Ekonomická univerzita v Bratislave
Fakulta hospodárskej informatiky

Evidenčné číslo: 103004/B/2018/ 36097107837351684

Kryptomeny

Bakalárska práca

2018 **Tomáš Baláži**

Ekonomická univerzita v Bratislave
Fakulta hospodárskej informatiky
FHI

Kryptomeny

Bakalárska práca

Študijný program: Hospodárska informatika

Študijný odbor: Hospodárska informatika

Školiace pracovisko: Katedra aplikovanej informatiky

Vedúci práce: Ing. Igor Bandurič, PhD.

Bratislava 2018 **Tomáš Baláži**

POĎAKOVANIE

Týmto by som sa rád poďakoval všetkým ľuďom, ktorí mi verili a podporovali ma pri písaní tejto práce. Moja vďaka patrí vedúcemu mojej bakalárskej práce za poskytnutú trpezlivosť a užitočné rady.

ČESTNÉ PREHLÁSENIE

Čestne prehlasujem, že vypracovanie tejto bakalárskej práce bolo spracované na základe poznatkov z uvedenej literatúry a nadobudnutých vlastných poznatkov.

.....

Tomáš Baláži

Abstrakt

BALÁŽI, Tomáš: *Kryptomeny* – Ekonomická univerzita v Bratislave. Fakulta hospodárskej informatiky; Katedra aplikovanej informatiky.
– Vedúci záverečnej práce: Ing. Igor Bandurič, PhD. – Bratislava: FHI, 2018, 61 s.

Hlavnými cieľmi bakalárskej práce je priblíženie sveta kryptomien, fungovanie a porovnanie niektorých z nich. Na svete existuje mnoho kryptomien, ktoré sa môžu líšiť v technológiách a vlastnostiach. V záverečnej práci sú porovnávané 4 kryptomeny: Bitcoin, Ethereum, Dash a Ripple. Každá z nich je porovnávaná s Bitcoinom na základe stanovených hľadísk a kritérií ako napríklad validácia operácií, trhová kapitalizácia, dosahovaný konsenzus v platobných systémoch či rýchlosť transakcií. Cieľom je porovnať tieto kryptomeny a poukázať na odlišnosti a podobnosti. V práci tiež interpretujem niektoré vlastnosti blockchainovej technológie na zdrojovom kóde programovacieho jazyka. Záverečná práca je rozdelená do 3 kapitol. Obsahuje 12 obrázkov a 7 tabuliek. Teoretická časť práce je venovaná zoznámeniu sa so základnými pojmami a technológiami, potrebnými na pochopenie danej problematiky. V druhej kapitole sme stanovili naše ciele a použitú metodiku. V tretej časti sme sa zoznámi s kritériami a na základe nich sme začali kryptomeny porovnávať s Bitcoinom. Na záver po porovnaní daných kryptomien sú čiastočne interpretované vlastnosti blockchainovej technológie.

Kľúčové slová: kryptomena, blockchain, platobný systém,Bitcoin, Ethereum, Dash, Ripple

Abstract

BALÁŽI, Tomáš: Cryptocurrencies - University of Economics in Bratislava. Faculty of Economic Informatics; Department of Applied Informatics.
- Supervisor: Ing. Igor Bandurič, PhD. - Bratislava: FHI, 2018, 61 s.

The main goals of the bachelor thesis are to get closer to the world of cryptocurrencies, to learn how they work and to compare some of them. There are many cryptocurrencies in the world that may vary in technology and features. In the final thesis, four cryptocurrencies are compared: Bitcoin, Ethereum, Dash and Ripple. Each of these is compared to Bitcoin based on established views and criterias, such as transaction validation, market capitalization, consensus in payment systems, or transaction time. The aim is to compare these cryptocurrencies and point to their differences and similarities. Some features of blockchain technology are also interpreted by the source code of the programming language. The final thesis is divided into 3 chapters. It contains 12 pictures and 7 tables. The theoretical part is dedicated to familiarization with the basic concepts and technologies needed to understand the given topic. In the second chapter we set our goals and the methodology used. In the third part, we have defined the criteria and based on them, we have begun to compare cryptocurrencies with Bitcoin. In the end, the properties of the blockchain technology are partially interpreted after comparing the cryptocurrencies.

Keywords: cryptocurrency, blockchain, payment system, Bitcoin, Ethereum, Dash, Ripple.

Obsah

Úvod

Už tisíce rokov sa fyzické platidlá ako napríklad kožušiny, zlato, mince, bankovky používajú ako platobné prostriedky. V prípade, že boli kupujúci a predávajúci na jednom mieste, boli takéto prostriedky vhodnými. Táto možnosť však nie je k dispozícii, ak sa dve strany nenachádzajú na rovnakom mieste, čo si vyžaduje používanie digitálnej meny. Digitálne peniaze používa v dnešnej dobe azda každý. Veď kto už v dnešnej modernej dobe nemá účet v banke či platobnú kartu. Takéto digitálne platidlo poskytujú rôzne finančné inštitúcie a banky a donedávna poskytovali jedinú možnosť pre platby v digitálnej forme.

V roku 2009 však prišla na scénu elektronických peňazí alternatíva vo forme platobného systému a zároveň digitálnej meny Bitcoin, ktorý bol založený neznámou osobou vystupujúcou pod pseudonymom Satoshi Nakamoto. Zaujímavým bolo hlavne to, že tento systém sa prezentoval tým, že dokáže fungovať bez akejkoľvek tretej autoritatívnej strany. V minulosti bolo už veľa pokusov o vytvorenie digitálnych platidiel, ktoré však v konečnom dôsledku z rôznych dôvodov nemali úspech. Tak čím sa mohol javiť Bitcoin výnimočným? Odpovedí na túto otázku je niekoľko. V jednoduchosti možno povedať, že to je hlavne vďaka technológiám, ktoré mal v sebe obsiahnuté. Tento systém využíva kryptografiu na šifrovanie svojich transakcií a sleduje kto je vlastník každého bitcoinu. To funguje vďaka technológii blokového reťazca, ktorý funguje ako účtovná kniha danej kryptomeny. Overovanie každej transakcie majú na svedomí užívatelia tohto systému, pretože touto činnosťou majú možnosť slušného zárobku. Táto kryptomena zožala veľký úspech vďaka komplexnosti celého systému a otvorila dvere na trhu ďalším alternatívam podobných kryptomien založených na rovnakom alebo obdobnom princípe.

Počas ďalších rokov sa vyvinulo mnoho ďalších platobných systémov – kryptomien. Tie by však nemali šancu napredovať keby neimplementovali do svojich systémov ďalšie inovácie a vylepšenia. V súčasnosti existujú stovky ďalších kryptomien. Zatiaľ však úspech svojho predchodcu žiadna nepredbehla, teda aspoň z hľadiska kapitalizácie trhu. Z hľadiska použitých vylepšení by sa o tom však dalo polemizovať. Od vzniku Bitcoinu prešlo 9 rokov a na trhu sa vyvinulo mnoho nových digitálnych peňazí, ktoré v sebe implementujú svoju vnútornú hodnotu vďaka technickým inováciám a novým možnostiam ich využitia.

1 Súčasný stav riešenej problematiky doma a v zahraničí

1.1 Úvod do sveta kryptografických technológií a pojmov

1.1.1 Kryptografia

Kryptografia je veda, ktorá sa zaoberá konštrukciou matematických metód, slúžiacich k zaisťovaniu bezpečnosti dát. Základné kryptografické metódy sa nazývajú šifrovanie a dešifrovanie. Metódy šifrovania transformujú otvorený text (správa, dáta) pomocou kryptografického algoritmu na zašifrovaný text. Naopak metódy dešifrovania transformujú zašifrovaný text späť na otvorený text. [1]

Zatiaľ čo kryptografia sa zaoberá návrhom a implementáciou šifrovacích systémov, tak kryptoanalýza je vedný odbor zaoberajúci sa metódami získavania obsahu zašifrovaných informácií. Kryptografia tvorí spolu s kryptoanalýzou vedný odbor nazývajúci sa kryptológia. Môžeme povedať, že kryptológia je veda, ktorá sa zaoberá šifrovaním zo všetkých uhlov pohľadu. [1]

Významný svetový kryptograf, autor rady publikácií a člen Centra Aplikovaného Kryptografického Výskumu Alfred Menezes definuje kryptografiu ako: Kryptografia sa zaoberá štúdiom matematických metód v súvislosti s aspektami informačnej bezpečnosti, ako sú dôvernosť, integrita dát, autentizácia subjektu a overovanie pôvodu dát.[2]

Výrazom šifra je označovaný kryptografický algoritmus, ktorý prevádza čitateľnú správu na jej nečitateľnú podobu. Cieľom šifrovania je skryť obsah správy pred každým, komu táto správa nie je určená. Dešifrovanie je opačný postup vzhľadom k šifrovaniu, je to prevedenie šifrovaného textu späť do podoby otvoreného textu. [2]

Výraz kľúč značí tajnú informáciu, bez ktorej nejde zašifrovanú správu prečítať. Dĺžkou kľúča obvykle rozumieme počet bitov jednotlivého kľúča, počet bitov je rovný logaritmu so základom dva a veľkosťou množiny kľúčov. Tajný kľúč alebo tiež šifrovací kľúč, je výraz pre kľúč používaný v symetrickej kryptografii, je známy zúčastneným stranám, ale nesmie byť známy neoprávneným stranám. Zdieľaný tajný kľúč je kľúč zdieľaný viac stranami, obvykle býva výsledkom dohody na kľúči. Verejný kľúč je jedným z dvojice kľúčov používaný v asymetrickej kryptografii, obvykle býva široko dostupný a je využívaný k šifrovaniu správ, zatiaľ čo súkromný kľúč je vlastníctvom iba jednej entity a nesmie byť nikomu inému prezradený a je využívaný k dešifrovaniu správ. Autentizovaný

kľúč je viazaný cestou autentizácie na svojho užívateľa, napríklad digitálnym certifikátom. [3]

1.1.2 Asymetrická kryptografia

Samostatná trieda šifrovacích algoritmov využíva na šifrovanie iný kľúč ako na dešifrovanie, pričom dešifrovací kľúč nie je možné efektívne vypočítať zo šifrovacieho kľúča. V tomto prípade hovoríme o asymetrickom šifrovaní, prípadne o šifrovaní s verejným kľúčom. Ako názov napovedá, šifrovací kľúč (označovaný aj ako verejný kľúč) je zvyčajne zverejnený a teda ktokoľvek môže šifrovať. Dešifrovať je možné len so znalosťou dešifrovacieho kľúča (kľúč býva označovaný ako súkromný kľúč).[3]

