedy aktuálnej verzie bitcoinu. Uverejnil ju Satoshi Nakamoto, ktorý neskôr zostal v kontakte s niekoľkými vývojármi. Od apríla 2011 o ňom nikto nič nevie.

Akonáhle zaznamenal bitcoin prvotný úspech, v roku 2011 sa začali objavovať alternatívne kryptomeny tiež známe ako altcoiny. Altcoiny boli prioritne vytvárané za účelom vylepšenia bitcoinu. Mnoho z nich v porovnaní s bitcoinom dosahovalo vyššiu rýchlosť transakcií, výraznejšiu anonymitu a tiež efektívnejšie šifrovanie. V dnešnom svete sú známe tisíce kryptomien.

Začiatkom 2013 hodnota bitcoinu bola prvýkrát v histórii vyššia ako 1 000 dolárov. Bol to veľký skok, po ktorom hodnota kryptomeny opäť výrazne klesla a stagnovala. Práve výrazný prepád spôsobil negatívne ohlasy užívateľov a investorov, ktorí zaznamenali veľké straty. Práve kvôli negatívnym ohlasom sa ale bitcoin stal ešte populárnejší.

V roku 2014 bola najvýznamnejšou burzou kryptomien Gox. Burza bola napadnutá hackermi, ktorí ukradli 850 000 bitcoinov. Do dnes nie je známe, kto stál za útokom a ani kde bitcoiny skončili. Práve kvôli nevystopovateľnosti kryptomien sa začali v obrovskom meradle využívať na čiernom trhu.

Dnes už známa kryptomena ethereum bola spustená v roku 2015. Ethereum zaviedol inteligentné zmluvy, ktoré umožňujú vytvárať decentralizované aplikácie so širokým využitím. Mnoho investorov považuje projekt ethereum za veľmi užitočnú inováciu. Práve ethereum umožnilo spustenie mnohých projektov. Priaznivci kryptomien mohli kupovať mince za účelom investície, ale tiež tým mohli podporiť prebiehajúce projekty. Mnohé z projektov boli ale Ponziho schémy. Projekty, ktoré pretrvali, umožnili vytvorenie užitočných produktov.

Neustále sa zvyšoval počet krypto búrz, ktoré uľahčovali ich nákup a predaj. Celý systém začal výrazne rásť a stával sa stále populárnejším. V roku 2018 trhová kapitalizácia kryptomien presiahla 800 miliárd dolárov. Takto rýchly rast ale nebol udržateľný, hodnoty jednotlivých coinov začali klesať a mnohé projekty sa začali rúcať. Projekty, ktoré sa dokázali vysporiadať so všetkými problémami sa stali silnejšími.

V bakalárskej práci analyzujem a porovnávam z hľadiska využitia do budúcnosti kryptomeny, ktoré sú v dnešnom svete považované za tie s najväčším potenciálom. Medzi tieto kryptomeny patria bitcoin, ethereum a cardano, ktoré sa technológiu a možnosťou vytvárať decentralizované aplikácie podobá ethereu.

1 Teoretické vymedzenie problematiky

1.1 Blockchain

Blockchain je možné chápať ako verejnú knihu alebo databázu záznamov o transakciách. Táto databáza záznamov je udržiavaná a zároveň distribuovaná celosvetovou sieťou počítačov. Každá nová transakcia musí byť overená a informácia, ktorá je raz v tejto databáze zapísaná, sa už nedá vymazať. Blockchain má v sebe záznam o každej uskutočnenej transakcii. Na rozdiel od bánk, na záznamy dohliada značná skupina ľudí a nikto nad nimi nemá kontrolu. Inak povedané blockchain sa distribuuje medzi používateľov softvéru. Je preto nemožné získať kontrolu nad sieťou jednou centrálnou entitou. Blockchain je založený na decentralizovanej sieti, čo znamená, že funguje ako peer to peer. V praxi, ak ktokoľvek zrealizuje transakciu, transakcia postupuje do siete, kde algoritmy určujú jej legitímnosť. V prípade, že sa transakcia preukáže ako pravá, transakcia sa prepojí s predchádzajúcou transakciou a následne sa vytvorí reťazec transakcií, ktorý sa nazýva blockchain. Pri každej transakcii sa predchádzajúci vlastník podpisuje tzv. podpisovým kľúčom, ktorý je tajný (Bartoletti, Pompianu, 2017).

1.2 Vysvetlenie transakcií vo všeobecnosti

Podpisový kľúč zodpovedá adrese hash transakcie, v ktorej bitcoiny dostal a adrese ďalšieho vlastníka. Bitcoin je tvorený súborom transakcií. V tomto súbore odkazujú jednotlivé transakcie na tie predchádzajúce. V teoretickej rovine je pre tieto transakcie možné mať viacero vstupných a výstupných adries. V prípade, že chce vlastník bitcoiny odoslať, musí uviesť odkiaľ prišli. Transakcie sú z časového hľadiska zoradené do blokov. Každý blok odkazuje na predchádzajúci a tým sa ich legitímnosť ešte zvyšuje. Existuje tzv. reťazec blokov, ku ktorému je možné sa dostať. Preto, ak sa vlastník pokúsi previesť napríklad bitcoin, ktorý už previedol, je možné zistiť, ktorá transakcia bola vykonaná skôr (Zhang, Zhou, Liu, Xu, 2021).

1.3 Pojmy

Genesis Block - je úplne prvý blok v reťazci blokov ľubovoľnej digitálnej mince (US Sentencing Commission, 2018).

Súkromný kľúč – je neverejný údaj. Súkromný kľúč oprávňuje previesť/minúť kryptomenu digitálnym podpisom. Súkromný kľúč je pri využívaní softvérovej peňaženky uložený v počítači. V prípade využívania webovej peňaženky sú súkromné kľúče uložené na serveroch. Tieto kľúče nemôžu byť odhalené, pretože umožňujú z danej peňaženky mínať kryptomeny (US Sentencing Commission, 2018).

Proof of work – predstavuje výsledok snahy ťažby kryptomien (US Sentencing Commission, 2018).

Verejný kľúč - adresa bitcoinu - reťazec písmen a čísel. V prípade hashovania verejného kľúča privátnym kľúčom digitálne podpisuje transakciu (US Sentencing Commission, 2018).

Satoshi – bitcoinový „cent“. 1 bitcoin = 1 000 000 satoshi (US Sentencing Commission, 2018).

Hash - je matematická funkcia, ktorá na základe spracovania informácií vytvára stručný kód, pomocou ktorého je možná identifikácia, hash je teda unikátny. Hash môže byť vytvorený iba 1 zoskupením informácií. Dve takéto zoskupenia nemôžu vytvoriť identický hash. Hashom sa dá dokázať, že dané zoskupenie dát nebolo menené. Hash je veľmi dôležitý prvok ťažby bitcoinov, pretože je súčasťou každého nového bloku, ktorý bol vytážený. Súčasťou každého takéhoto bloku je ale aj hash predchádzajúceho bloku. Blok je potom podstatne ťažšie hacknúť/ovládať (US Sentencing Commission, 2018).

Hash rate - je základná MJ výpočtového výkonu bitcoinovej siete (US Sentencing Commission, 2018).

Mining - Ťažba bitcoinov je decentralizovaný proces, ktorý vyžaduje najmä výpočtový výkon. Je to proces matematických výpočtov, kde ide o potvrdzovanie transakcií a zvyšovanie bezpečnosti. V tomto procese môže prakticky ktokoľvek pridať blok transakcií bez potreby povolenia akejkoľvek inštitúcie či orgánu. Minery si za vytáženie bitcoinu môžu účtovať transakčné poplatky a tiež vytážený bitcoin. Ťažba je ale veľmi zložitý proces, ktorý sa komplikuje zároveň s hashovacím výkonom siete. V praxi to znamená, že čím je väčší výpočtový výkon, tým väčší výkon potrebuje aj človek, ktorý sa snaží o presadenie kontroly siete. Systém funguje dobre, až kým entita alebo väčšia skupina nemá pod kontrolou príliš hashovacej sily. Ak by k tomu došlo, entita alebo skupina môže mať pod kontrolou rôzne aspekty systému. Momentálne je veľká väčšina

blokov ťažená „poolmi“ a v prípade, že sa pripojí niekoľko poolov zároveň, môžu vykonávať zmeny a presadzovať kontrolu nad sieťou (Bohdan, 2019).

1.4 Výhody a nevýhody kryptomien

Ohľadom budúcnosti kryptomien sa názory pomerne rozchádzajú. Delia sa prevažne na dve skupiny. Liberálni podporovatelia moderných technológií sú veľmi optimistickí a v kryptomenách vidia budúcnosť. Táto skupina ľudí sa zameriava na jednoduchosť a bezpečnosť transakcií elektronickej meny. Prevody kryptomien sa realizujú za minimálne poplatky. Viaceré krajiny, ktoré sa snažia zbaviť sa hotovosti prejavili tiež veľmi optimistický postoj k tejto digitálnej mene. Na druhej strane ekonómovia a vedci sú v tomto smere veľmi skeptickí. Špecialisti v obore sa obávajú používania digitálnej meny vo svete financií. Hlavné dôvody ich neistoty sú vysoká volatilita a tiež fakt, že kvôli zložitému šifrovaniu a možnej anonymite transakcií sú kryptomeny veľmi často využívané na čiernom trhu (Bunjaku, Gjorgieva-Trajskovska, Miteva-Kacarski, 2018).

1.5 Cardano

Cardano bolo spustené v roku 2015 Charlesom Hoskinsonom a Jerryom Woodom. Práve Charles Hoskinson bol spoluzakladateľom veľmi známej kryptomeny ethereum. Neskôr sa stal generálnym riaditeľom nadácie práve tejto kryptomeny. Keď bolo cardano spustené, absolútny počet ADA tokenov bolo stanovených na 45 miliárd. Tvorcovia a investori si počas prvého obdobia rozdelili 31,11 miliardy tokenu ADA. Ostatných 13,89 miliardy tokenu ADA bolo prenechávaných investorom postupom rokov (Grayscale Investments, 2021).

1.5.1 Konkurencia

Cardano sa chce výrazne odlíšiť od konkurenčných blockchainov dôrazom na vykonávanie správnych krokov hneď na prvýkrát. Cardano chce tento cieľ dosiahnuť využitím rôznych výskumov, formálnym overovaním súkromia a systémom peer-revie. Hlavné ciele kryptomeny môžu aj za jej najväčšie nedostatky, medzi ktoré patrí najmä neistota fungovania decentralizovaných aplikácií, kvôli nedostatku inteligentných kontraktov z historického hľadiska. Navzdory pochybnostiam sa cardano stalo tretou najväčšou kryptomenou s prekonaním hodnoty výšky celkových transakcií v hodnote 1,6 bilióna USD (Grayscale Investments, 2021).