Centrálnou technológiou v technológii kryptomien je kryptografia s verejným kľúčom, ktorá sa pomocou hashovacej funkcie používa na generovanie adries kryptomien, podpisovanie transakcií a overovanie platieb. Kryptografia s verejným kľúčom je technológiou spoľahlivého určovania pravosti transakcií kryptomien používajúcich digitálne podpisy. Používa asymetrický algoritmus, ktorý generuje dva samostatné, ale asymetricky prepojené kľúče: verejný kľúč a súkromný kľúč. Kľúče sú asymetrické v tom zmysle, že verejný kľúč je odvodený zo súkromného kľúča, ale je výpočtovo nemožné získať súkromný kľúč z verejného kľúča. V takomto systéme sa verejný kľúč používa na overenie digitálnych podpisov v transakciách, zatiaľ čo súkromný kľúč sa používa na podpísanie transakcií na vytvorenie týchto digitálnych podpisov. Verejný kľúč je verejne prístupný. Napr. V systéme Bitcoin sa používa ako bitcoinová adresa do ktorej a z ktorej sú odosielané platby. Na druhej strane súkromný kľúč by mal byť uchovaný bezpečne a v tajnosti Krása takéhoto systému spočíva v tom, že transakcie možno ľahko overiť pomocou verejného kľúča bez zdieľania súkromného kľúča používaného na podpísanie transakcií.[4]

1.1.3 Hashovacia funkcia

Hashovacie funkcie sú definované ako jednosmerné matematické funkcie. To znamená, že v jednom smere sú ľahko vyriešiteľné a v opačnom smere nesmú byť vyriešiteľné. [5]

Tento fakt nám ponúka zamyslieť sa nad rozmanitosťou možností využitia tohto druhu matematických funkcií v rámci informačnej bezpečnosti. Na vstup hashovacích funkcií je možné priviesť napríklad textovú správu alebo súbory rôzneho typu. Výstupu hašovacej funkcie hovoríme digitálny odtlačok (hash). Digitálny odtlačok je reťazec,

ktorého dĺžka je pevne stanovená. Je to zvyčajne hodnota rádovo niekoľkokrát menšia ako hodnota na vstupe funkcie. Napriek tomu, príslušná výstupná hodnota jednoznačne identifikuje hodnotu pôvodnej správy, z ktorej bola vygenerovaná. Okrem toho je nutné zabezpečiť ďalší predpoklad, a to bezkolíznosť. Bezkolíznosť v praxi znamená, že nebude možné vytvoriť dva rovnaké odtlačky z dvoch rôznych vstupných hodnôt. Predpokladajme, že máme k dispozícii súbor údajov A, ku ktorému vytvoríme digitálny odtlačok $H(x_0)$. Potom musí platiť, že $H(x_0)$ nesmie byť zhodné so žiadnym iným $H(x_n)$. Ak máme výstup funkcie pre súbor údajov A, tak pri súčasnej výpočtovej sile počítačov by malo trvať veľmi dlho, aby sme našli taký súbor údajov B, ktorého odtlačok by bol zhodný s odtlačkom súboru A. [6][7]

Hashovacia funkcia musí zabezpečiť pri zmene čo i len jediného bitu na vstupe funkcie vyvolanie maximálnej zmeny výstupnej hodnoty. Z toho ďalej vyplýva, že pomocou hašovacích funkcií sme schopní jednoducho zistiť akúkoľvek zmenu na vstupe funkcie a tým môžeme jednoznačne odhaliť, či bola porušená integrita spracovávaných údajov. [5]

1.1.4 Strom Merkle tree

Strom vytvorený spájaním spárovaných dát tzv. listy, nasledujúc párovaním a šifrovaním výsledkov, kým nezostane iba jeden hash tzv. Merkle root. V kryptomenách sú listy takmer vždy transakcie z jedného bloku.[4]

1.1.5 Uzol Merkle root

Je koreňový uzol stromu merkle tree. Je to potomok všetkých zašifrovaných dvojíc v strome. Hlavičky blokov musia obsahovať platný merkle root, ktorý pochádza zo všetkých transakcií v tomto bloku.[4]

1.2 Teoretické hľadisko kryptomien a ich technológií

1.2.1 Peer to peer sieť

Peer to peer znamená rovný s rovným a označuje sa tiež ako P2P sieť. Všetky počítače v sieti sú rovnocenné. Každá stanica v sieti môže vyčleniť nejaký svoj prostriedok (diskový priestor, tlačiareň, mechaniku) na zdieľanie. Iná stanica môže tieto prostriedky využívať. Tento typ siete obvykle nemá centrálnu správu, každý uzol sa spravuje sám. Zdieľanie prostriedkov je možné aj cez internet. [8]

1.2.2 Digitálna mena

Digitálna mena je typ meny dostupný výhradne v digitálnej forme, a teda nie vo fyzickej. Vykazuje vlastnosti podobné fyzickým menám, ale umožňuje okamžité transakcie a bezhraničný prevod vlastníctva. [4]

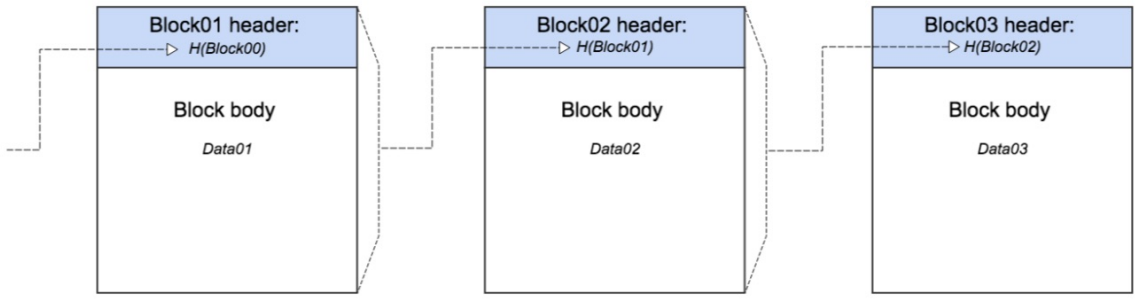
1.2.3 Kryptomena

V jednoduchosti, môžeme povedať, že **kryptomena** je digitálne aktívum, ktoré je vytvorené tak, aby slúžilo ako prostriedok výmeny, a to za pomoci technológie kryptografie, ktorá slúži na zabezpečenie transakčného toku, ako aj riadenia vytvárania ďalších jednotiek takejto meny. Pojem kryptomena tiež pomenúva platobný systém a zároveň sieť danej kryptomeny. Preto sa môžeme stretnúť s označovaním danej kryptomeny ako systém či sieť. [9]

1.2.4 Blockchain

Blockchain by sme mohli nazvať reťazcom blokov, v ktorých sú alokované záznamy o každej vykonanej transakcii. Často sa to označuje ako účtovná kniha danej kryptomeny. Poradie blokov nie je náhodné, určuje poradie, v akom sa transakcie uskutočnili. Reťazec blokov slúži na potvrdenie toho, že odosielateľ naozaj kryptomenu vlastnil a transakcia sa uskutočnila. Nový blok je pripojený k predchádzajúcemu bloku reťazca, za určitý čas, ktorý môže byť rôzny v závislosti od konkrétnej kryptomeny. [10]

Na obrázku č.1 môžeme vidieť následnosť blokov v blockchaine. Hlavička sa vždy skladá z hashu predchádzajúceho bloku.



OBRÁZOK Č. 1- VŠEOBECNÁ ŠTRUKTÚRA BLOCKCHAINU [21]

1.2.5 Hashrate – hashovacia sila

Hash Rate, alebo tiež hashovacia sila je meracia jednotka, ktorá meria, koľko sieť danej kryptomeny spotrebúva energie, aby bola nepretržite funkčná. Tým, že bude

nepretržite funkčná, je myslené, koľko spotrebuje energie, na generovanie alebo nájdenie blokov v normálnom priemernom čase validácie bloku transakcií.[4]

Hashovacia sila je jednotka meraná v hashoch za sekundu (h/s). V tabuľke č.1 uvádzam jeho zvyčajné nominálne hodnoty, ktoré môže hashrate nadobúdať.

1 kH / s	1000 hash / s
1 MH / s	1 000 000 hash / s
1 GH / s	1 000 000 000 hash / s
1 TH / s	1 000 000 000 000 hash / s
1 PH / s	1 000 000 000 000 000 hash / s
1 EH / s	1 000 000 000 000 000 000 hash / s

TABUĽKA Č. 1– NOMINÁLNE HODNOTY HASHOVACEJ SILY.[12]

1.2.6 Náročnosť

Náročnosť je parameter, ktoré používajú kryptomeny na udržanie priemerného času medzi validáciou blokov v stabilnej miere, aj keď sa v danom systéme kryptomeny mení hashrate. Tento parameter poukazuje na to ako ťažké je nájsť hash pod konkrétnym cieľom.[4]

Vytvorenie jednoduchého hashovania pre súbor transakcií by bolo triviálne pre moderný počítač, takže aby sa proces premenil na prácu, sieť kryptomeny vytvára určitú **úroveň náročnosti**. Toto nastavenie je nastavené tak, aby bol nový blok vyťažený a teda pridaný do blockchainu vygenerovaním validného hashu za stanovený čas. Nastavenie úrovne náročnosti sa dosahuje vytvorením cieľa pre hash. Čím nižší je cieľ, tým menšia je množina validných hashov a tým je ťažšie vytvoriť hash. Ak by však používateľ zmenil čo i len jednu sumu transakcie o 0,0001 bitcoin, výsledný hash by nebol rozpoznateľný a sieť by zistila a následne odmietla podvod.[11]

1.2.7 Cieľ

Cieľ je veľmi veľké číslo, ktoré zdieľajú všetci klienti danej kryptomeny. Hash SHA-256 hlavičky bloku musí byť menší alebo rovný aktuálnemu cieľu pre blok, aby bol prijatý sieťou. Čím je cieľ menší, tým je ťažšie vygenerovať blok.[4]

1.2.8 Závislosť hashrate a náročnosti

Hashrate a náročnosť sú vzájomne závislé rôznymi spôsobmi. Kedykoľvek sa zvýši náročnosť v sieti, je potrebná aj väčšia hash sila, aby sa mohli ťažiť alebo nájsť bloky a ako výsledok ťažiari získali blokovú odmenu. Zaujímavosťou je, že náročnosť tej-ktorej kryptografickej siete sa zvyšuje pretože viac baníkov sa pripája do siete, a preto je potrebné zvýšiť hashrate. To znamená, že je potrebné viac výpočtových odhadov za sekundu na nájdenie riešenia).[12]

1.2.9 Kapitalizácia trhu

Kapitalizácia trhu poukazuje na celkovú trhovú hodnotu akcií spoločnosti. Pri normálnych okolnostiach sa vypočíta ako počet všetkých vydaných akcií spoločnosťou vynásobenou aktuálnou trhovou cenou jednej akcie. Investičná komunita používa tento ukazovateľ na určenie veľkosti spoločnosti na rozdiel od ukazovateľov ako sú predaj a celkové aktíva spoločnosti. Keďže systémy kryptomien vo všeobecnosti nevydávajú kryptomeny ako svoje akcie, tak musí byť kapitalizácia trhu mierne modifikovaná v tejto súvislosti. Spoločnosti nahradia systémy kryptomien, vydané akcie nahradia kryptomeny v obehu, a cenu akcie nahradí aktuálna cena jednotky danej kryptomeny. Takže kapitalizáciu trhu v tomto prípade môžeme vypočítať ako počet jednotiek danej kryptomeny v obehu vynásobených ich trhovou hodnotou.[13]

1.3 Ťažba kryptomien

1.3.1 Ťažba

Ťažba kryptomien môže byť definovaná ako validácia transakcií danej kryptomeny za účelom vytvorenia nových jednotiek tejto meny. Validáciu sprostredkúvajú samotní užívatelia daného systému kryptomeny. Je na to potrebný softvér a hardvér s dostatočným výkonom. Takíto používatelia sa nazývajú ťažiari. [4]

1.3.2 Ťažiarske pooly

Ťažiarske pooly sú skupiny spolupracujúcich ťažiarov, ktorí súhlasia so zdieľaním blokových odmien v takom pomere s akou hashovacou silou prispievajú do ťažby. Ťažiarske pooly sú pre bežného ťažiara vhodnou voľbou, pretože dostávajú stabilnejšie odmeny a robia tieto odmeny tiež predvídateľnejšími. Mineri sa však môžu kedykoľvek rozhodnúť presmerovať svoju hashovú silu do iného ťažiarskeho poolu.[14]

1.3.3 ASIC

Application Specific Integrated Circuits sú zariadenia špeciálne navrhnuté tak, aby robili len jednu činnosť a to ťažbu určitej kryptomeny s extrémnou rýchlosťou a relatívne nízkou spotrebou energie. Pretože tieto čipy sú špeciálne navrhované na túto úlohu, môžu byť drahé a časovo náročné na výrobu. [15]

1.4 Konsenzus

Mechanizmus konsenzu je mechanizmus tolerantný voči chybám, ktorý sa používa v počítačových a blokových systémoch na dosiahnutie potrebnej dohody o jednotnej dátovej hodnote alebo o jedinom stave siete medzi distribuovanými procesmi alebo systémami s viacerými agentmi. Okrem iného je užitočné pri vedení záznamov. V každom centralizovanom systéme, ako je databáza obsahujúca kľúčové informácie o vodičských preukazoch v krajine, má centrálny správca oprávnenie na údržbu a aktualizáciu databázy. Úloha vykonávania akýchkoľvek aktualizácií - ako je pridanie, vymazanie alebo aktualizácia mien osôb, ktoré sa kvalifikovali pre určité licencie - vykonáva ústredný orgán, ktorý zostáva jediným zodpovedným za vedenie skutočných záznamov. Verejné blockchainy, ktoré fungujú ako decentralizované, samoregulačné systémy pracujú v globálnom meradle bez jedinej autority. Zahŕňajú prispievanie od stoviek tisíc účastníkov, ktorí pracujú na overovaní a autentifikácii transakcií, ktoré sa vyskytujú v blockchaine, a na ťažiarskych činnostiach blokov. V takomto dynamicky sa meniacom štatúte blockchainu tieto verejne zdieľané záznamy potrebujú efektívny, spravodlivý, funkčný, spoľahlivý a bezpečný mechanizmus fungujúci v reálnom čase, ktorý zabezpečí, aby všetky transakcie, ktoré sa vyskytujú v sieti, boli pravé a všetci účastníci sa dohodli na konsenze o stave záznamu o transakciách. Táto dôležitá úloha sa vykonáva prostredníctvom konsenzuálneho mechanizmu, ktorý je súborom pravidiel, ktoré rozhodujú o príspevkoch rôznych účastníkov blockchainu.[16]

Predstavíme si 2 mechanizmy konsenzu:

- Proof of stakes
- Proof of work

1.4.1 Proof of stakes

Koncept dôkazu o vklade (Proof of Stakes) hovorí, že osoba môže ťažiť alebo overovať blokové transakcie vzhľadom k tomu, koľko jednotiek kryptoemny má. To znamená, že čím viac kryptomincí ťažiar vlastní, tým viac má ťažiarskeho výkonu. Dôkaz o vklade bol vytvorený ako alternatíva k dokladu o práci. Po spustení transakcie sa údaje o transakcii vložia do bloku s maximálnou kapacitou 1 megabajt a potom sa duplikujú na viacerých počítačoch alebo uzloch v sieti. Uzly sú administratívnym orgánom blockchainu a overujú oprávnenosť transakcií v každom bloku. Ak chcete vykonať overovací krok, uzly alebo ťažiari budú musieť vyriešiť výpočtovú hádanku známu ako dôkaz o práci. Prvý ťažiar, ktorý dešifruje každý transakčný problém bloku, dostane odmenu v podobe kryptomincí. Po overení bloku transakcií sa pridá k blockchainu, verejnému transparentnému záznamu.[17]

1.4.2 Proof of Work

Doklad o práci (proof of work) opisuje systém, ktorý vyžaduje nie zanedbateľné, ale realizovateľné úsilie na odvrátenie ľahkovážneho alebo škodlivého používania výpočtovej sily, ako je odosielanie spamových e-mailov alebo spustenie útokov odmietnutia služby (denial of service attack). Tento koncept bol v roku 2004 adaptovaný k peniazom vďaka Hal Finney-mu prostredníctvom myšlienky opätovne použiteľného dokladu o práci. Po zavedení v roku 2009 sa Bitcoin stal prvou široko prijatou aplikáciou Finneyho myšlienky. Zaujímavosťou je, že Finney bol tiež príjemcom prvej transakcie bitcoin. Doklad o práci je základom mnohých ďalších kryptomien.[18]

1.5 Predstavenie vybratých kryptomien

1.5.1 Bitcoin

Bitcoin je peer to peer platobná sieť elektronických peňazí umožňujúca posielanie online platieb priamo od jednej strany k druhej bez zahrnutia akejkoľvek finančnej inštitúcie. [19]

Bitcoin je virtuálna menová jednotka a preto nemá žiadnu fyzickú reprezentáciu. Bitcoin je tiež kryptomena a označuje sa skratkou BTC. Bitcoin ako platobná sieť zaznamenáva všetky transakcie kryptomeny bitcoin.[19]

Uzlami v takejto P2P sieti sú všetky počítače, s nainštalovaným príslušným softwarovým vybavením. Každý uzlový bod overí, uchová a distribuuje informácie

všetkým ostatným uzlovým bodom, ktoré sú v sieti pripojené. Takto je zaistené šírenie informácií v rozsahu celej sieti. Protokol Bitcoin je open-source a je neustále zlepšovaný vývojárskou komunitou, na dosiahnutie konsenzu medzi všetkými používateľmi siete. Hashovacia funkcia, ktorá sa používa v systéme Bitcoin je SHA-256, ktorá bola pôvodne navrhnutá agentúrou NSA v USA. Algoritmus SHA bol rozsiahle analyzovaný a vyhlásený za bezpečný. SHA-256 je aktualizácia z algoritmu SHA-1 a v súčasnosti sa používa v systéme Bitcoin na digitálne podpisy, ktoré zabezpečujú transakcie a ich ukladanie do blockchainu a tvoria základ matematického problému dôkazu o práci (Proof of work). [4]

Kompresná funkcia SHA-256 funguje na 512-bitovom bloku správ a na 256-bitovej medziľahlej hash hodnote. Ide v podstate o 256-bitový blokový šifrovací algoritmus, ktorý zašifruje medziľahlú hodnotu hash pomocou blokovej správy ako kľúča. [20]

1.5.2 Ethereum

Ethereum obdržalo počiatočné financovanie v roku 2014 ako vývojový projekt kolektívneho financovania, ktorý sa predstavuje ako vylepšený protokol Bitcoinu. Vylepšenie hodnoty oproti Bitcoinu spočíva v tom, že Ethereum má byť niečim viac než len kryptomenou. A to tak, že umožňuje funkcionality ako definovanie a vykonávanie tzv. inteligentných zmlúv resp. kontraktov na svojom blockchaine. Ethereum funguje ako platforma. Užívatelia tohto systému môžu navrhovať decentralizované aplikácie ako druhú vrstvu na povrchu Etherea – Ethereum by mal byť globálny virtuálny stroj dostupný pre každého. K uľahčeniu tejto funkcionality, Ethereum poskytuje stavový blockchain s ukladacími možnosťami a vlastný skriptovací jazyk s názvom Turing-complete. Ethereum navyše vytvára svoju vlastnú menu - Ether - ktorá má pre systém vnútornú hodnotu, ktorá je tiež palivom systému Ethereum. [21]

Inteligentné kontrakty sú zmluvy s vlastnou realizáciou, pričom podmienky dohody medzi kupujúcim a predávajúcim sú priamo zapísané do riadkov kódu. Kód a dohody, ktoré sú v ňom obsiahnuté, existujú v distribuovanej, decentralizovanej blockchainovej sieti. Inteligentné zmluvy umožňujú realizovať dôveryhodné transakcie a dohody medzi rôznymi, anonymnými stranami bez potreby centrálneho orgánu, právneho systému alebo externého mechanizmu presadzovania práva. Robia transakcie sledovateľné, transparentné a nezvratné.[22]

Systém Ethereum je založený a vyvíjaný nadáciou The Ethereum Foundation. The Ethereum Foundation má na starosti rozvíjanie špecifikácií pre protokol Ethereum, ako aj niekoľko typov open-source klientov, ktoré dokážu prevádzkovať protokol.[23]

Účty sú stavové objekty Etherea. Transakcie do účtov a z účtov spôsobujú zmeny stavov účtov. Napríklad pravidelný prevod finančných prostriedkov by spôsobil aktualizáciu zostatku účtu a zmenu stavu účtu. Existujú dva typy účtov, ktoré sú definované tým, ako sú vytvorené a ako sú kontrolované:

- externe vlastnené účty
- zmluvné účty [24]

Externe vlastnený účet môže byť vytvorený každým. Pár verejného a súkromného kľúča pre externe vlastnený účet je generovaný pomocou generovania kľúčov ECDSA a adresa účtu sa potom odvodí z výstupného verejného kľúča. Súkromný kľúč musí byť chránený, pretože ten, kto má súkromný kľúč, má pod kontrolou finančné prostriedky na účte. Externe vlastnené účty sú identifikované ich adresou - kde adresa je posledných 160 bitov hash verejného kľúča.[24]