1.5.2 Smart kontrakty

Na inteligentných kontraktoch sa v súčasnosti vykonávajú rôzne testy, na základe ktorých sa budú ďalej vyvíjať decentralizované aplikácie. Existuje naozaj mnoho faktorov, ktoré môžu ovplyvniť vývoj cardana. Napríklad v prípade, že sa na serveri rozbehnú nové tokeny alebo decentralizované aplikácie, držitelia ADA ju môžu presunúť do týchto aktív. Z veľkej časti sú to ale práve investori, ktorí rozhodnú, či cardano dosiahne dlhodobý úspech. Či už ako systém decentralizovaných aplikácií alebo ako cloudová platforma. Burza práve týchto krypto platforiem je stále väčšou príležitosťou. Dnešné cloudové systémy ako napríklad Microsoft Azure, Google Cloud, Alibaba Cloud alebo iné zožali tiež veľký úspech. V prípade, že sa cardanu podarí dosiahnuť účel jeho vzniku, má naozaj veľkú šancu tvoriť výraznú časť celej cloudovej platformy v krypto svete (Mora, 2021).

1.5.3 Spustenie siete

Počiatočná forma cardana prostredníctvom siete bola spustená na prelome rokov 2015/2016. Vďaka protokolu známemu ako Ouroboros bolo možné cardano testovať v prostredí pod dohľadom odborníkov. Hlavným rozdielom medzi známymi kryptomenami je proces, akým sa počítače v sieti „zhodnú“ na vykonaní transakcie. Rozdiely v tomto procese sú spôsobené systémom, ktorý kryptomeny využívajú. Kryptomena cardano využíva Ouroboros tiež známy ako Proof of stake. Kryptomena bitcoin využíva Proof of work. Systém Proof of stake umožnil držiteľom ADA tokenov staking. Staking pracuje s objemom ADA tokenov a náhodne vyberá rady, ktoré majú výrazný vplyv na poradie transakcií v danej sieti. Bezpečnosť systému bola nezávisle overená na základe mnohých výskumov (Grayscale Investments, 2021).

1.5.4 Transakcie digitálnych aktív

Priemerný počet transakcií za deň stále rastie. Od roku 2021 vzrástol takmer 13-násobne na 115 000 transakcií za deň. Je veľmi pravdepodobné, že za tento rast môže príležitosť uskutočňovať transakcie s rôznymi digitálnymi aktívami (digitálne umenie, NFT...). Cardano sa od iných kryptomien odlišuje aj možnosťou obchodovať v jednej transakcii so širšou škálou aktív. Táto možnosť umožňuje investorom ušetriť na transakčných poplatkoch (Grayscale Investments, 2021).

1.5.5 Veľká základňa aktívnych používateľov

ADA má veľmi obsiahlu a výrazne rastúcu databázu investorov, resp. používateľov. Ak by sme chceli porovnávať aktívnych používateľov cardana a napríklad etherea, ethereum vyhráva cca 2,5-krát. Od júla aktívni používatelia etherea ubúdajú. Na druhej strane používatelia cardana pribúdajú. Aktuálna cena oboch kryptomien je veľmi nízka, zohráva tu ale výraznú úlohu situácia vo svete, cena plynu a podobne. Zaujímavá je tiež štatistika rozdielnej „hodnoty používateľa“ týchto dvoch kryptomien. Priemerná hodnota používateľa etherea je cca 55 000 USD, priemerná hodnota používateľa cardana je cca 30 000 USD. Toto porovnanie nám ukazuje, že cardano má oproti konkurencii stále nižšiu hodnotu. Mnoho investorov ale nemusí považovať túto štatistiku za relevantnú, môžu preferovať iné ukazovatele (Grayscale Investments, 2021).

1.5.6 Riadenie a financovanie

Kryptomena cardano má do budúcnosti mnoho plánov, a práve preto má vlastnú pokladnicu na ich financovanie. Pokladnica je momentálne spravovaná Cardano Foundation ale je možné, že bude mať nad ňou kontrolu sieť Voltaire. V budúcnosti má totiž táto sieť prejsť upgradom a to premenou cardana na samostatne autonómny distribuovaný systém organizácie (DAO). Aktuálne sa v pokladnici nachádza cca 585 miliónov ADA. Hodnota kryptomeny je nestála, a preto nebudem písať prepočet v dolároch (Grayscale Investments, 2021).

1.5.7 Vývoj

Vývoj cardana sa dá rozdeliť do 5 významných krokov:

- foundational (Byron) – fáza zameraná na spustenie cardana, umožniť investorom nákup a predaj,
- decentralization (Shelley): fáza zameraná na decentralizáciu pomocou Ouroboros PoS, ADA bude schopná odmeňovať investorov,
- smart contracts (Goguen) – súčasná fáza zameraná na spustenie možnosti inteligentných zmlúv kvôli možnosti vytvárania decentralizovaných aplikácií,
- scaling (Basho) – súčasná fáza zameraná na zlepšovanie interoperability a škálovateľnosti zavedením paralelných účtovných štýlov a bočných reťazcov.

V budúcnosti je naplánované zavedenie hlasovania a správy pokladnice používateľmi, ktoré z Cardana urobia plne komunitno-riadenú distribuovanú autonómnou organizáciu (Grayscale Investments, 2021).

1.5.8 Výhody

Cardano má síce jedinečnú technológiu a mechanizmus, ale zahŕňa aj prvky z iných sietí, ktoré sú dôležité. Medzi jeho najvýznamnejšie prednosti možno zaradiť nasledovné aspekty:

- zakladateľom je známy Charles Hoskins,
- zastúpenie výraznej skupiny ľudí potrebnej pre úspech akéhokoľvek open-source programu,
- úplná decentralizácia ADY spolu s novinkou Shelly,
- jednoduchá kúpa a predaj prakticky na každej krypto-burze,
- dostatočná rezerva v pokladnici (Grayscale Investments, 2021).

1.5.9 Potenciálne riziká

Cardano čelí tiež množstvu rizík:

- sile konkurentov, či už v systéme šifrovania (blockchain) alebo smart-kontraktov (solana, ethereum),
- nedávno nastalo spustenie možnosti inteligentných zmlúv, ale cardano ešte stále nemá žiadnu mainnetovú aplikáciu, uvidí sa ako budú fungovať decentralizované aplikácie v spolupráci s používateľmi,
- nízke poplatky cardana v porovnaní s konkurenciou, ak ich kryptomena nezvýši, je otázne, či rezerva cashflowu bude postačujúca,
- v právnom smere cardano môže v budúcnosti čeliť rôznym regulátorom (ako napr. bitcoin),
- je možné, že kryptomena bude v budúcnosti čeliť problémom bezpečnosti, technickým problémom alebo iných nedostatkom protokolu, v najhoršom variante sa môže stať, že sieť bude nezabezpečená (Grayscale Investments, 2021).

1.6 Bitcoin

Bitcoin bol prvýkrát spustený v roku 2009. Od tohto významného momentu pre svet kryptomien ich vzniklo naozaj veľké množstvo. Mnoho z nich bolo pôvodne spustených pre širokú škálu transakcií, či už na komerčných alebo online trhoch. Bitcoin a teda aj ostatné kryptomeny vyvinuté na tento účel zaujali nielen zložitou technológiou šifrovania – blockchainom, ale tiež ich vysokou volatilitou a možnosťou ich využitia na čiernom trhu či pri praní špinavých peňazí. Takmer neobmedzené možnosti kryptomien na čiernom trhu spôsobili rozličné reakcie nadnárodných organizácií a ministerstiev. Z dôvodu, že kryptomeny na čele s bitcoinom nepodliehali mnohým regulátorom, bolo mnoho oficiálnych pokusov ich zakázať. V oblasti digitálnych transakcií a búrz sú nestále pokusy o začlenenie prvkov blockchainu, ktoré majú praktické využitie práve v krypto-sfére. Najmä snaha o bližšie spoznanie technológie blockchainu a jeho využitie v rôznych odvetviach spájajú sily vedcov z rôznych oblastí (Campbell-Verduyn, 2018).

1.6.1 Porovnanie s dnešným bankovým systémom

Na rozdiel od spomínaného systému dosahuje dnešný bankový systém ochranu súkromia prostredníctvom tretej strany. V mnohých prípadoch nevyhnutnosť zverejňovať a uchovávať informácie o transakciách obmedzuje, prípadne až vylučuje anonymitu. Možnosť zachovať súkromie je možná v prípade, že všetky verejné kľúče sú anonymné. Verejnosti je v tomto prípade známe, že subjekt posielal sumu inému subjektu. Neexistujú ale žiadne informácie, ktoré by transakcie s niekým spájali. V prípade takzvaného multivstupu sa určitému úniku informácií vyhnúť nedá. Riziko spočíva v odhalení vlastníka kľúča. Toto odhalenie by mohlo spôsobiť zistenie veľkého množstva informácií o ďalších transakciách (Campbell-Verduyn, 2018).

Bol predstavený potenciálny systém pre transakcie, ktoré sú uskutočňované elektronicky. Elektronická minca, ktorá je založená na databáze digitálnych podpisov má riziko jej dvojitého minutia. Aby sme tomuto riziku zabránili, je navrhnutá sieť peer-to-peer založená na proof-of-work, ktorá ukladá históriu transakcií. V prípade, že väčšinu výkonu ovláda CPU a nie organizovaná skupina, systém funguje (Campbell-Verduyn, 2018).

1.6.2 Zhrnutie

Kryptomena bitcoin je digitálne aktívum. Je navrhnutá tak, aby ju bolo možné využívať ako prostriedok výmeny. Bitcoin využíva kryptografiu na zabezpečenie transakcií, na kontrolu vytvárania ďalších jednotiek a na overenie prevodu aktív. Bitcoin a jeho deriváty využívajú na rozdiel od centralizovaných elektronických peňazí a systémov centrálného bankovníctva decentralizovanú kontrolu nad systémom. Decentralizovaná kontrola súvisí s využívaním databázy blockchain transakcií bitcoinu v úlohe distribuovanej účtovnej knihy. Pri bitcoine je každá transakcia prevodom určitej hodnoty bitcoinu medzi účastníkmi a každá transakcia je zaznamenaná na blockchaine bitcoinu. Decentralizovaná kryptomena je produkovaná celým systémom kryptomien kolektívne, rýchlosťou, ktorá je definovaná pri vytváraní systému a ktorá je verejne známa. V centralizovaných bankových a ekonomických systémoch, ako sú predstavenstvo spoločností alebo vlády, kontrolujú dodávky meny tlačením jednotiek, alebo požadovaním dodatkov do účtovných kníh digitálneho bankovníctva. V prípade decentralizovanej kryptomeny nemôžu spoločnosti alebo vlády produkovať nové jednotky. Doteraz neposkytli podporu pre iné firmy, banky alebo korporácie, ktoré majú v držbe meranú hodnotu aktív (Gurusamy, Darshak, 2018).

O bitcoine sa vo všeobecnosti hovorí aj ako o decentralizovanej digitálnej mene. Objavujú sa ale dôležité, doposiaľ nezodpovedané otázky:

- Ktorá vláda so silnou ekonomikou túto digitálnu menu podporuje?
- Kto a ako sa budú pri bitcoine určovať úrokové sadzby?
- Môže byť pri mene akceptovateľná tak extrémna volatilita, akú si všímame pri bitcoine?