Zmluvný účet sa vytvorí vykonaním transakcie o vytvorení zmluvy z externe vlastneného účtu. Transakcia o vytvorení zmluvy špecifikuje programový kód pre nový účet. Tento kód kontroluje správanie zmluvy v budúcich transakciách. Zmluvné účty možno považovať za autonómnych agentov, ktorí ožijú, keď sú s nimi viazaní prostredníctvom iných transakcií. Zmluva má prístup na čítanie a zápis do ukladacieho priestoru svojho účtu a môže využiť tento prístup, ak bol pôvodný kód správne vytvorený. Kód, s ktorým bola zmluva inicializovaná je však po vytvorení zmluvy nemenný. Zmluvy môžu tiež vytvárať nové zmluvy, ak sú definované v pôvodnom kóde. Keďže zmluvný účet je kontrolovaný implicitným kódom na zmluvnom účte, nemá pridružený žiaden súkromný či verejný kľúč. Bez verejného kľúča na odvodenie adresy sa adresa zmluvného účtu vygeneruje ako posledných 160 bitov z hodnoty hashu odvodeného z adresy odosielajúcej adresu účtu a nonce.[24]

Generický stavový objekt účet sa skladá zo štyroch polí a je identifikovaný 160-bitovým číslom s názvom Adresa. V závislosti od toho, s akým typom účtu sa zaoberáme polia dát v účte budú nadobúdať rôzne hodnoty a vlastnosti. [21]

V tabuľke č.2 môžeme vidieť všeobecný formát stavového objektu účet.

nonce	Počítadlo, ktoré sa zvyšuje na základe počtu odoslaných transakcií a zmlúv vytvorených účtom.
balance	Hodnota vlastnená týmto účtom.
storageRoot	Koreňový hash stromu Merkle Patricia, ktorý tvorí úložisko účtu.
codeHash	hash kódu, ktorý určuje, ako má účet fungovať. Toto je prázdne, ak je účet externým typom účtu.

TABUĽKA Č. 2 – VŠEOBECNÝ FORMÁT OBJEKTU ÚČET [21]

V Ethereu existujú dva dôležité kryptografické prvky: funkcia hash a digitálny podpis. Ethereum využíva neštandardnú verziu SHA3 – Keccak pre svoje hashovacie operácie. Rovnaké vlastnosti zabezpečenia pre SHA3 sa vzťahujú aj na Keccak, existujú však niektoré implementačné rozdiely. [21]

SHA3 Keccak patrí do rodiny hashovacích funkcií Secure Hash Algorithm-3 (SHA-3) pracujúcich na binárnych dátach. Každá z funkcií SHA-3 je založená na inštancii algoritmu KECCAK, ktorá bola vybraná za víťaza súťaže SHA-3 Cryptographic Hash Algorithm. Tento štandard tiež špecifikuje skupinu matematických permutácií KECCAK-p vrátane permutácie, ktorá je základom KECCAK, ktorá môže slúžiť ako hlavné zložky ďalších kryptografických funkcií, ktoré môžu byť špecifikované v budúcnosti. Skupina SHA-3 sa skladá zo štyroch kryptografických hashových funkcií a dvoch rozšíriteľných výstupných funkcií. Kryptografické hashovacie funkcie sa nazývajú SHA3-224, SHA3-256, SHA3-384 a SHA3-512. Pre hashovacie funkcie sa vstup nazýva správa a výstup sa nazýva zhrnutie (správy) - hodnota hashu. Dĺžka správy sa môže síce meniť, ale dĺžka hashu je pevná. Kryptografická hashovacia funkcia je hashovacia funkcia, ktorá je navrhnutá tak, aby poskytovala špeciálne vlastnosti vrátane odolnosti proti kolíziám a odolnosti voči vzorovaniu kódu, ktoré sú dôležité pre mnoho aplikácií v oblasti

informačnej bezpečnosti. Napríklad šifrovacia funkcia zvyšuje bezpečnosť a efektívnosť digitálneho podpisu, keď je hash digitálne podpísaný namiesto samotnej správy. V tomto kontexte odolnosť hash funkcie proti kolízii poskytuje istotu, že pôvodná správa nemohla byť zmenená na inú správu s rovnakou hodnotou hash, a teda rovnakým podpisom. Iné aplikácie kryptografických hashových funkcií zahŕňajú generovanie bitov pseudonáhodnosti, kódy autentifikácie správ a funkcie odvodzovania kľúčov. [25] [26]

1.5.3 Dash

Dash (DASH) je digitálna mena zameraná na súkromie s okamžitými transakciami. Je založená na bitcoinovom softvéri, ale má dvojvrstvovú (resp.dvojstupňovú) sieť, ktorá ju zlepšuje. Dash vám umožňuje zostať v anonymite, keď uskutočňujete transakcie podobne ako je to pri platbe v hotovosti. [27]

Masternódy sú počítače, ktoré vedú Dash peňaženku a robia rozhodnutia, ako napríklad zamknutie transakcií s okamžitým odoslaním, koordinovanie miešania kryptomincí a hlasovanie o rozpočtovom financovaní. Masternódy musia mať minimálne 1000 Dash, špeciálnu IP adresu a musia byť schopné bežať 24 hodín denne bez straty pripojenia viac ako na 1 hodinu. Masternódy dostanú zaplatené 45% blokovej odmeny na každom bloku, ktorý sa rozdeľuje na masternódy jeden po druhom. Obvykle sa každých 7 dní vypláca každému masternode približne 2 dashe. [27]

Kryptomena Dash používa hashovaciu funkciu X11 na šifrovanie transakcií. X11 je široko používaný hashovaci algoritmus, ktorý využíva iný netradičný prístup známy ako spájanie algoritmov. X11 pozostáva zo všetkých jedenástich SHA3 algoritmov, každý hash je vypočítaný a potvrdený do ďalšieho algoritmu v reťazi. Použitím viacerých algoritmov je pravdepodobnosť, že bude ASIC zariadenie vytvorené pre menu minimálna až do neskoršej časti jej životného cyklu.[27]

1.5.4 Ripple

Ripple je decentralizovaný platobný systém založený na kreditných sieťach. Tento platobný systém prišiel na trh spolu s vlastným tokenom s názvom XRP. Zdrojový kód je typu open-source a teda je k dispozícii pre verejnosť. To znamená, že ktokoľvek môže disponovať inštanciou Ripple. Uzly môžu zastávať až tri rôzne úlohy v Ripple:

- **používatelia**, ktorí uskutočňujú a prijímajú platby,
- **tvorcovia trhu**, ktorí pôsobia ako obchodníci v systéme, a

- **overovanie serverov**, ktoré vykonáva konsenzusový protokol spoločnosti Ripple, s cieľom skontrolovať a overiť všetky transakcie, ktoré sa uskutočňujú v systéme [28]

Ripple protokol používajú aktéri rôznych inštitúcií, ako sú veľké banky a obchody s peňažnými službami. Funkcia natívneho tokenu s názvom XRP má slúžiť ako spojovacia mena medzi národnými menovými pármi, ktoré sa zriedka obchodujú, a zabrániť tak spamovým útokom. [30]

Menový pár je štruktúra cien a kurzov mien obchodovaných na forexovom trhu. Hodnota meny je kurz (rate) a je určený jeho porovnaním s inou menou. Prvá uvedená mena menového páru sa nazýva základná mena a druhá mena sa nazýva kótovacia mena. Menový pár udáva, koľko kótovacej meny je potrebné na nákup jednej jednotky základnej meny.[31]

Ripple užívatelia sú odkazovaný pomocou pseudonymov. Používatelia majú verejný a súkromný kľúč. Ak používateľ chce odoslať platbu inému používateľovi, kryptograficky podpíše prevod peňazí denominovaných vo vlastnej mene spoločnosti Ripple - XRP alebo v akejkoľvek inej mene. V prípade platieb uskutočnených v menách, ktoré nie sú v systéme XRP, spoločnosť Ripple nemá žiadny spôsob, ako vymáhať platby, a zaznamenáva len čiastky dlžné jedným subjektom druhému subjektu. Konkrétnejšie v tomto prípade systém Ripple implementuje systém distribuovanej kreditnej siete. [29]

2 Cieľ práce, metodika práce a metódy skúmania

Primárnym cieľom bakalárskej práce je charakteristika a porovnanie vybraných kryptomien z hľadiska vybraných kritérií. Výsledok práce má poukázať na diverzitu porovnávaných kryptomien aj napriek tomu, že majú niektoré charakteristiky a technológie rovnaké resp. podobné. Sekundárnym cieľom je implementácia blockchainovej technológie v programovacom jazyku a poukázanie na jeho vlastnosti.

Objektami porovnávania v bakalárskej práci sú kryptomeny Bitcoin, Ethereum, Dash a Ripple. Ako všeobecne stanovené kritériá som vybral nasledujúce:

- technológiu verejného záznamu
- operácie, s ktorými daná kryptomena pracuje
- konsenzus
- Validácia operácií
- trhová kapitalizácia a cena danej kryptomeny

Porovnávané kryptomeny budem porovnávať s kryptomenou Bitcoin, pretože tvorí základ moderných kryptomien, keďže bola prvou zo všetkých porovnávaných objektov a vďaka svojmu veľkému úspechu si z nej väčšina neskôr vzniknutých kryptomien vzala príklad. Preto som pre ostatné kryptomeny vybral ďalšie kritérium- Iné odlišnosti a inovácie.

V bakalárskej práci „Kryptomeny“ som využil nasledovné výskumné metódy: logická analýza literatúry a publikácií spojených s problematikou kryptomien a technológií spojených s nimi. Vďaka tejto metóde sa mi podarilo vytvoriť si potrebný rešerš k danej problematike, čím som získal kvalitný zdroj informácii na vytvorenie tejto práce. V teoretickej časti som vysvetlil základné pojmy potrebné na pochopenie kryptomien ako takých, ale aj porovnávaných kritérií.

V praktickej časti som vďaka komparácii vybraných kryptografických mien poukázal na odlišnosti ale aj spoločné vlastnosti a technológie. Dané kryptomeny som porovnával na základe stanovených kritérií, keď som vysvetlil fungovanie danej oblasti a hneď poukázal na odlišnosti voči Bitcoinu. Kryptomeny sú porovnávané jedna po druhej a na konci každej je súhrn odlišností voči Bitcoinu. Výsledky práce sú zapisované v priebehu porovnávania, pričom na konci každého porovnania Bitcoinu s danou menou sa nachádza aj súhrn odlišností.

V záverečnej časti praktickej časti som poukázal na spoločný menovateľ týchto mien, ktorou je blockchainová technológia. V zjednodušenej podobe som ju implementoval v jazyku Java a vysvetlil na príklade niektoré vlastnosti.