Práve kvôli týmto otázkam, ktoré sú z hľadiska budúcnosti kryptomeny strategické, sa o nej budeme radšej vyjadrovať ako o elektronickom aktíve.

1.6.3 Ako sa bitcoiny ukladajú?

Vlastníctvo bitcoinov sa zaznamenáva na blockchain. bitcoiny sú spojené „bitcoinovými adresami“. Bitcoiny samotné sa neukladajú. Dôležité kľúče, ktoré sú potrebné na uskutočňovanie platieb, sú uložené v „peňaženkách“. Peňaženky sú aplikácie, ktoré spravujú dôležité informácie ako napríklad kľúče, adresy a tiež platby. Bitcoinová

adresa je podobná číslu bankového účtu, samozrejme s rozdielmi (Mueller, Bergsträsser, Rizk, Steinmetz, 2018).

1.6.4 Čo sa stane, keď uskutočním platbu bitcoinom?

Pri platbe resp. transakcii uskutočnenej bitcoinom sú určité kroky, ktoré je potrebné si všimnúť.

1. Aké bitcoiny sa posielajú?
2. Z akej adresy sa posielajú?
3. Z akej adresy sa posielajú Validátorom?

Hneď ako prvý počítač dostane pokyn, skontroluje technické detaily a detaily obchodnej logiky (napr. Pokúša sa moja platba vytvoriť bitcoiny z ničoho? Boli odosielané mince už minulé, resp. odoslané inam?). Ak transakcia testami prejde, spustí sa reakcia. Počítač ich odovzdá ostatným v sieti, z ktorých každý vykoná rovnaké overovacie testy. Overovanie je založené na tom, že si v tejto sieti počítače navzájom nemôžu „dôverovať“. Musia byť teda vykonané rovnaké testy. Ku koncu overovania platby sa transakcia objavuje ako „nepotvrdená“ na všetkých počítačoch v sieti a na všetkých obrazovkách všade na svete. Transakcia je nepotvrdená z dôvodu, že aj keď bola platba overená, ešte nie je zapísaná v účtovnej knihe (Mueller, Bergsträsser, Rizk, Steinmetz, 2018).

1.7 Ethereum

Ethereum je v poradí druhá najväčšia a najvýznamnejšia kryptomena. Z hľadiska trhovej kapitalizácie predstavuje cca 14% celkového trhu s kryptomenami, čo znamená, že je hneď za bitcoinom. Cieľom etherea je vytvoriť nové peer-to-peer aplikácie. Je to veľký rozdiel v porovnaní s konkurenčným bitcoinom, ktorého snahou je vytvorenie peer-to-peer elektronického systému. Na úvod je veľmi dôležité rozlíšenie éter (ETH) od etherea. Ethereum označuje blockchainovú platformu. Táto platforma funguje na princípe open-source decentralizovanej blockchain technológii a pracuje s programami a aplikáciami bez požitia centralizovanej strany. Éter je označenie pre konkrétnu kryptomenu, ktorá sa používa na blockchaine (Wisdomtree, 2019).

1.7.1 Decentralizované aplikácie Ethereum

Decentralizované aplikácie (dApps) sú výrazne podporované smart contract protokolom. Na realizáciu prevodu hodnoty informácií (napr. peňazí, hlasovacieho práva, majetku) sa vykonávajú transakcie typu peer-to-peer. Tieto transakcie prebiehajú vďaka skupinovému výkonu distribuovanej siete. Fungovanie kryptomeny ethereum môžeme prirovnať k „počítaču“ na blockchaine, kde pevným diskom stroja je základná blockchain technológia. Jednotlivé programy predstavujú smart kontrakty a používatelia platia za využitie počítača kryptomenou ethereum (Wisdomtree, 2019).

1.7.2 Ako ethereum funguje?

Jadrom etherea sú smart kontrakty. Inteligentné zmluvy sú jedným z dvoch typov účtov etherea, v ktorých sú spísané pokyny systému. Vývojár Nick Szabo často porovnával koncept s kódmi predajných automatov. Pri kryptomene sa inteligentná zmluva spustí transakciou. Pri predajnom automate táto transakcia predstavuje vloženie mince kupujúcim. Pri kryptomene sa po spustení inteligentnej zmluvy vykonávajú transakcie na základe podmienok „ak...tak..“. Opäť v prípade automatu si konkrétny tovar, ktorý si kúpime, môžeme predstaviť ako výsledok inteligentnej zmluvy na sieti etherea. Tento výsledok inteligentnej zmluvy môže predstavovať napríklad ako prevod etherea na iný účet, alebo ako transakciu, ktorá predchádza spusteniu ďalšej inteligentnej zmluvy. Inteligentná zmluva funguje na základe preddefinovaného súboru pravidiel, ktoré jej umožňujú spúšťať kód rovnakým spôsobom na ľubovoľnom uzle v sieti etherea. Práve táto funkcionálna eliminuje potrebu zásahu tretej strany, čím sa kryptomena stáva decentralizovanou (Wisdomtree, 2019).

1.7.3 Gas

Poplatok, ktorý je potrebné zaplatiť ťažiarom, sa nazýva gas. Cena gasu je malý zlomok ETH. Tento zlomok sa označuje v jednotkách Gwei (prepočet 10⁹ Gwei = 1 ETH). Gas je nevyhnutný na udržanie siete Ethereum. Poplatok predstavuje odmenu baníkov za spracovanie a overovanie transakcií. Poplatok gas za transakciu je ekvivalentný hodnote kryptomeny, k nemu je ešte pripočítaný transakčný poplatok. Cena gasu má určitú volatilitu na základe ponuky a dopytu po spracovateľskom výkone. Ťažiari sa môžu rozhodnúť nespracovať transakcie, keď sú ceny gasu príliš nízke. Gas má ďalšiu dôležitú

funkciu a to predchádzanie neúmyselného plytvania energiou. Ethereum je turingovo kompletné, a preto existuje možnosť, že program bude bežať neobmedzene dlho a transakcia môže spotrebovať veľmi veľa energie. Limit gasu je stanovený ako maximálna cena, ktorú sú používatelia ochotní zaplatiť za transakciu. Keď sa minie gas, program sa ukončí a nespotrebuje sa žiadna ďalšia energia (Shariyah Review Bureau, 2022).

1.7.4 Porovnanie s bitcoinom

Keďže kryptomena ethereum je inšpirovaná blockchainovým rámcom bitcoinu, kryptomeny zdieľajú základný blockchain. Obe sú decentralizované, verejné a nemenné. Existuje ale mnoho rozdielov medzi ethereum a bitcoinom. Systém bitcoinu je viac definovaný a rigidnejší, pretože sa zameriava na prípad použitia kryptomeny. Systém ethereum je niečo flexibilnejší a prístupnejší. Systém sa tiež neustále vyvíja, keďže jeho vývoj závisí od vybudovania rozsiahlej siete aplikácií. Ethereum vytvára príležitosť narušiť zaužívané systémy odstránením sprostredkovateľov a maximalizáciou efektívnosti. Jeho inovácie majú naozaj veľký potenciál získať výrazný vplyv vo svete.

2 Cieľ práce a metódy spracovania

Hlavným cieľom bakalárskej práce je na základe detailnej analýzy identifikovať kryptomenu, ktorá má najväčší potenciál využitia v budúcnosti. Porovnali sme kryptomeny bitcoin, ethereum a cardano. V prvom rade sme sa zamerali na sumarizáciu poznatkov z oblasti. Na základe vybraných faktorov sme potom porovnali dané kryptomeny z hľadiska potenciálu stať sa v budúcnosti finančným aktívom, resp. uznávanou menou. Pre komplexnejší pohľad sme vykonali tiež porovnanie kryptomien z hľadiska ich investičného potenciálu. Na základe spomenutých dvoch porovnaní sme vybrali konkrétnu kryptomenu, ktorá má z dlhodobého hľadiska najväčší finančný a tiež technologický potenciál.

Pri práci s vybranou problematikou bakalárskej práce sme postupovali nasledovne.

Problematika kryptomien je skutočne rozsiahla. Na jej kompletne spracovanie sme využili primárne a tiež sekundárne údaje, ktoré boli čerpané prevažne z vedeckých článkov od zahraničných autorov.

V rámci teoretickej časti práce sme pomocou analýzy systematicky zhromaždili informácie o danej problematike.

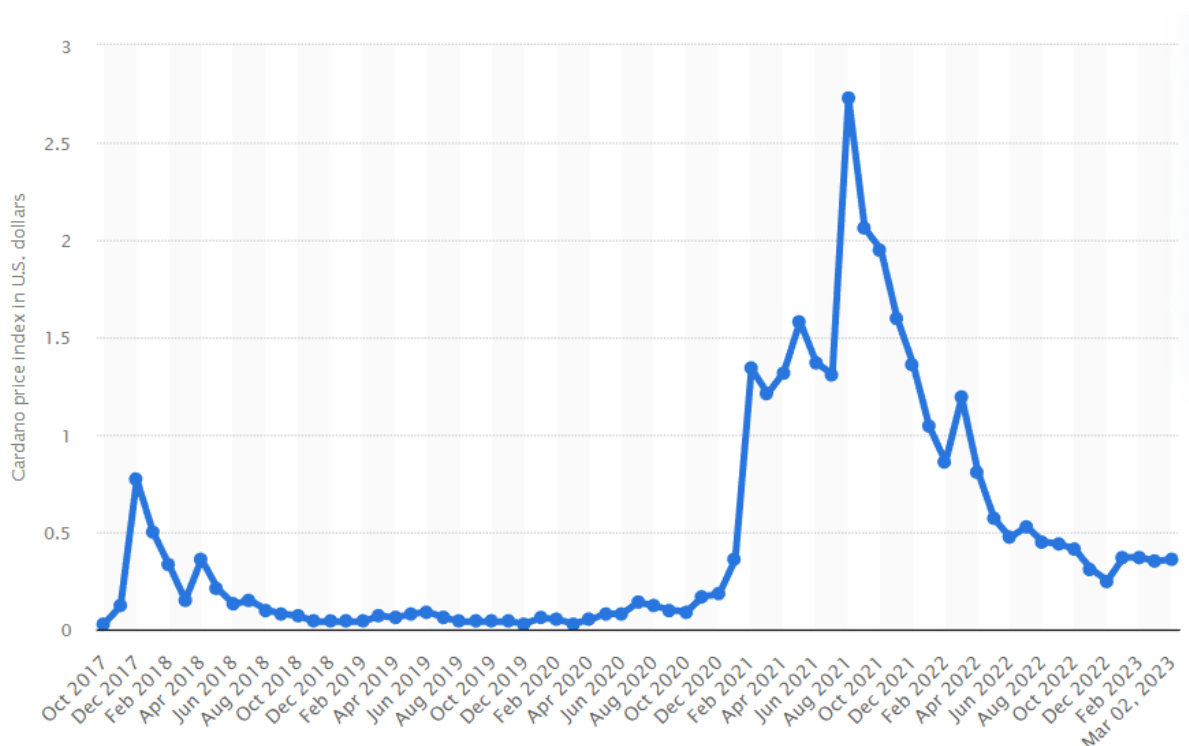
Dominantou metódou spracovania praktickej časti bakalárskej práce je komparácia. Vykonali sme syntézu a analýzu vybraných faktorov daných kryptomien. Pomocou komparácie sme identifikovali rozdiely medzi jednotlivými kryptomenami z hľadiska ich technológie, zamerania, celkových cieľov a iných strategických faktorov. Použili sme tiež logické metódy skúmania – indukcie a dedukcie za účelom spracovania, analýzy a interpretácie výsledkov. Výsledky hodnotenia kryptomien sú za účelom lepšej efektivity zobrazené v tabuľkách.