3 Výsledky práce a diskusia

3.1 Kritéria porovnania pre kryptomeny

Technológia verejného záznamu

Tento pohľad priblíži technológiu distribuovanej databázy, ktorá je jedným zo základných technologických pilierov každého kryptografického platobného systému. Táto databáza sa zväčša prejavuje svojou nemennosťou záznamov, čím sa dosahuje u používateľov dôvera.

Operácie

Systémy kryptomien sa môžu líšiť ako vo svojich funkcionalitách, tak aj vo forme komunikácie a teda aj základných operáciách, ktoré sú sledované a zaznamenávané v rámci toho-ktorého systému.

Konsenzus

Vybraté kryptomeny môžu poukazovať na rôzne správania sa v spojitosti s verejnou dohodou v sieti – konsenzom.

Validácia operácií

Tento pohľad nám dovolí nahliadnuť do validácie základných operácií napr. Transakcií. V závislosti od danej kryptomeny sa môžu procesy líšiť. Priblížim tiež čas potrebný na validáciu operácií, veľkosť bloku a tiež náročnosť validácie.

Iné odlišnosti a inovácie

Tento pohľad priblíži aké inovácie naviac kryptomeny majú. Keďže za základnú kryptomenu považujem Bitcoin, inovácie sa budú týkať ostatných porovnávaných kryptomien. Toto je spôsobené hlavne tým, že Bitcoin bol prvou známou kryptomenou a ďalšie sa od neho inšpirovali. Takže by bolo veľmi nepravdepobné, že by Bitcoin mal technologicky niečo viac ako oveľa mladšie kryptomeny.

Kapitalizácia trhu a hodnota danej kryptomeny

Keďže hodnota jednotky kryptomeny a kapitalizácia trhu sú so sebou úzko spojené, môžeme si všimnúť, že ich krivky budú vždy totožné. Kapitalizácia trhu preto bude značiť o rozšírenosti konkrétnej kryptomeny, ktorá je určovaná krivkou dopytu a ponuky po danej kryptomene.

3.2 Bitcoin

3.2.1 Technológia verejného záznamu - Blockchain

Bitcoin blockchain je decentralizovaný blokový záznam systému Bitcoin, ktorý obsahuje záznamy o všetkých predchádzajúcich bitcoinových transakciách vrátane vytvorenia nových jednotiek Bitcoin. Bitcoin blockchain sa skladá zo série blokov, kde každý blok nadväzuje na svojich predchodcov a obsahuje informácie o nových bitcoinových transakciách. Prvý blok, blok s číslom 0, bol vytvorený v roku 2009. V čase písania tejto práce bol blok s číslom 519625 pripojený ako posledný blok pridaný do blockchainu. Keďže je to verejný záznam každý si môže stiahnuť a prečítať Bitcoin blockchain. Každý účastník môže slobodne spravovať svoju vlastnú kópiu databázy. Momentálna veľkosť bitcoinového blockchainu dosahuje veľkosť 197.76 GB. [32] [33]

3.2.2 Operácie

V systéme Bitcoin sú jediným druhom operácie transakcie, ktoré sa zaznamenávajú v decentralizovanom zázname transakcií s názvom blockchain. Obsah platobnej transakcie v sebe môže mať ľubovoľný počet vstupných a výstupných údajov. Vstupný údaj pozostáva z odkazu na výstupný údaj z predchádzajúcej transakcie. Výstupný údaj pozostáva z adresy doručenia a posielanej čiastky. [4]

V tabuľke č.3 môžeme vidieť formát transakcie v Bitcoine aj so stručným popisom a vymedzením veľkosti.

pole	Popis	Veľkosť
Version number	Číslo verzie	4 bajty
In-Counter	Kladné celé číslo – počítadlo vstupov.	1-9 bajtov
List of inputs	Zoznam vstupov. Prvá vstup prvej transakcie sa zvykne nazývať coinbase	<in-counter> počet vstupov
Out-counter	Kladné číslo – počítadlo výstupov	1-9 bajtov
List of outputs	Zoznam výstupov	<out-counter> počet výstupov
Lock time	Časová známka	4 bajty

TABUĽKA Č. 3 - FORMÁT TRANSAKCIE V BITCOINE [21]

3.2.3 Konsenzus v Bitcoine

V systéme Bitcoin je použitý tzv. Proof of work (PoW) mechanizmus, z čoho vyplýva, že systém požaduje od používateľa určitý výpočet, ktorý stojí ako čas tak aj energiu a za to ho systém odmení. Výpočty, o ktorých hovoríme sú čisto náhodné a riadia sa tzv. pokus-omyl spôsobom. Práve preto platí fakt, že čím väčšia výpočtová sila, tým väčšia pravdepodobnosť, že sa danému užívateľovi výpočet podarí začo budú jeho odmenou bitcoiny. [19]

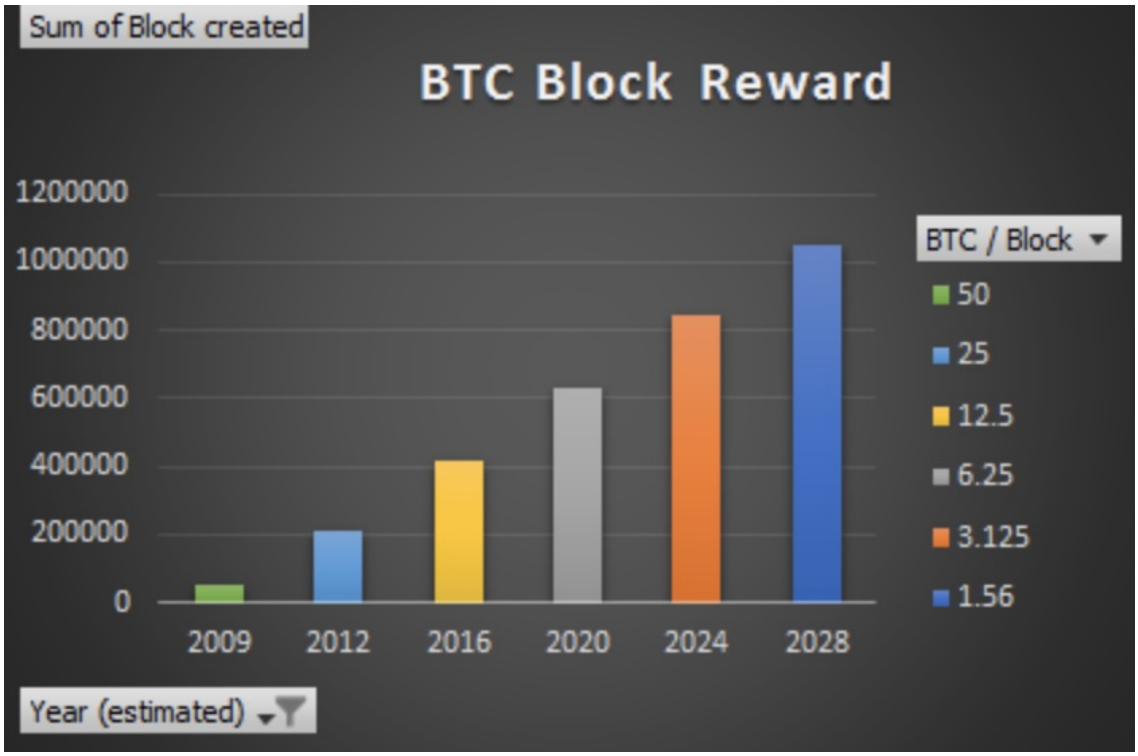
Konsenzusový protokol Bitcoinu bol nazvaný Nakamoto Consensus vďaka pôvodnej myšlienke od Satoshi Nakamota. Stratégiu možno zhrnúť jednoduchou vetou: Najväčší reťazec vyhrá. Znamená to, že ak je uzol siete predstavený s viac ako jedným blokom, ktorý nie je súčasťou toho istého reťazca t.j. vetvenie blockchainu, tak je doporučeným postupom zostať v reťazci, ktorý má najviac blokov. Ak má nejaká vetva rovnaké množstvo blokov, blok s najvyššou náročnosťou vyhrá. [21]

3.2.4 Validácia operácií

Ťažba

Aby sme pochopili mechanizmus systému Bitcoin, musíme najprv diskutovať o úlohe ťažiarov. Ťažiar zbiera čakajúce bitcoinové transakcie, overuje ich legitímnosť a zostaví ich do formy známej ako kandidát na blok. Motiváciou robiť túto aktivitu je získať novovytvorené bitcoinové jednotky. Ťažiar v tomto uspeje, ak dokáže presvedčiť všetkých ostatných účastníkov siete, aby pridali jeho kandidáta na blok k bitcoinovému blockchainu. Odmenou za tzv. vyťaženie bloku je momentálne 12,5 BTC. Výška odmeny klesá o polovicu každých 210 000 blokov, alebo asi každé 4 roky. Takže výška tejto odmeny najbližšie klesne z 12.5 na 6.25 bitcoinu. Toto sa stane 28.mája 2020. Keď Bitcoin začínal, odmena za úspešné vyťaženie bloku bolo 50 bitcoinov. Bitcoinov je obmedzený počet a to 21 000 000. Akonáhle sa všetky vyťažia, už nebudú vydané žiadne ďalšie. [4] [34]

Na obrázku č.2 môžeme vidieť stĺpcový graf, ktorý vyjadruje znižovanie blokovej odmeny v nepriamej úmere s pribúdaním Bitcoinov.



OBRÁZOK Č. 2 – ZNIŽUJÚCA SA ODMENA S PRIBÚDAJÚCIMI BITCOINAMI V OBEHU [35]

V životnom cykle Bitcoinu sa začala ťažba fanúšikmi, ktorí používali procesory na ťaženie tejto kryptomeny. V neskoršej časti životného cyklu však ťažbu pomocou procesorov CPU nahradila ťažba pomocou grafických čipov GPU. Roky po cykle GPU boli vytvorené ASIC alebo Application Specific Integrated Circuits, ktoré rýchlo nahradili jednotky GPU. [4]

Ťažba bitcoinov je bez obmedzení. Ktokoľvek sa môže stať ťažiarom, stačí si stiahnuť príslušný software a najaktuálnejšiu kópiu bitcoinového blockchainu. V praxi však existuje niekoľko veľkých ťažiarskych poolov, ktoré produkujú väčšinu nových všeobecne prijatých blokov.. Dôvodom je, že konkurencia sa stala obrovskou a iba veľké ťažobné farmy s vysoko špecializovaným hardvérom a ťiež s prístupom k lacnej elektrickej energii môžu stále profitovať z ťažby bitcoinov.[4]

Veľkosť bloku

Každý jeden ťažiar má k dispozícii celú históriu vykonaných transakcií, čiže každý môže zistiť kto je v konkrétnom okamihu vlastníkom bitcoinov. Transakcie sú uložené do blokov. Množstvo transakcií v danom bloku môže byť rôzne a vychádza z veľkosti konkrétnych transakcií. Bloková veľkosť má obmedzenú kapacitu 1MB pre zabezpečenie jeho rýchlej distribúcie bez akýchkoľvek chýb a problémov. Počet vstupov a výstupov transakcie určuje veľkosť samotnej transakcie.[19]

Nasledujúca tabuľka reprezentuje blok, ktorý sa skladá z 2 častí:

- hlavička – znázornená žltou farbou
- telo – znázornené modrou farbou

Samotné transakcie sa nachádzajú v tele bloku, zatiaľ čo hlavička pozostáva zo siedmich polí. Prvou transakciou je špeciálna coinbase transakcia, ktorá úspešnému ťažiarovi poskytne bitcoiny ako odmenu za ťažbu. [36]

V tabuľke č.4 máme znázornený formát bloku v bitcoinovom blockchaine.

Version	02000000
Previous block hash (reversed)	1dbd981fe6985776b644b173a4d0385d dc1aa2a829688d1e0000000000000000

Merkle root (reversed)	e320b6c2fffc8d750423db8b1eb942a e710e951ed797f7affc8892b0f1fc122b
Timestamp	358b0553
bits	535f0119
nonce	48750833
Transaction count	87
Coinbase transaction	
transactions	

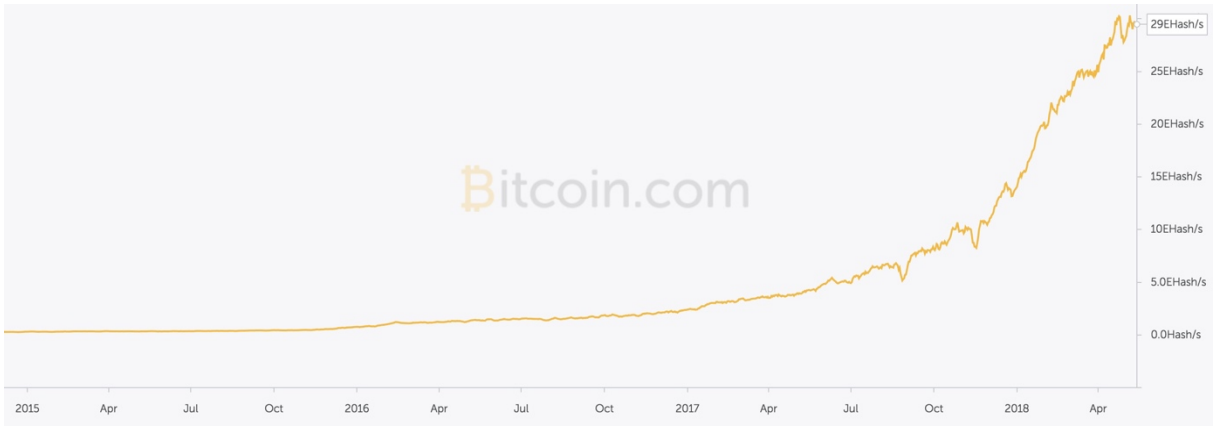
TABUĽKA Č. 4– FORMÁT BLOKU V SYSTÉME BITCOIN [36]

Pole version hovorí o verzii softvéru, používaného ťažiarom, ktorý daný blok vygeneroval. Políčko s názvom previous block slúži ako odkaz na predchádzajúci blok vo formáte 256-bitového hashu. Nasledujúce pole s názvom merkle root predstavuje všetky transakcie obsiahnuté v aktuálnom bloku a to vo forme 256-bitového hashu. Pole timestamp predstavuje časovú známku daného bloku. Pole s názvom bits sa dá definovať ako akuálny cieľový údaj, ktorý je zmenšovaný s obtiažnosťou riešenia tohto bloku. Nonce je pole s veľkosťou 4 bajty a jeho úlohou je meniť hodnotu tak aby bol daný hash pod cieľom políčka bits. Toto pole má na začiatku hodnotu 0 a je zväčšovaný každým hashom. Táto hodnota sa počíta až pokým nie je nájdený hash, ktorá obsahuje žiadaný počet núl nachádzajúcich sa na začiatku. V poli transaction count je počítadlo transakcií obsiahnutých v bloku. V transactions poli sú evidované jednotlivé transakcie.[36]

Čas vyťaženia bloku je 10 minút. Čas potvrdenia transakcie však je o niečo dlhší. V Bitcoin protokole je všeobecné nastavenie, že je treba 6 potvrdení od ťažiarov aby bola transakcia sprocesovaná. To znamená, že v priemere trvá potvrdenie transakcie asi 60 minút. Ale v skutočnosti to môže byť naozaj individuálne a závisí to od aktivity v sieti a výšky transakčných poplatkov.[21]

Hashrate

Hashovacia sila Bitcoinu je momentálne 31 EHash/s, čo je momentálne najvyššia hodnota spomedzi všetkých kryptomien.



OBRÁZOK Č. 3-VÝVOJ HASHOVACEJ SILY BITCOINU V PRIEBEHU ČASU.[38]

Bitcoinová sieť spotrebováva veľa energie, pretože musí vyriešiť ťažké matematické výpočty aby pravidelne nachádzal bloky. Tieto výpočty na nájdenie blokov sú v podstate matematické hádanky, ktoré ťažiar nemôže len hádať bez rozsiahleho vypočítavania. Na úspešné vyťaženie bloku potrebuje baník zakódovať hlavičku bloku hashom tak, aby bola menšia alebo rovná ako cieľ. A ťažiari prichádzajú k tomuto konkrétnemu cieľu tak, že obmieňajú malú časť hlavičky bloku, ktorá sa nazýva nonce. Hodnota nonce vždy začína 0 a je vždy zvyšovaný pre získanie požadovaného hashu (alebo cieľa). Keďže, hádanie hodnoty nonce sa rieši metódou pokus-omyl, šanca získať tento konkrétny hash (alebo cieľ), ktorý začína týmito mnohými nulami, je veľmi nízka. Preto ťažiari musia urobiť veľa pokusov aby uhádli nonce. Tak ako sa mení cieľ, tak sa mení aj náročnosť a to každých 2016 blokov. [21] [38]

3.2.5 Kapitalizácia trhu a cena Bitcoin

OBRÁZOK Č. 4 - VÝVOJ TRHOVEJ KAPITALIZÁCIE A VÝVOJ CENY BITCOINU VYJADRENÝCH V AMERICKÝCH DOLÁROCH.[39]

Obrázok č.4 znázorňuje vývoj trhovej kapitalizácie a ceny bitcoinu v čase, vyjadrených v amerických dolároch.

Bitcoin začal svoje účinkovanie v roku 2009. Vtedy však bola jeho cena nulová. V roku 2010 jeho cena stúpla keď dosiahol svoje maximum 0.39 $. Ďalší rok bol pre Bitcoin naozaj zlomový. Na začiatku roka 2011 dosiahol hodnotu 1 $ a to nebol zďaleka koniec. Druhého júna v roku 2011 dosiahol Bitcoin svoje vtedajšie maximum v hodnote 31.91 $. Avšak asi o týždeň v priebehu štyroch dní padla cena Bitcoinu na priepastných 10 dolárov. Naspäť na hranicu 31.91$ sa dostal Bitcoin až za rok aj pol vo feburári roku 2013. Postupne sa začal Bitcoin dostávať čoraz viac do povedomia okolia a rôzne obchody začali akceptovať Bitcoin ako formu platidla. To bol základ raketového zvýšenia hodnoty Bitcoinu v neskoršom období. Na prelome rokov 2013 a 2014 dosiahol Bitcoin hodnotu 1100 $ za jednotku. Toto však nebol zďaleka koniec. Rok 2017 bol pre Bitcoin zatiaľ najúspešnejším obdobím keď dosiahol svoje maximum a to v hodnote neuveriteľných 19498.63 $. Avšak táto bublina dlho nevydržala a momentálne má Bitcoin hodnotu 8524.87 $. [40] [41]

Jeho trhová kapitalizácia je 145 311 839 492 $ čím dosahuje prvenstvo medzi všetkými kryptomenami. Jeho trhová kapitalizácia je viac ako dvakrát vyššia ako druhá kryptomena v poradí – Ethereum. Počet bitcoinov v obehu je momentálne 17 045 637 BTC z celkového počtu 21 000 000. [39]

3.3 Ethereum

3.3.1 Technológia verejného záznamu – Ethereum blockchain

Ethereum má stavový blokchain, narozdiel od bitcoinového bezstavového blokchainu. Toto naznačuje, že v systéme Bitcoin sledovanie stavu toho, kto vlastní jednotky kryptomeny v systéme je síce odporúčané, ale nie je to bezpodmienečne nevyhnutné na generovanie blokov a ich validáciu. V systéme Ethereum je však nevyhnutné, aby bolo možné sledovať stav každého účtu, aby bolo možné získať nové bloky. V Ethereu sa tento pojem nazýva vo voľnom preklade svetový stav (z angl. World State). Svetový stav Etherea je strom Merkle Patricia dátových objektov nazvaných účty. Každá nová transakcia generovaná v Ethereu spúšťa funkciu prechodného stavu, ktorá je aplikovaná na aktuálny stav a deterministicky aktualizuje stav systému. Keď uzly v Ethereu dosiahnu všeobecnú dohodu v

blockchaine, aktualizovaný svetový stav je práve to, na čom sa dohodli. Momentálne dosahuje blockchain v systéme Ethereum 564.78 GB, čo je skoro trojnásobok veľkosti blockchainu v Bitcoine. Toto je spôsobené tým, že v Ethereu uchováva blockchain okrem transakcií aj iné údaje. [21] [33]

3.3.2 Operácie

Ethereum rozlišuje dva typy komunikácie:

- Transakcie
- Správy

Tieto dve triedy existujú z dôvodu povahy rôznych typov účtov dostupných v systéme. [23]

Transakcie

Generovanie transakcií je to, ako vonkajšie subjekty - uzly v sieti komunikujú s blockchainom. Transakcie sú zostavené vonkajšími subjektami a následne propagované do ostatných uzlov v sieti spôsobom peer to peer. Transakcie môžu byť predmetom škodlivého správania zo strany iných uzlov. Z tohto dôvodu transakcie musia podpísať vonkajšie subjekty, ktoré chcú vykonať transakciu s príslušným súkromným kľúčom na účet, z ktorého transakcia pochádza. To je podstate ten istý postup, ako poznáme pri Bitcoine, s výnimkou, že podpis nie je určený na minutie nespotrebovaného výstupu transakcie, ale skôr na autorizáciu stavového prechodu na externom účte. Všimnite si, že pri Bitcoine musí byť celá hodnota v adrese Bitcoin použitá v transakcii, to však nie je pri Ethereu nevyhnutné. Je úplne v poriadku využiť len zlomok hodnoty na účte v systéme Etherea.[21][23]

Nasledujúca tabuľka č.5 znázorňuje a opisuje polia obsiahnuté v transakcii Etherea.

nonce	Hodnota, ktorá sa rovná celkovému počtu transakcií poslaných z účtu odosielateľa.
gasPrice	Cena za jeden výpočtový krok.

gasLimit	Maximálna akumulovaná cena za všetky výpočty týkajúce sa tejto transakcie.
to	Adresa účtu príjemcu.
value	Množstvo Etherov posielaných na adresu príjemcu
v, r, s	Hodnoty r a s reprezentujú digitálny podpis pre túto konkrétnu transakciu podpísanú odosielateľovým účtom. Hodnota v je obnovovacie ID podpisu.
data/init	Toto pole je využívané pre transakcie vykonávajúce kód.