3 Porovnania kryptomien a výsledky práce

3.1 Porovnanie kryptomien z hľadiska potenciálu finančného aktíva

3.1.1 Cardano

Cardano volatilita



Obrázok 1: Vývoj ceny cardana v čase

Zdroj: www.statista.com

Na grafe je zobrazená hodnota Cardano v závislosti od času. Po spustení kryptomeny nastal výrazný vzostup jeho ceny, ktorá bola najvyššia na prelome rokov 2017 a 2018. Následne jeho hodnota klesla a od konca roka 2018 až po koniec roka 2020 sa držala na minime. Začiatkom roka 2021 sa opäť spustil výrazný rast kúpnej resp. predajnej ceny kryptomeny, ktorý dosiahol v auguste 2021 historické maximum v hodnote 2,73 dolára. V priebehu 7 mesiacov hodnota cardana klesla na 0,86 dolára, čo znamená prepád o 68,5%. Aj napriek miernym nárastom má kryptomena aktuálne (marec 2023) hodnotu 0,36 dolára. Vzhľadom k požadovanej konzistentnej hodnote (nízkej volatilite) meny je prepád 68,5% v priebehu 7 mesiacov pre mnohých veľkým otáznikom.

Cardano využiteľnosť

Ako je už v opise kryptomeny spomenuté, medzi hlavné využitia cardana patrí vytváranie inteligentných zmlúv a následne decentralizovaných aplikácií a protokolov. Tiež umožňuje okamžite odosielať a prijímať finančné prostriedky za nízke poplatky. V praktickej rovine cardano umožňuje písanie a realizáciu smart kontraktov. Napríklad, ak ľudia vymenili peniaze za akcie, technológia cardana je schopná vykonať transakciu a zaznamenať peniaze a tiež vlastníctvo akcií v blockchaine. V dnešnej podobe je cardano možné využiť ako špekulatívnu investíciu, využívať ho na špecifické nákup a tiež je možné ho vymieňať. Je možné ho využiť aj na staking, teda získanie viac tokenov. Ak ale niekto chce cardano držať dlhodobo, je dôležité dať naozaj veľký pozor na výber peňaženky (Rodeck, Curry, 2023).

Cardano rýchlosť spracovanie transakcie

Cardano dosahuje jednu z najvyšších rýchlostí spracovania transakcií. Je schopné spracovať viac ako 250 transakcií v jednej sekunde (TPS). Tento faktor spôsobuje, že sieť kryptomeny je veľmi škálovateľná (Choudhury, 2022).

Cardano bezpečnosť

Mnohí ľudia považujú za významný prvok bezpečnosti siete uvedenie mainnetovej Ouroboros Pos formy spolu s aktualizáciou nazývanou Shelley. Tento významný krok podstúpilo cardano v roku 2020, v júli (Kondratiuk, Seijas, Nemish, Thompson, 2021).

Cardano možnosť stakingu

Ďalšia z výhod cardana je jeho možnosť stakingu. Staking znamená, že kryptomena ponúka možnosť investorom „pasívne zarábať“. Staking generuje úroky z investorom držaného cardana. Investori majú možnosť stakingu tokenov ADA vo viac ako 2400 stakingových pooloch. Fondy sa odlišujú v mnohých vlastnostiach, napríklad vo výške úrokov a pod. Jednotlivé pooly tvoria obrovskú cloudovú sieť. Táto sieť sa riadi predpismi, ktoré sú dané protokolom cardano. Jednotlivé pooly dostávajú tokeny ADA, ktoré sú získané z transakčných a iných poplatkov. Tieto tokeny dostávajú ako protislužbu za pridanie sa do spoločného cloudu. Tokeny sú potom vyplatené investorom, ktorí využívajú staking. Táto neštandardná možnosť cardana – získavať tokeny z rôznych poplatkov, pridáva kryptomene ďalšiu výhodu. Je možné ju nazvať aj produktovým kapitálovým aktívom (Madelintwente, 2022).

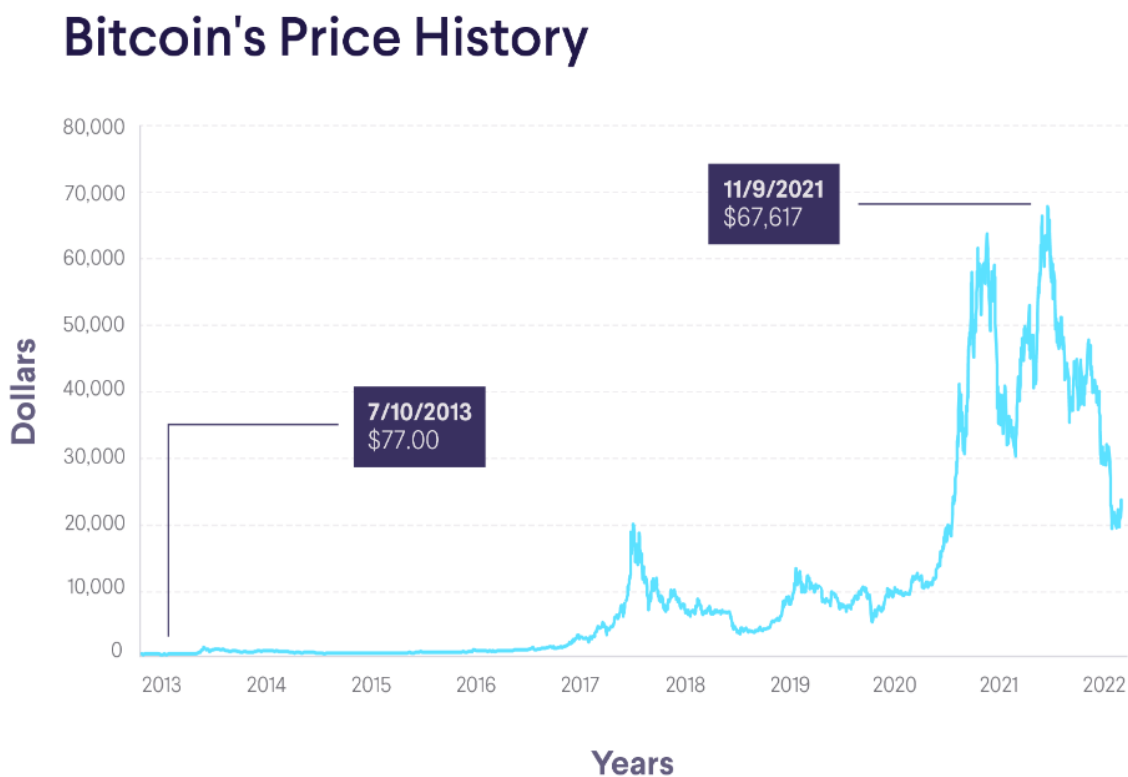
Cardano využitie v praktickej rovine

Cardano sa aj dnes využíva v prebiehajúcich projektoch. Medzi najznámejšie z nich v roku 2022 patria:

- 4.1 MinSwap (MIN),
- 4.2 SundaeSwap (Sundae),
- 4.3 MELD (MELD),
- 4.4 Cornucopias (COPI),
- 4.5 Empowa (EMP),
- 4.6 Djed (DJED),
- 4.7 Revuto (REVU), (Madelintwente, 2022).

3.1.2 Bitcoin

Bitcoin volatilita



Obrázok 2: Vývoj ceny bitcoinu v čase

Zdroj: www.sofi.com

Na grafe je zobrazená hodnota bitcoinu v závislosti od času. Graf nezobrazuje vývoj kryptomeny od úplného začiatku, pretože bitcoin bol spustený v roku 2009, kedy mal hodnotu 0 dolárov. Do roku 2013 sa jeho cena pohybovala v rozmedzí 1 až 80 dolárov. Hodnota bitcoinu zaznamenala prvý výraznejší vzostup na prelome rokov 2017 a 2018. Nasledoval výrazný pokles. Neskôr sa jeho hodnota s pomerne vysokou volatilitou pohybovala v rozmedzí 3 000 až 13 000 dolárov. Bitcoin zaznamenal extrémny rast hodnoty na prelome rokov 2020 a 2021, kedy sa len za 4 mesiace jeho cena vzrástla o vyše 500% (z 10 683 dolárov na takmer 57 000 dolárov). Nasledoval trojmesačný pokles hodnoty kryptomeny o polovicu. S menším prepadom v septembri roku 2021 sa jeho cena vyšplhala v novembri toho istého roku (2021) do výšky 64 940 dolárov, čo predstavuje historické maximum. Kryptomena zaznamenala ročný pokles o takmer 75%. Momentálne jeho hodnota kolíše na cca 20 000 dolároch. Opäť zaznamenávame vysokú volatilitu či už rastu alebo poklesu hodnoty kryptomeny. Vzhľadom na cieľ bitcoinu (stať sa menou) predstavuje tento faktor vysokej volatility veľkú neistotu.

Bitcoin využiteľnosť

Internetové transakcie boli dlhodobo sprostredkované skrz finančné inštitúcie. Mnoho z týchto platieb ale nebolo dostatočne zabezpečených pred útokmi hackerov. Pre mnoho inštitúcií, ktoré takéto platby sprostredkovali, to predstavovalo zbytočné náklady, ktoré sa transformovali do transakčných nákladov a nakoniec ich musel platiť konečný spotrebiteľ platformy. V tomto ohľade musia zodpovední pracovníci platform chrániť svojich zákazníkov. Danému percentu útokov sa ale zabrániť nedá. Práve týmto podvodom sa dá vyhnúť hotovosťou. Doposiaľ totiž nie je známy žiadny systém na sprostredkovanie platieb bez tretej strany (Gurusamy, Darshak, 2018).

Pre potreby ako sú vyššie spomínané, je nevyhnutný systém, ktorý je založený na prepracovanej technológii šifrovania. Pri tomto systéme by malo byť možné obom spotrebiteľom uskutočňovať medzi sebou obchodné transakcie bez potrebnej tretej strany. Takéto typy platieb, kde je storno takmer nemožné, by mohli chrániť spotrebiteľov rovnako ako poskytovateľov. Nižšie je rozobraté teoretické riešenie tohto problému prostredníctvom systému peer-to-peer. V prípade, že uzly kontrolujú najviac výkonu CPU (v porovnaní s inými skupinami), riešenie funguje (Gurusamy, Darshak, 2018).