TABUĽKA Č. 5- ŠTRUKTÚRA TRANSAKCIE ETHEREA S VYSVETLENÍM JEDNOTLIVÝCH POLÍ.[21]

Správy

Správy sú odlišné od transakcií. Ide o komunikáciu, ktorá vznikla vykonaním zmluvného kódu, napr. pochádzajú zo zmluvného účtu. Správa sa vždy vytvára ako efekt transakcie, volajúcej zmluvu. Správy nie sú podpísané, pretože zmluvy nemajú žiadne kľúče na podpísanie. Čo je ešte dôležitejšie, správy nemusia byť podpísané, pretože sa nikdy neprenášajú v sieti a existujú iba ako súčasť exekučného prostredia Etherea, a to ako následok spustenia programového kódu. Všetky transakcie musia pochádzať z externe vlastneného účtu. Správy sa odovzdávajú zo zmluvných účtov a medzi zmluvnými účtami iba ako výsledok počiatočného transakčného spúšťania kódu na zmluvnom účte. [21] [23]

Nasledujúca tabuľka č.6 znázorňuje štruktúru takejto správy.

sender	Zmluvná adresa, ktorá vytvorila správu - odosielateľ.

transaction originator	Adresa externe vlastneného účtu, ktorý zavolal vykonanie zmluvného kódu odosielateľa – pôvodca transakcie
recipient	adresa príjemcu správy.
code account to be executed	Účet, ktorého kód by mal byť vykonaný, zvyčajne rovnaký ako kód príjemcu.
startGas	Dostupné palivo pre túto správu.
value	hodnota transferovaná v tejto správe.
gasPrice	cena za výpočtový krok
data	Voliteľné vstupné údaje týkajúce sa volania správ.
depth of execution stack	Súčasná hĺbka vykonávajúceho zásobníka.

TABUĽKA Č. 6 - ŠTRUKTÚRA SPRÁVY ETHEREA SPOLU S VYSVETLENÍM JEDNOTLIVÝCH POLÍ.[21]

3.3.3 Konsenzus v Ethereu

Ethereum vo svojom protokole tiež využíva mechanizmus proof of work. Narozdiel od Bitcoinu, však systém Ethereum používa odlišný prístup na dosiahnutie konsenzu ako Bitcoin: The Greedy Heaviest Observed Sub Tree (GHOST). Protokol prvýkrát opísali páni Sompolinsky a Zohar a z praktických dôvodov bol mierne upravený v implementácii Etherea. [21]

Protokol GHOST je variantom konsenzu Nakamoto, kde všeobecná stratégia selekcie blokov už nie je typu - najdlhšia reťaz vyhráva, ale skôr najsilnejší podstrom vyhráva.

Najmohutnejším stromom je strom, ktorý má najviac vykonanej výpočtovej práce dokopy – a teda nielen na hlavnej vetve, ale započítava platnú výpočtovú prácu vykonanú aj na úzko spojených vetvách. [21] [23]

3.3.4 Validácia operácií

Ťažba, odmena

Pred začatím ťaženia Etherea si potrebuje ťažiar zaobstarať špeciálny počítačový hardvér, ktorý bude určený čisto na ťažbu. Existujú dva typy takéhoto hardvéru:

- hardvér využívajúci grafickú kartu GPU
- hardvér využívajúci centrálny procesor CPU

GPU však dosahujú vyšší výkon v podaní hashovacej sily a momentálne sú jedinou možnosťou pri efektívnej ťažbe etherea. Narozdiel od bitcoinu však zatiaľ neexistujú špeciálne ťažiarske zariadenia ASIC pre ethereum. Odmena za vyťaženiu bloku Ethera je momentálne 3 ethery plus transakčné poplatky.[33] [42]

Palivo (z angl. gas) je pre Ethereum to isté ako je benzín pre motor. Často sa v bežnej analógii nazýva kryptopalivom. Všeobecná myšlienka kryptopaliva spočíva v tom, že každý výpočtový krok, ktorý musí baník vykonať, aby spustil kód v transakcii, má cenu - gasPrice, ktorú pôvodca transakcie musí zaplatiť ťažiarovi.[21]

Spotrebované palivo - ether sa stáva transakčným poplatkom pre ťažiarov. Pretože ťažiarsky poplatok priamo súvisí s komplexnosťou výpočtu, ťažiari nie sú odrádzaní od ťažby veľkých programov. Aj keď ich overovanie trvá dlhšie, odmena bude zato vyššia.[23]

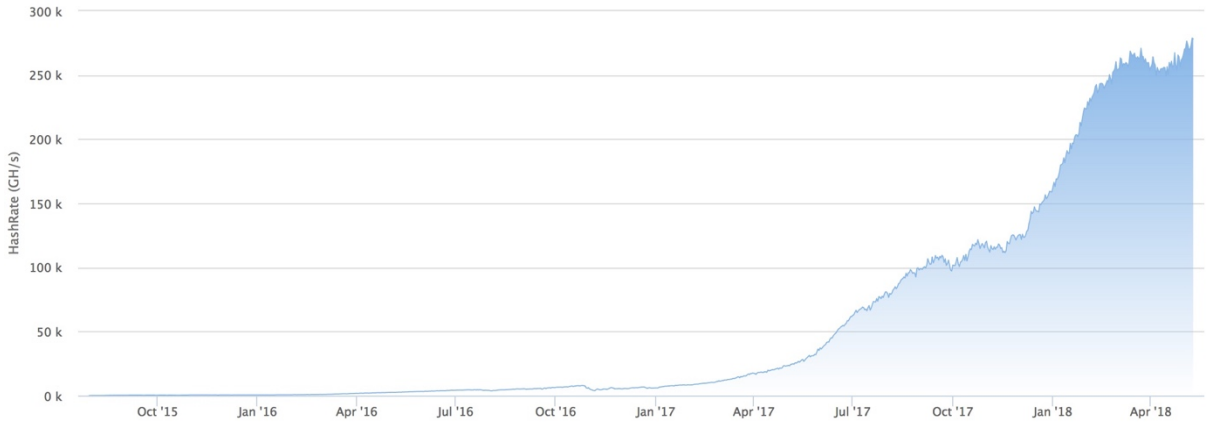
Veľkosť bloku

Veľkosť bloku Etherea nie je pevne stanovená – je flexibilná. Táto flexibilita zaručuje oveľa vyššiu rýchlosť transakcií ako to je pri Bitcoine. Čas validácie bloku je v priemere 13 sekúnd, ale znova platí, že potvrdenie transakcie je o niečo dlhšie. Momentálne sa tento čas pohybuje v priemere 10 minút. Ale môže to byť individuálne v závislosti od aktivity siete a tiež transakčných poplatkov.[33]

Hashrate

Súčasný hashrate dosahuje hodnotu 274.5286 TH/s. V porovnaní s Bitcoinom je to oveľa menšia hodnota, keď hashrate BTC dosahuje 31 EH/s. To je v prepočte 31 000 000 TH/s čo robí medzi týmito menami naozaj priepastný rozdiel. To je spôsobené aj tým, že v Ethereu zatiaľ neexistujú ASIC zariadenia na ťažbu etherov. [43]

Na obrázku č.5 môžeme vidieť vývoj hashovacej sily Etherea v priebehu času, vyjadrených v GH/s.



OBRÁZOK Č. 5 - VÝVOJ HASHOVACEJ SILY ETHEREA V PRIEBEHU ČASU V GH/S.[43]

3.3.5 Iné odlišnosti a inovácie

Ethereum Virtual Machine (EVM)

EVM je exekučné prostredie Etherea. Všetky obsadené uzly v Ethereu spustia rovnakú inštanciu EVM a transakcie, ktoré sú vstupom do virtuálneho stroja, zmenia stav systému deterministicky, tak že všetci majú rovnaký aktualizovaný stav systému. Každý obsadený uzol musí vykonať programový kód vyvolaný z každej transakcie. To znamená vysokú úroveň redundantných výpočtov, ale toto je zároveň to, čo zaručuje dôveru v tento systém. [23]

3.2.6 Kapitalizácia trhu a cena Etherea

Ethereu momentálne patrí druhá priečka v trhovej kapitalizácii kryptomien dosahujúc hodnotu 70 036 867 910 $. Ak by sme sa však bavili o rebríčku cien kryptomien tak by jej patrila tretia priečka dosahujúc hodnotu 704.42 $. Momentálne cirkuluje v obehu 99 569 567 ETH. [39]

OBRÁZOK Č. 6 - VÝVOJ TRHOVEJ KAPITALIZÁCIE ETHEREA A VÝVOJ JEHO CENY V AMERICKÝCH DOLÁROCH[39]

Obrázok č.6 znázorňuje vývoj trhovej kapitalizáce a ceny Etherea, vyjadrených v amerických dolároch.