Medzi hlavné faktory potenciálnej využiteľnosti bitcoinu v budúcnosti patria:

- transakcie - možnosť uskutočňovania transakcií od jedného subjektu k druhému bez ohľadu na jurisdikciu alebo geografickú polohu,
- používatelia - potenciálnymi používateľmi bitcoinu môžu byť subjekty alebo komunity, ktorým nie úplne vyhovuje momentálny finančný systém (nedostatočná obsluha bankami, nespoľahlivosť alebo zdržanlivosť),
- volatilita - negatívom z hľadiska meny, no pre investorov a špekulantov, ktorí hľadajú aktívum s potenciálom vysokého rastu môže byť práve bitcoin zaujímavý,
- konverzia – pre mnohých predstavuje nevýhodu, pretože ak chce investor bitcoin zameniť za iné aktívum, je potrebné si nájsť niekoho, kto je opačnú výmenu ochotný podstúpiť
- poplatky - bitcoin je často spomínaný ako extrémne nízko nákladové až bezplatné aktívum, pre komplexný pohľad je dôležité si uvedomiť a spočítať transakčné a konverzné náklady z prechodu zo svetových mien do bitcoinu a naspäť. (Gurusamy, Darshak, 2018).

Bitcoin rýchlosť spracovania

Bitcoinu trvá spracovanie transakcie priemerne 40 minút. Tento čas závisí od viacerých faktorov, napríklad od poplatkov, veľkosti bloku, blokovania a tiež sieťovej prevádzky. Transakcie pri konkurenčných kryptomenách ako napríklad cardano alebo solana, je možné spracovať takmer okamžite. Práve rýchlosť transakcie ukazuje, ktorá kryptomena je efektívnejšia. Pre bitcoin to teda predstavuje konkurenčnú nevýhodu (Gurusamy, Darshak, 2018).

Bitcoin bezpečnosť

Potenciálne elektronické platidlo môže byť definované ako databáza digitálnych podpisov je dôležité, aby sa tieto podpisy nedali mazať. Podstata šifrovania je v tom, že aktuálny majiteľ prevedie napr. bitcoin na nového majiteľa digitálnym podpisom (hashom). Nový vlastník napr. bitcoinu má možnosť tieto podpisy (hashe) overiť. Nedostatok systému spočíva v tom, že nový vlastník bitcoinu nevie s určitosťou zistiť, či daná minca už nebola minutá. Ideálnym riešením v tomto prípade by bolo zaviesť centrálu, ktorá by mala pod dohľadom všetky takéto transakcie. Bolo by možné zamedziť takémuto dvojnásobnému mŕňaniu a podobným podvodom. Na druhej strane problém by bol, že celý

takto vytvorený systém by závisel od jednej centrály. Je nevyhnuté prísť pri takomto systéme meny na spôsob, ako si môže prijímateľ platby overiť, že platba nebola skôr podpísaná. Vo svete kryptomien sa považuje za legitímnu práve skoršia transakcia. Ďalšie pokusy sú z hľadiska legitímnosti irelevantné. Pre kompletnú informovanosť oboch strán je potrebné, aby boli transakcie verejne oznámené, mali verejnú chronologickú históriu a dôkazy, že všetky transakcie boli z hľadiska hashov legitímne. Potenciálne zvládnutie problému overovania legitímnosti transakcie by mohlo spočívať v časových pečiatkach. Každá takáto pečiatka by mala obsahovať hash predchádzajúcej časovej pečiatky, ktorý je súčasťou reťazca. V prípade, že je CPU riadený legitímnymi uzlami, legitímny reťazec sa rozrastie najrýchlejšie. Ak by chcel niekto napadnúť takto vzniknutý reťazec, potreboval by zmeniť predchádzajúci blok a prejsť „testom“ každého ďalšieho bloku, až kým by nedobehol legitímne uzly. Dôležitým faktom ale je, že pravdepodobnosť sa s pribúdajúcimi blokmi výrazne znižuje. Táto náročnosť sa zvyšuje ešte viac v prípade, že sú bloky vytvárané frekventovane (Narayanan, Bonneau, Felten, Miller, Goldfeder, 2016).

Nová a teda prvá transakcia v konkrétnom bloku je stále tvorcom bloku. Táto transakcia spúšťa novú mincu, uzly a potrebnú podporu siete. Konštantný rast digitálnych mincí v obehu je priamo úmerný s klesajúcim počtom minerov. Za náklady sú v tomto prípade považované elektrina a vynaložený čas CPU. V prípade, že by niekto chcel tento systém napadnúť, musel by byť schopný ovládnuť sieť najväčším výkonom CPU. V tomto prípade má útočník dve možnosti. Mohol by buď zasiahnuť systém platieb a teda podviesť ľudí, alebo si môže sám vygenerovať digitálne mince. Na overenie platby stačí, ak má užívateľ hlavičky blokov reťazca proof-of-work. Je dôležité, aby bol tento reťazec najdlhší. Opäť ale platí, že overenie má výpovednú hodnotu iba, ak sieť ovládajú uzly, ktoré nie sú zmanipulované. V prípade, že je sieť napadnutá, môže útočník vymyslieť fake transakcie. Teoretická ochrana proti napadnutiu systému útočníkom by spočívala v systéme kontroly varovaní zo sieťových uzlov. Je tiež pravdepodobné, že spoločnosti, ktoré pracujú s danou technológiou na dennej báze, budú z dôvodu bezpečnosti a overovania riadiť prevádzku na vlastných uzloch (Narayanan, Bonneau, Felten, Miller, Goldfeder, 2016).

Bitcoin možnosť stakingu

Bitcoin funguje na princípe proof of work. V porovnaní napríklad s konkurenčným cardanom, ktoré funguje na princípe proof of stake. Práve toto je dôvod, prečo bitcoiny nie

je možné získavať využitím stakingu (Narayanan, Bonneau, Felten, Miller, Goldfeder, 2016).

Bitcoin využitie v praktickej rovine

V septembri 2021 sa stredoamerický štát Salvador stal prvým na svete, ktorý uznal bitcoin ako oficiálnu menu. Pre mnoho obyvateľov štátu to bol od začiatku zlý nápad. Pre prezidenta krajiny ale práve táto možnosť predstavovala riešenie, ako obísť prípadné sankcie USA a financovať projekty bez formalít týkajúcich sa medzinárodného menového fondu. Bol to ale nezáujem Salvádorčanov, ktorý zachránil krajinu pred krachom. Vo vládnej peňaženke má dnes 2 381 bitcoinov hodnotu o polovicu menšiu, ako bola ich kúpna hodnota. Experiment bol teda o rok neskôr označený ako jednoznačne neúspešný (Howson, 2022).

3.1.3 Ethereum

Ethereum volatilita



Obrázok 3: Vývoj ceny etherea v čase

Zdroj: www.crypto.com

Na grafe môžeme vidieť vývoj hodnoty etherea v závislosti od času. Od spustenia etherea sa držalo na úplnom minime až do roku 2017, kedy zaznamenalo prvé vzostupy. 8.

januára 2018 dosiahlo hodnotu 1 317 dolárov, kedy jeho hodnota za jediný mesiac stúpila viac ako trojnásobne. Nasledoval trojmesačný prepád, ktorý vyvrcholil v apríli 2018, kedy malo ethereum hodnotu 387 dolárov. Ďalej si môžeme všimnúť ešte jeden výraznejší vzostup a potom opäť pomerne volatilnú krivku, ktorá sa ďalšie takmer tri roky pohybovala v rozmedzí 100 až 300 dolárov. Nasledoval výrazný vzostup, ktorý vyvrcholil 10. mája 2021, kedy ethereum dosiahlo hodnotu 3 661 dolárov, kedy tiež v priebehu dvoch mesiacov stúplo viac ako dvojnásobne. Po výraznom vzostupe nasledoval mesačný pokles na takmer polovicu hodnoty. Po ďalších prudkých vzostupoch a zostupoch krivky, cena tejto kryptomeny historicky vyvrcholila 8. novembra 2021, kedy dosiahla hodnotu takmer 4 600 dolárov. Historicky najvýraznejší pokles začal 4. apríla roku 2022. Od tohto dátumu v priebehu ďalších dvoch mesiacov hodnota etherea klesla z 3 523 na 1 080 dolára. Pokles predstavuje pokles o takmer 70%. Volatilita, ktorú si všímame pri ethereu, dosahuje tiež veľmi výrazné skoky.

Ethereum využiteľnosť

Sieť etherea, ktorej podstatou je tiež blockchain bola predstavená v roku 2013. Sieť bola finálne vytvorená a obohatená o aktualizácie v roku 2015. Ako už vieme, základ decentralizovanej blockchain technológie je vytvorený bitcoinom. Jeho funkčnosť je ale obmedzená na elektronické peer-to-peer prevody financií. Práve toto obmedzenie rozširuje kryptomena ethereum o programovateľné aplikácie (Crypto.com, 2023).

Ethereum rýchlosť spracovania

Čo sa týka rýchlosti spracovania transakcií, ethereum je momentálne schopné spracovať cca 30 transakcií za sekundu. Nová verzia etherea (ethereum 2.0) by mala byť schopná spracovať 100 000 transakcií za sekundu, čo je naozaj veľký posun z hľadiska efektívnosti kryptomeny (Boehm, 2022).

Ethereum bezpečnosť

Ethereum funguje na princípe inteligentných zmlúv, ktoré sú naozaj flexibilné aj pri veľkom množstve údajov. Systém stále funguje v rámci nemennej logiky na kóde blockchainu. Vytvoril sa ekosystém decentralizovaných aplikácií, ktoré sú zvýhodnené oproti starším systémom. Na druhej strane je to ale aj príležitosť pre útočníkov, ktorí sa snažia využiť nedostatky inteligentných zmlúv. Verejné blockchainya naďalej robia otázku zabezpečenia smart kontraktov zložitejšou. Opraviť bezpečnostné chyby v existujúcich

zmluvách nie je vždy možné. Ďalšou nevýhodou je, že ukradnuté aktíva z inteligentných zmlúv sa väčšinou nedajú sledovať a už vôbec nie získať. Odhaduje sa, že celková suma ukradnutej hodnoty aktív v dôsledku bezpečnostných chýb v inteligentných zmluvách predstavuje sumu väčšiu ako 1 miliarda dolárov (hacknutie DAO - krádež 3,6 milióna ETH, v hodnote viac ako 1 miliardy USD, hacknutie peňaženky Parity - 30 miliónov dolárov, problém zmrazenej peňaženky Parity vyše 300 miliónov USD v ETH navždy uzamknuté). Problémy bezpečnosti si vyžadujú výrazne väčšiu investíciu do bezpečnosti (Ethereum foundation, 2023).

Ethereum možnosť stakingu

Ethereum je možné stakeovať mnohými spôsobmi. Ether je možné jednoducho uložiť, a účtovné vytyčovacie systémy vám nie len nastaví uzol, ale ho tiež spravujú. Poznáme sólo a rôzne iné stakeovacie platformy. Základný rozdiel medzi nimi je v ovládaní súkromného kľúča validátora. Poskytovateľ stakeovacieho poolu spravuje a má na starosti aktíva investora. Za svoje služby si títo poskytovatelia účtujú časť odmien. Množstvo etherea, ktoré je investorom pridelené závisí od celkovej sumy investovaného etherea (Ghosh, 2021).

Ethereum využitie v praktickej rovine

Etherisc je decentralizovaná poisťňa aplikácia, ktorá funguje na sieti etherea. Členovia si môžu zakúpiť poistenie natívnym tokenom priamo v aplikácii. Pooly predstavujú zhromaždené peniaze, ktoré sú získané cez poisťné platby. Keď dôjde k poistenej udalosti, poisťné plnenie bude vyplatené poškodeným členom bez toho, aby ste museli prechádzať tradičným procesom v poisťovníctve. Napríklad poistenie plodín by mohlo vyplatiť peniaze poškodeným automaticky v prípade sucha alebo povodňovej udalosti hlásenej vládnu agentúrou. Otázne je zneužívanie takéhoto systému (Ghosh, 2021).

3.1.4 Závěrečné porovnanie

	Volatilita	Využitelnosť	Rýchlosť spracovania	Bezpečnosť	Možnosť stakingu	Pokus v praktickej rovine	Spolu
Cardano	2	4	4	5	5	3	23
Bitcoin	3	5	2	5	1	1	17
Ethereum	2	2	2	2	5	3	16

Tabuľka 1: Závěrečné porovnanie kryptomien z finančného hľadiska

Zdroj: Vlastné spracovanie

V záverečnom porovnaní sme zisťovali, ktorá z 3 kryptomien má najväčší potenciál stať sa finančným aktívom. V rámci porovnania sa brali do úvahy faktor volatility, využitelnosť kryptomeny, rýchlosť spracovania a teda jej efektívnosť, bezpečnosť, možnosť stakingu a teda potenciál budúceho krypto-termínovaného vkladu a tiež, či daná kryptomena je alebo bola používaná v projektoch. Porovnaním získala kryptomena cardano 23 bodov, bitcoinu bolo priradených 17 bodov a ethereu 16 bodov. Kryptomena, ktorá má najväčší potenciál stať sa finančným aktívom je cardano.

Napriek tomu je pravda, že na rozdiel od bitcoinu, ktorý bol vyvinutý za týmto účelom, má cardano aj iné ciele. Bitcoinu ale v hodnotení uškodil výsledok projektu v Salvadore, ktorý skončil úplným fiaskom. Pri bitcoine nám tiež odpadá možnosť stakingu, čiže potenciálny krypto-termínovaný vklad nebude možný. Napriek výsledku hodnotenia sa aj pri cardane stretávame s viacerými neistotami. Medzi hlavné patrí jeho vysoká volatilita, a tiež fakt, že cardano nemá za sebou projekt, akým si prešiel bitcoin v Salvadore. Nie je preto vylúčené, že by to aj v prípade tejto kryptomeny neskončilo podobne neúspešne.

3.2 Porovnanie kryptomien z hľadiska investičného potenciálu

3.2.1 Cardano

Cardano šifrovanie

Cardano – sieť šifier, ktorá je zameraná na zrod globálnej cloudovej ekonomiky. Token siete cardana je ADA. Tento token je možné využiť na staking, uskutočňovanie transakcií, poplatky platobných sietí a tiež poskytuje mnohým spotrebiteľom kontrolu nad

ovládáním. S cardanom súvisí aj funkcia smart contract, ktorá je novinkou. Cieľom tejto funkcie je pridať ďalšiu možnosť využitia ADA a to umožniť vývojárom vyvíjanie decentralizovaných aplikácií. V tomto smere je stále otáznе, ako budú aplikácie s technológiou fungovať. V prípade úspešného vývoja decentralizovaných aplikácií by sa cardano mohlo stať konkurentom aj kryptomenám v mnohých nových oblastiach (Kondratiuk, Seijas, Nemish, Thompson, 2021).

Cardano technológia

Cardano je založené na blockachaine. Je to online platforma najnovšej generácie. Je to tiež otvorená obchodovateľná krypto sieť. Open-source softvér cardana ovláda viacero decentralizovaných počítačov v mnohých krajinách a zjednocuje ich do cloudovej platformy plne ovládanej vlastníkom (používateľom). Token ADA reprezentuje časť vlastníctva tohto systému (Kondratiuk, Seijas, Nemish, Thompson, 2021).

Cardano potenciál decentralizovaných aplikácií

ADA predstavila možnosti inteligentného uzatvárania zmlúv so zámerom vytvorenia cloudovej siete a následne decentralizovaných aplikácií. Spustenie týchto aplikácií (známych aj ako dApps) na mainette stále postupuje a testuje sa (Etoro, 2018).

Cardano cieľ kryptomeny

Budúcnosť, či už cloudov alebo webov, môžu tvoriť prepracované krypto siete. Cardano sa zameriava na cloudové systémy, má výnimočný mechanizmus, ale ďaleká budúcnosť kryptomeny je stále nejasná. Kryptomena sa posunula na úroveň inteligentných zmlúv, ktoré sú kľúčové z hľadiska tvorby decentralizovaných aplikácií. Komunita používateľov kryptomeny stále rastie, čo je veľmi dôležité pre jej ďalší rozvoj. V prípade, že sa technológia cardana ujme, decentralizované aplikácie a cloudové siete môžu zožať naozaj veľký úspech (Etoro, 2018).

Cardano aktuálna hodnota

Aktuálna burzová kapitalizácia kryptomeny cardano sa pohybuje v objeme 11,9 miliardy dolárov (Blockworks, 2023).

Cardano limitované množstvo kryptomeny

Cardano má limitovaný počet tokenov. Tento počet je ale v porovnaní s konkurenčnými kryptomenami veľmi vysoký. Maximálny počet tokenov je stanovený na 45 miliárd. Toto obmedzenie je podobné ako v prípade bitcoinu (Boffey, 2021).

3.2.2 Bitcoin

Bitcoin šifrovanie

Potenciálne elektronické platidlo môže byť definované ako databáza digitálnych podpisov. Je dôležité, aby sa tieto podpisy nedali mazať. Podstata šifrovania je v tom, že aktuálny majiteľ prevedie napr. bitcoin na nového majiteľa digitálnym podpisom (hashom). Nový vlastník napr. bitcoinu má možnosť tieto podpisy (hashe) overiť. Nedostatok systému spočíva v tom, že nový vlastník bitcoinu nevie s určitosťou zistiť, či daná minca už nebola minutá. Ideálnym riešením v tomto prípade by bolo zaviesť centrálu, ktorá by mala pod dohľadom všetky takéto transakcie. Bolo by možné zamedziť takémuto dvojnásobnému mŕňaniu a podobným podvodom. Na druhej strane problém by bol, že celý takto vytvorený systém by závisel od jednej centrály. Je nevyhnuté prísť pri takomto systéme meny na spôsob, ako si môže prijímateľ platby overiť, že platba nebola skôr podpísaná. Vo svete kryptomien sa považuje za legitímnu práve skoršia transakcia. Ďalšie pokusy sú z hľadiska legitímnosti irelevantné. Pre kompletnú informovanosť oboch strán je potrebné, aby boli transakcie verejne oznámené, mali verejnú chronologickú históriu a dôkazy, že všetky transakcie boli z hľadiska hashov legitímne. Potenciálne zvládnutie problému overovania legitímnosti transakcie by mohlo spočívať v časových pečiatkach. Každá takáto pečiatka by mala obsahovať hash predchádzajúcej časovej pečiatky, ktorý je súčasťou reťazca. V prípade, že je CPU riadený legitímnymi uzlami, reťazec sa rozrastie najrýchlejšie. Ak by chcel niekto napadnúť takto vzniknutý reťazec, potreboval by zmeniť predchádzajúci blok a prejsť „testom“ každého ďalšieho bloku, až kým by nedobehol legitímne uzly. Dôležitým faktom ale je, že pravdepodobnosť sa s pribúdajúcimi blokmi výrazne znižuje. Táto náročnosť sa zvyšuje ešte viac v prípade, že sú bloky vytvárané frekventovane. Nová a teda prvá transakcia v konkrétnom bloku je stále tvorcom bloku. Táto transakcia spúšťa novú mincu, uzly a potrebnú podporu siete. Konštantný rast digitálnych mincí v obehu je priamo úmerný s klesajúcim počtom minerov. Za náklady sú v tomto prípade považované elektrina a vynaložený čas CPU. V prípade, že by niekto chcel tento systém napadnúť, musel by byť schopný ovládnuť sieť najväčším výkonom CPU.

V tomto prípade má útočník dve možnosti. Mohol by buď zasiahnuť systém platieb a teda podviesť ľudí, alebo si môže sám vygenerovať digitálne mince. Na overenie platby stačí, ak má užívateľ hlavičky blokov reťazca proof-of-work. Je dôležité, aby bol tento reťazec najdlhší. Opäť ale platí, že overenie má výpovednú hodnotu, iba ak sieť ovládajú uzly, ktoré nie sú zmanipulované. V prípade, že je sieť napadnutá, môže útočník vymyslieť fake transakcie. Teoretická ochrana proti napadnutiu systému útočníkom by spočívala v systéme kontroly varovaní zo sieťových uzlov. Je tiež pravdepodobné, že spoločnosti, ktoré pracujú s danou technológiou na dennej báze budú z dôvodu bezpečnosti a overovania riadiť prevádzku na vlastných uzloch (Narayanan, Bonneau, Felten, Miller, Goldfeder, 2016).

Bitcoin technológia

Bitcoin, ako väčšina kryptomien funguje na báze peer-to-peer a nie na báze klient-server. Ako už bolo vysvetlené, peer-to-peer funguje ako sieť klebiet. Každý povie niečo nové ďalším ľuďom a nakoniec sa novinka dostane ku každému v sieti. Sieť peer-to-peer sa nespolieha na jeden centrálny bod kontroly, ktorý môže teoreticky zlyhať. Takzvanú zbierku uzlov bitcoinových peer-to-peer protokolov nazývame pojmom „bitcoinová sieť“. Pri bitcoine sa okrem peer-to-peer protokolu využívajú aj iné protokoly ako napríklad Stratum. Protokol Stratum sa využíva na ťažbu a mobilné peňaženky. Dodatočné protokoly vytvárajú servery, ktoré prichádzajú do styku s bitcoinovou sieťou pomocou peer-to-peer protokolu a postupne sieť rozširujú na uzly s inými protokolmi. Napríklad servery Stratum spájajú ťažobné uzly Stratum s využitím protokolu Stratum a hlavnej bitcoinovej siete premostujú protokol Stratum s bitcoinovým peer-to-peer protokolom. Pojem „rozšírená bitcoinová sieť“ sa využíva na označenie celkovej siete. Táto sieť zahŕňa bitcoinový predovšetkým peer-to-peer protokol, pool-mining protokoly, a tiež protokol Stratum (Narayanan, Bonneau, Felten, Miller, Goldfeder, 2016).

Bitcoin potenciál decentralizovaných aplikácií

Vzhľadom k architektúre a cieľom kryptomeny stať sa elektronickou mincou sa bitcoin neuberá smerom tvorby decentralizovaných aplikácií (Boyle, Salazar, 2021).

Bitcoin cieľ Kryptomeny

Bol predstavený potenciálny systém pre transakcie, ktoré sú uskutočňované elektronicky. Elektronická minca, ktorá je založená na databáze digitálnych podpisov má

riziko jej dvojitého minútia. Aby sme tomuto riziku zabránili, je navrhnutá sieť peer-to-peer založená na proof-of-work, ktorá ukladá históriu transakcií. V prípade, že väčšinu výkonu ovláda CPU a nie organizovaná skupina, systém funguje (Boyle, Salazar, 2021).

Bitcoin aktuálna hodnota

Aktuálna trhovú kapitalizácia bitcoinu je 432,62 miliárd dolárov. Toto číslo sa veľmi často mení o zanedbateľné čiastky. Takáto vysoká trhovú kapitalizácia kryptomeny v porovnaní s konkurenciou dokazuje, ako vysoko je aktívum trhovu hodnotené (Blockworks, 2023).

Bitcoin limitované množstvo kryptomeny

Celkový objem bitcoinov je stanovený na 21 miliónov. 19 miliónov bitcoinov bolo už vyťažených. Bitcoin je teda z tohto hľadiska veľmi vzácny. Cieľom obmedzenia je udržať ponuku a zároveň dopyt po kryptomene. Limitované množstvo bitcoinu do výšky v akej je, je jeden z dôvodov, prečo má bitcoin na trhu mnohonásobne väčšiu cenu, ako má cenu napríklad cardano (Boffey, 2021).

3.2.3 Ethereum

Ethereum Šifrovanie

Ethereum je blockchainová sieť. Na odosielaní a prijímaní transakcií pracujú uzly v sieti. Pred tým ako niekto odošle údaj o transakcii, sa použijú súkromné kľúče na ich šifrovanie. Keby sa tento súkromný kľúč na šifrovanie nepoužil, každý používateľ etherea by bol stále schopný dešifrovať prenos údajov, platieb a tiež správ. Symetrickým šifrovaním označujeme najbežnejšiu metódu šifrovania. Práve táto metóda využíva jedinečný kľúč alebo heslo na šifrovanie a tiež dešifrovanie údajov (Gupta, 2022).

Ethereum technológia

Ethereum predstavuje decentralizovanú blockchainovú sieť, ktorá je poháňaná tokenom ether. Jadrom etherea sú smart kontrakty, ktoré umožňujú kryptomene sa uberať smerom tvorby decentralizovaných aplikácií. Sieť umožňuje jej používateľom vykonávať transakcie, hrať hry a využívať staking na úročenie množstva držaných kryptomien (Ghosh, 2021).

Ethereum potenciál decentralizovaných aplikácií

Aplikácie ethereua využívajú v prvom rade decentralizovanú a nemennú povahu technológie blockchain. Môže ich vytvoriť ktokoľvek bez toho, aby sa znížila bezpečnosť systému. Ich funkcie sú rôzne. Tu je niekoľko príkladov:

- Decentralizované financie (DeFi): Cieľom DeFi je vybudovať globálny finančný systém, ktorý je otvorený a ku ktorému má prístup ktorákoľvek osoba s prístupom na internet. Na rozdiel od finančného odvetvia založeného na dôvere. Pri DeFi je dôvera minimalizovaná, čo znamená, že celkové fungovanie systému nezávisí od zodpovednej osoby. Cieľom platformy je umožnenie, transparentného prístupu. Systém spája peer-to-peer ponuku a dopyt, čím sa eliminuje potreba sprostredkovateľov. Mnoho funkcií DeFi sa rozrástli a stali sa finančným ekosystémom. Teraz si môžu bežní používatelia požičiavať peniaze, investovať, obchodovať, zarábať na úrokoch, zabezpečovať si rôzne poistenia a prevádzať peniaze tak, ako by to bolo možné v tradičnom finančnom systéme.
- Decentralizovaná autonómna organizácia (DAO): DAO označuje organizáciu bez tretej strany, ktorá je vytvorená za spoločným cieľom. Táto organizácia funguje na princípe zdieľaného, definovaného a automatizovaného protokolu. Cieľom protokolu je zabezpečiť vypočutie hlasov všetkých členov skupiny. Rozhodovací proces je plne transparentný. Každý DAO má zabudovanú pokladnicu, v ktorej sú finančné prostriedky. Tieto financie sa vynakladajú podľa rozhodnutí prijatých hlasovaním členov. Jedným z príkladov DAO je spustený decentralizovaný fond rizikového kapitálu s názvom „DAO“. Fond bol spustený v roku 2016. Členovia mali možnosť zakúpiť si tokeny DAO, aby získali právo hlasovať o investičných návrhoch. Ak sa odhlasovaný projekt stal ziskovým, členovia by dostali odmenu priamo úmernú ich vkladom. DAO bol inovatívny nápad, zlyhal ale kvôli chybe, ktorá existovala v kóde inteligentnej zmluvy. Hackerom sa podarilo ukradnúť časť prostriedkov organizácie.
- Nezastupiteľné tokeny (NFT): NFT sú záznamy údajov v blockchaine. Zahrňujú digitálne aktíva, ako sú fotografie, audio, videá, akcie a tiež certifikáty na fyzické aktíva, ako sú nehnuteľnosti a maľby. Keďže digitálne súbory sa dajú ľahko replikovať, majú nezameniteľné tokeny, ktoré dokazujú vlastníctvo digitálneho obsahu. To znamená, že keď sa NFT kúpi, vlastník získa nezmeniteľný záznam o vlastníctve. Príťažlivosť NFT pre digitálne aktíva spočíva práve vo vzácnosti, ktorú

vytvára a tým aj zvyšuje zberateľskú hodnotu majetku. Umelcom predávajúcim aktíva umožňujú NFT priamejšie šírenie ich diel bez aktívnej tretej strany. V prípade NFT podporovaných skutočnými fyzickými aktívami tokenizácia si aj digitálne vlastníctvo položky zachováva jej jedinečnosť (WisdomTree, 2021).

Ethereum cieľ kryptomeny

Kryptomena sa zameriava na vytvorenie decentralizovanej počítačovej siete na spustenie rôznych aplikácií. Takto fungujúca decentralizovaná sieť môže potenciálne zautomatizovať rozhodnutia a transakcie, čím môže znížiť potrebu dôveryhodnej siete centrálnej strany. Výhodou je tiež potenciálne zníženie potreby sprostredkovateľov, nákladov na arbitráže a tiež zabránenie podvodom (WisdomTree, 2021).

Ethereum aktuálna hodnota

Ethereum je podľa trhovej kapitalizácie po bitcoine druhá najväčšia kryptomena. Trhová hodnota kryptomeny, ktorá je aktuálne na 192,08 miliardy dolárov, sa neustále mení. Trhová kapitalizácia, ktorá je naozaj vysoká, nám ukazuje, do akej výšky je aktívum trhom hodnotené (Coinbase, 2023).

Ethereum limitované množstvo kryptomeny

Ethereum nemá limitované množstvo tokenov. V januári 2021 bolo v obehu niečo cez 113 miliónov tokenov. V apríli 2022 ich bolo už vyše 120 miliónov. Ethereum sa síce dá obchodovať, kúpiť alebo predáť podobne ako ostatné kryptomeny, nie je to ale len minca na uchovávanie hodnoty ako napríklad bitcoin. To je dôvodom, prečo jej množstvo nemusí byť obmedzené. Ethereum je totiž postavené na rôznorodom blockchaine, ktorý je naozaj rozsiahly. V rámci je možné vytvoriť ľubovoľný počet decentralizovaných projektov (The healthy journal, 2021).

3.2.4 Závěrečné porovnání

	Šifrování	Technologie	Potenciál decentralizovaných aplikací	Cíle kryptominy	Aktuální hodnota	Limitované množství kryptominy	Spolu
Cardano	4	4	5	5	1	4	23
Bitcoin	4	3	1	3	5	5	21
Ethereum	3	4	5	4	3	1	20

Tabulka 2: Závěrečné porovnání kryptomín z investičního hlediska

Zdroj: Vlastné zpracování

Cílem porovnání bylo zjistit, která z vybraných 3 kryptomín má největší potenciál z dlouhodobého investičního hlediska. Brali jsme do úvahy faktory jako složitost a zpracovanost šifrování, technologii, možnost vývoje decentralizovaných aplikací danou kryptomínou, cíle kryptominy, její aktuální hodnotu a také, či je množství tokenů kryptominy limitované. Cardano získalo v porovnání 23 bodů, bitcoin dosáhl 21 bodů a ethereum připadlo 20 bodů. Nejlepší investiční možností je tedy kryptomína cardano. V hodnocení jí pomohlo její zaměření do budoucna, možnost vytváření decentralizovaných aplikací a také její limitované množství tokenů, při kterých je větší šance, že si udržia vzácnost a hodnotu. Cardano má také zpracovanou technologii a složitě šifrování, kterým dosahuje vysokou úroveň bezpečnosti.

Záver

Cieľom bakalárskej práce bolo na základe vybraných faktorov porovnať jednotlivé kryptomeny z finančného a tiež investičného hľadiska a vybrať jednu konkrétnu s najväčším potenciálom.

Kryptomeny sa od ich úplného začiatku v roku 2008 stávajú čoraz populárnejšími. Od roku ich vzniku pribudlo nespočetné množstvo veľmi zaujímavých, ale tiež úplne zbytočných altcoinov. My sme si vybrali tri kryptomeny, ktoré sú v dnešnom svete považované za suverénne najznámejšie a tiež za tie s najväčším potenciálom. Sú to kryptomeny bitcoin, ethereum a cardano.

Vopred definovaný cieľ práce sa podarilo dosiahnuť. Problematiku sme z hľadiska teoretickej časti zhrnuli v prvej kapitole. V kapitole druhej sme si stanovili metódy, ktoré budeme v snahe o dosiahnutie cieľa práce využívať. V tretej kapitole sme hlbšie analyzovali jednotlivé faktory, ktoré sú pre porovnanie kľúčové. Vykonali sme porovnanie kryptomien z hľadiska finančného a tiež z hľadiska investičného potenciálu do budúcnosti. Pri porovnaní z hľadiska potenciálu stať sa finančným aktívom sme brali ohľad na faktory volatility, využiteľnosti, rýchlosti spracovania transakcií a bezpečnosti. Za relevantné sme tiež považovali otázku, či má daná mena potenciál možnosti stakingu a tiež, či už bola využitá v praktickej rovine. Pri porovnaní z investičného hľadiska boli ako porovnávacie faktory zvolené šifrovanie, technológia, ktorou daná kryptomena disponuje, cieľ kryptomeny a jej aktuálna hodnota. Tiež sme do porovnania zahrnuli otázku, či disponuje daná kryptomena obmedzeným množstvom alebo nie.

Výsledky porovnania sme prehľadne zobrazili v tabuľkách. Úspešne sa nám podarilo vybrať kryptomenu s najväčším potenciálom do budúcnosti. Touto kryptomenou je cardano. Cardano dosiahlo najvyššie skóre v oboch porovnaniach. Faktom je, že v porovnaní z hľadiska finančného aktíva jej v súboji s bitcoinom pomohol jeho tragický pokus o implementovanie vo svete bankovníctva v štáte Salvador. Vzhľadom k momentálnej situácii vo svete a prebiehajúcim projektom v krypto-sfére je ale práve cardano kryptomena s najväčším potenciálom do budúcnosti.

Zoznam použitej literatúry

BARTOLETTI, Massimo - POMPIANU, Livio. An empirical analysis of smart contracts: Platforms, Applications, and Design Patterns [online]. In *Financial Cryptography and Data Security: FC 2017 International Workshops*. Cham: Springer, 2017, vol. 10323, p. 494-509 [Citované dňa: 10.11.2022]. ISBN 978-3-319-70278-0. Dostupné na: https://link.springer.com/chapter/10.1007/978-3-319-70278-0_31

Blockworks. *ADA Price* [online]. Blockworks. [Citované dňa: 9.4.2023]. Dostupné na: <https://blockworks.co/price/ada>

Blockworks. *Bitcoin Price* [online]. Blockworks, 2023. [Citované dňa: 9.4.2023]. Dostupné na: <https://blockworks.co/price/btc>

BOEHM, Betsy. *What's Ethereum 2.0?* [online]. In WorldCoin, [Citované dňa: 24.3.2023]. Dostupné na: <https://worldcoin.org/articles/whats-ethereum-2-0#toc-1>

BOFFEY, P. (2021). *How Many Cardano Tokens Are There and How Many Are Left?* [online] *OriginStamp*. [Citované dňa: 25.3.2023]. Dostupné na: <https://originstamp.com/blog/how-many-cardano-tokens-are-there-and-how-many-are-left/>

BOYLE, J. - SALAZAR, C. *What is a Decentralized Exchange (DEX)?* [online]. Chainlink, Inc. 2021. [Citované dňa: 9.4.2023]. Dostupné na: <https://chain.link/education-hub/what-is-decentralized-exchange-dex>

BUNJAKU, Flamur - GJORGIEVA-TRAJKOVSKA, Olivia - MITEVA-KACARSKI, Emilija. *Cryptocurrencies – Advantages and Disadvantages* [online]. In *International Journal of Engineering and Innovative Technology. Indonesia: IJEIT*, vol. 8, no. 3, p. 226-230 [Citované dňa: 12.1.2023]. ISSN 2277-3754. Dostupné na: https://www.ijeit.com/Vol%208/Issue%203/IJEIT1412201807_28.pdf

CAMPBELL-VERDYUN, Malcolm. *Bitcoin and Beyond: Cryptocurrencies, Blockchains, and Global Governance* [print]. In: *Bitcoin and Beyond: Cryptocurrencies, Blockchains, and Global Governance*. New York: Routledge, 2018, pp. 1-17. ISBN 978-1-138-10600-1. [Citované dňa: 20.3.2023].

Coinbase. *Ethereum (ETH) Price* [online]. Coinbase, 2023. [Citované dňa: 9.4.2023]. Dostupné na: <https://www.coinbase.com/price/ethereum>

Crypto.com. *Ethereum (ETH) Price* [online]. Crypto.com. [Citované dňa: 9.4.2023]. Dostupné na: <https://crypto.com/price/ethereum>

Ethereum Foundation. *Smart Contract Security* [online]. Ethereum Foundation, 2023. [Citované dňa: 10.4.2023]. Dostupné na: <https://ethereum.org/en/developers/docs/smart-contracts/security/>

ETORO Research Team. *ADA: Cardano's Cryptocurrency* [online]. In *eToro Research. eToro*, July 2018. [Citované dňa: 25.3.2023]. Dostupné na: <https://www.etoro.com/wp-content/uploads/2018/07/ADA-eToro-Research.pdf>

GHOSH, A. *Ethereum 2.0 staking: A beginner's guide on how to stake ETH* [online]. Cointelegraph, 2021. [Citované dňa: 10.4.2023]. Dostupné na: <https://cointelegraph.com/learn/ethereum-2-0-staking-a-beginners-guide-on-how-to-stake-eth>

Grayscale Investments, LLC. *CARDANO: Building Blocks for a New Era* [online]. New York: Grayscale Investments, LLC, 2021 [Citované dňa: 20.1.2023]. Dostupné na: https://grayscale.com/wp-content/uploads/2021/09/CARDANO_Building-Block.pdf

GUPTA, Abhimanyu. *Which Algorithm is Used to Encrypt Ethereum Private Keys?* [online]. In: *Coinmonks*. [Citované dňa: 25.03.2023]. Dostupné na: <https://medium.com/coinmonks/which-algorithm-is-used-to-encrypt-ethereum-private-keys-e4077496aff8>

GURUSAMY, Vairaprakash - DARSHAK, Akbari. *Bitcoin: A cryptocurrency*. [print]. In *International Journal of Engineering & Technology*. Chennai: IJET Publications, 2018, roč. 7, č. 4. strany 1282-1286 [Citované dňa: 24.2.2023]. ISSN: 2319-8613

HOWSON, Peter. *Bitcoin: El Salvador's failed experiment has important lessons* [online]. In: *The Conversation* [Citované dňa: 23.3.2023]. Dostupné na: <https://theconversation.com/bitcoin-el-salvadors-failed-experiment-has-important-lessons-189503>

CHOUDHURY, S. (2022). *Cardano Transaction Speed Per Second Is 250 While BitGert Transaction Speed Is 100,000 Per Second, Faster Than Solana, Avalanche or Matic* [Online]. In: *Analytics Insight. Valued Insightful Information Pvt. Ltd.* [Citované dňa: 25.3.2023]. Dostupné na: <https://www.analyticsinsight.net/cardano-transaction-speed-per-second-is-250-while-bitgert-transaction-speed-is-100000-per-second-faster-than-solana-avalanche-or-matic/>

second-is-250-while-bitgert-transaction-speed-is-100000-per-second-faster-than-solana-avalanche-or-matic/

IVASHCHENKO, A.I. *Using Cryptocurrency in the Activities of Ukrainian Small and Medium Enterprises in order to Improve their Investment Attractiveness* [online]. In *Problems of Economy*. Ukraine: INZHEK Publishing House, 2016, no.3, p. 267-273 [Citované dňa: 10.10.2022]. ISSN 2311-1186. Dostupné na: <https://www.problems-of-economy.com/userfiles/file/Archive/2016/3/25.pdf>

KONDRATIUK, Dmytro - LAMELA Seijas, Pablo - NEMISH, Alexander - THOMPSON, Simon. (2021). *Standardized Crypto-Loans on the Cardano Blockchain. Proceedings of the International Conference on Financial Cryptography and Data Security (FC 2021)*, 41, 592-602. doi: 10.1007/978-3-662-63958-0_41. [Citované dňa: 21.3.2023].

LEWIS, Anthony. *Blockchain*. In *A Gentle Introduction to Bitcoin Mining* [online]. 2019, [Citované dňa: 25.11.2022]. Dostupné na: <https://assets.ctfassets.net/sdlntm3tthp6/5CbV1gD3NuCCkKauWug6aU/b24fcd5fa2a5cd4a0c32e7dd90838c8a/A-Gentle-Introduction-To-Bitcoin-Mining-WEB.pdf>

MADLIN, Twente. *Introduction to Cardano Stake Pools* [online]. *Junostakepool*, 2022 [Citované dňa: 25.3.2023]. Dostupné na: https://junostakepool.com/wp-content/uploads/presentations/introduction_to_cardano_stake_pools.pdf

MORA, Arturo. *IOG Academy: The pathway to becoming a Cardano smart contract developer* [online]. *IOG Academy*, 2021. [Citované dňa: 9. apríla 2023]. Dostupné na: <https://ioacademy.io/blog/the-pathway-to-becoming-a-cardano-smart-contract-developer/>.

MUELLER, Paul – BERGSTRÄSSER, Sonja - RIZK, Amr - STEINMETZ, Ralf. *An Architectural Overview of the Bitcoin Blockchain*. [print]. In: *IEEE Communications Surveys & Tutorials*. Piscataway, NJ: IEEE Communications Society, 2018, roč. 20, č. 4, strany 3609-3634. [Citované dňa: 10.3.2023]. ISSN: 1553-877X

NARAYANAN, Arvind – BONNEAU, Joseph – FELTEN, Edward – MILLER, Andrew – GOLDFEDER, Steven – CLARK, Jeremy. *Bitcoin and Cryptocurrency Technologies* [book]. In: *Princeton University Press*. 2016, 1st edition, 1st printing, 336 pages. [Citované dňa: 23.2.2023]. ISBN 978-0691171692

RODECK, D. - CURRY, B. (2021). *What Is Cardano (ADA)?* [Online]. In: *Forbes Advisor*. Forbes Media LLC. [Citované dňa: 21.3.2023]. Dostupné na: <https://www.forbes.com/advisor/investing/cryptocurrency/cardano-ada/>

SHARIYAH, Review Bureau. (2022). *Sharia Analysis* [online]. In: *Compliance and Sharia Advisory Services*. Manama, Bahrain: Shariyah Review Bureau. ISSN not available. [Citované dňa: 25.3.2023]. Dostupné na <https://shariyah.net/wp-content/uploads/2022/03/PDF-CARDANO.pdf>

The Healthy Journal. *Why Does Ethereum Not Have a Max Supply?* [online]. The Healthy Journal, 2021. [Citované dňa: 9.4.2023]. Dostupné na: <https://www.thehealthyjournal.com/q-and-a/why-does-ethereum-not-have-a-max-supply>

US Sentencing Commission. *Emerging Technology: & Crypto* [online]. In *Annual National Training Seminar*. Washington D.C.: US Sentencing Commission, 2018, [Citované dňa: 10.12.2022]. Dostupné na: https://www.ussc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2018/Emerging_Tech_Bitcoin_Crypto.pdf

WisdomTree. *Ethereum: Frequently Asked Questions* [online]. WisdomTree Europe, April 2021. [Citované dňa: 25.3.2023]. Dostupné na :https://www.wisdomtree.eu/-/media/eu-media-files/other-documents/faq/wisdomtree_ethereum_april2021.pdf

WisdomTree. *The World Computer: Introduction to Ethereum*. [online]. In: *WisdomTree Blog: Research & Insights*. New York: WisdomTree Investments, Inc., 2019. [Citované dňa: 20.3.2023]. Dostupné na: <https://www.wisdomtree.com/-/media/us-media-files/etf-strategies/etf-education/2019/the-world-computer-introduction-to-ethereum.pdf>

ZHANG, Limeng - ZHOU, Rui - LIU, Qing - XU, Jiajie, CHENGFEI, Liu. *Transaction Confirmation Time Estimation in the Bitcoin Blockchain* [online]. In *Web Information Systems Engineering WISE 2021: 22nd International Conference on Web Information Systems Engineering*. Cham: Springer, 2022, vol. 13080, p. 33-44 [Citované dňa: 23.11.2022]. ISBN 978-3-030-90888-1. Dostupné na: https://doi.org/10.1007/978-3-030-90888-1_3