3.3.7 Súhrn rozdielov Etherea voči BTC

- Blockchain Etherea je stavový, narozdiel od bezstavového blockchainu Bitcoinu
- blockchain uchováva okrem transakcií aj správy, čo má za dôsledok oveľa väčší blockchain ako v Bitcoine
- tento systém dokáže vykonávať okrem transakcií aj inteligentné kontrakty
- tento systém má svoj vlastný virtuálny stroj, kde pomocou vlastného programovacieho jazyka je možné programovať a vykonávať inteligentné kontrakty
- oveľa nižší hashrate, na ťažbu nie je potrebný tak drahý hardvér
- rozdiel v protokole konsenzusu, Ethereum používa GHOST, zatiaľ čo Bitcoin používa Nakamoto consensus

3.4 Dash

3.4.1 Technológia verejného záznamu – Dash blockchain

Pri Bitcoine sú transakcie zverejnené v blockchaine a môžete dokázať, kto ich uskutočnil alebo komu. Ale pomocou technológie anonymizácie siete Dash je prakticky nemožné ich vysledovať. Toto je dôležité, pretože bitcoinový blockchain je prístupný každému, kto má internetové pripojenie – čo je významnou prekážkou pre tých, ktorí nechcú, aby ich história transakcií a zostatky boli verejne dostupné. Dash to robí prostredníctvom zmiešavacieho protokolu využívajúceho inovatívnu decentralizovanú sieť serverov s názvom Masternodes, čím sa vyhýba potrebe dôveryhodnej tretej strany, ktorá

by mohla ohroziť integritu systému. Súčasná veľkosť blockchainu kryptomeny Dash je 6.15 GB, čo je oproti blockchainu Bitcoinu dosahujúceho veľkosť 197.76 GB naozaj obrovský rozdiel. Ten je spôsobený menšou popularitou kryptomeny Dash a tiež jej mladším vekom. [27][33]

3.4.2 Operácie

Transakcie

Dash transakcie sú takmer okamžite potvrdené sieťou Masternodes. Toto je veľké zlepšenie oproti systému Bitcoin, kde potvrdenia trvajú oveľa dlhšie, pretože všetku prácu vykonávajú ťažiari. Okrem toho Dash ponúka tiež súkromné transakcie, ktoré používajú zmiešavací protokol na anonymizáciu zdroja transakcie.[27]

3.4.3 Konsenzus v Dash

Dash pracuje tiež na mechanizme konsenzu typu proof of work. Ale z určitého hľadiska sa dá naň čiastočne pozerať ako mechanizmus proof of stakes. Dash umožňuje svojim držiteľom získavať dividendy vo forme DASH spustením masternode. Ale háčik je v tom, že potrebujete minimálne 1000 jednotiek DASH na prevádzkovanie masternode, pričom v čase písania tejto práce má jednotka DASH hodnotu približne 384 dolárov. Takže ak chce človek investovať 384 000 dolárov (tj 1000 jednotiek * 384 dolárov), aby ste dostali ročný výnos 7,5% plus odmenu v podobe zhodnotenia ceny DASHu v priebehu času, potom to bude dobrá cesta, pretože DASH je sľubnou kryptomenou pre držbu. A čo je lepšie ako zarábať aj na svojich držbách. Síce viem, že DASH v skutočnosti nefunguje na mechanizme konsenzuse Proof of stakes, ale jeho masternódy pracujú istým spôsobom ako pri konsenze proof of stakes, pretože držianie jednotiek DASH je v tomto prípade veľmi výnosné. [27][44]

3.4.4 Validácia operácií

Ťažba

Na rozdiel od väčšiny ostatných kryptomien blokové odmeny sú rovnako rozdelené medzi ťažiarov a masternódy t.j. 45% ťažiarom a 45% masternódam, pričom 10% príjmov ide do pokladnice na financovanie rozvoja, komunitných projektov a marketingu.[30]

Kvôli zložitosti a veľkosti potrebnej na vytvorenie ASIC pre ťažbu x11 sa očakávalo, že to bude trvať oveľa dlhšie ako to bolo pri Bitcoine, čo by umožnilo

priaznivcom zúčastňovať sa ťažby dlhšiu dobu. To je veľmi dôležité pre dobrú distribúciu a rast kryptomeny. Ďalšou výhodou reťazového hashovacieho prístupu sú profesionálne procesory, ktoré poskytujú priemernú návratnosť podobnú ako pri ťažbe grafickou kartou. Grafické karty tiež bežia o 30-50% chladnejšie, s menším výkonom ako napr. pri scrypt algoritme používanom veľkou časťou súčasných kryptomien. Avšak postupne sa Dash rozrástol do takej miery, že ťažba pomocou jednotiek procesora a grafického čipu už nie je efektívna. ASIC zariadenia sú jedinou možnosťou ako dosahovať profit ťažením jednotiek Dash a získavať blokové odmeny. [45]

Bloková odmena je 3.35 DASH plus transakčné poplatky. Táto odmena sa následne delí na už spomínané 3 časti, keď 10% ide do spoločného fondu a zvyšok sa rozdelí na polovicu medzi masternódy a ťažiarov. V praxi to znamená že 0.335 DASH (10% z odmeny) ide do fondu, masternódam ide 1,5075 DASH (45% odmeny) a ťažiarom, ktorí vyťažili blok tak isto 1,5075 DASH (45% odmeny). [33]

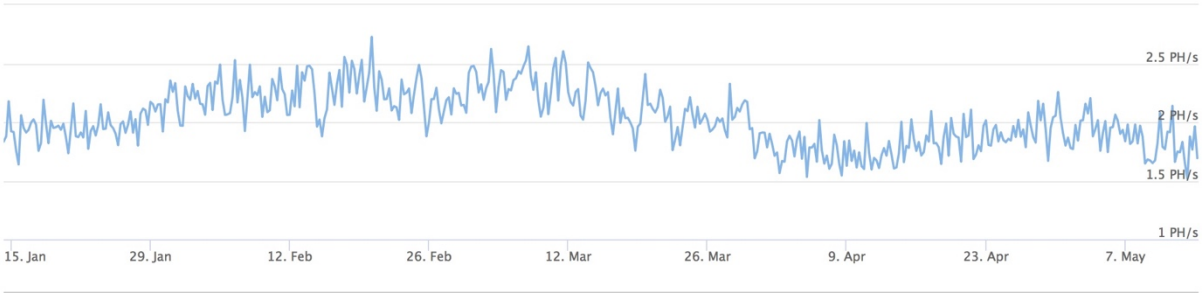
Veľkosť bloku

Veľkosť bloku môže byť maximálne 2 MB, čo robí výrazný rozdiel v porovnaní s Bitcoinom. Čas validácie bloku je vylepšený existenciou siete masternódov a práve zvýšenou veľkosťou bloku. Blok v systéme Dash je zvalidovaný priemerne za 2.5 minúty. [33] [27]

Hashrate

Hashovacia sila v systéme Dash dosahuje 1.819 PH/s. Táto pomerne vysoká hodnota je spôsobená tým, že ako pri Bitcoine tak aj tu bolo už vymyslené špeciálne zariadenie na ťažbu ASIC.

Obrázok č.7 znázorňuje hashrate systému DASH v priebehu času, vyjadrenú v PH/s.



OBRÁZOK Č. 7 - HASHRATE SYSTÉMU DASH V PH/S. [47]

V porovnaní s Bitcoinom, dosahuje hashovacia sila oveľa menšie hodnoty. Bitcoin v súčasnosti dosahuje hashrate 31 EHash/s čo je v prepočte 31 000 PHash/s. Z tohto vyplýva že hashovací algoritmus x11 síce dosahuje určité zlepšenie v oblasti náročnosti ťažby, ale efektívna ťažba je možná len zo zariadením ASIC vyrobeným špeciálne na ťaženie jednotiek Dash. Bitcoin používa tiež zariadenia ASIC ale potrebujú oveľa väčší výkon, čím sa náklady na energie stávajú drahšími ako je to v Dashi. [47]

DASH tiež používa open-source algoritmus, ktorý upravuje ťažobnú náročnosť a má názov Dark Gravity Wave. Výsledkom je, že úroveň náročnosti je upravená každým blokom namiesto každých 2016 blokov, ako to je pri Bitcoine. [27]

3.4.5 Iné odlišnosti a inovácie

InstantX

Použitím kvóra Masternode môžu používatelia posielať a prijímať okamžité nevratné transakcie. Po vytvorení kvóra sú vstupy transakcie uzamknuté tak, aby boli minuteľné len v určitej špeicifickej transakcii, pričom uzamknutie transakcie trvá približne 4 sekundy, aby sa to stihlo odzrkadliť v sieti. Ak sa dosiahne konsenzus o uzamknutí sieťou Masternode, všetky konfliktné transakcie alebo konfliktné bloky budú odmietnuté potom, pokiaľ nebudú zodpovedať presnému ID transakcie zámku na mieste. To umožní dodávateľom používať mobilné zariadenia namiesto tradičných platobných systémov pre obchodovanie v reálnom svete a používateľom rýchlo uspokojiť nekomerčné transakcie ako s bežnou hotovosťou. Toto sa vykonáva bez akéhokoľvek ústredného orgánu. [48]

PrivateSend

PrivateSend vám poskytuje skutočné finančné súkromie tým, že utají pôvod vašich finančných prostriedkov. Všetky jednotky Dash vo vašej peňaženke pozostávajú z rôznych vstupov, ktoré môžete považovať za samostatné, diskrétne mince. PrivateSend používa inovatívny proces na zmiešanie vašich vstupov so vstupmi dvoch ďalších ľudí bez toho, aby vaše mince vôbec opustili vašu peňaženku. Čiže používateľ má vždy kontrolu nad svojimi peniazmi. [49]

Decentralizované riadenie

Systém Dash implementoval aj decentralizovaný systém riadenia prostredníctvom využívania siete masternode. Tento systém umožňuje uzlom masternode hlasovať o

dôležitých problémoch a návrhoch rozpočtu, ktoré, ak sú schválené, sú financované priamo z blockchainu. To sa deje prostredníctvom rozdelenia blokových odmien medzi minerov (45%), masternódy (45%) a návrhy rozpočtu (10%). Tento systém je prvý svojho druhu a označuje sa ako decentralizované riadenie blockchainom. [48] [27]

3.4.6 Kapitalizacia trhu a cena DASH

Na obrázku č.8 môžeme vidieť vývoj trhovej kapitalizácie a ceny DASH v amerických dolároch.

OBRÁZOK Č. 8 - VÝVOJ KAPITALIZÁCIE TRHU A CENY JEDNOTKY DASH V AMERICKÝCH DOLÁROCH [39]

Kryptomene Dash momentálne patrí desiata priečka v trhovej kapitalizácii kryptomien dosahujúc hodnotu 3 258 922 946 $. Ak by sme sa však bavili o rebríčku cien kryptomien tak by jej patrila štvrtá priečka dosahujúc hodnotu 403.20 $. Momentálne cirkuluje v obehu 8 082 586 DASH z celkového množstva 19 000 000.[39]

3.4.7 Súhrn rozdielov Dash voči BTC

- vďaka funkcii anononymizácie je jeho blockchain a teda aj transakcie súkromné, čo sa pri Bitcoine povedať nedá
- funkcia InstantSend zabezpečuje takmer okamžité transakcie, zatiaľ čo pri BTC transakcia môže trvať hodiny
- rozšírené možnosti zárobku-okrem ťaženia kryptomincí je tu možnosť stať sa masternódou čo by mohla byť zaujímavá investícia
- odmena za vyťaženie bloku sa delí v pomere 0.45 : 0.45 : 0.1 = masternódy : ťažiari : fond. Pri Bitcoine ide celá odmena ťažiarom

- náročnosť sa mení po každom bloku, narozdiel od BTC , kde sa mení každých 2016 blokov
- Dash poskytuje vlastné decentralizované riadenie vďaka sieti masternód, zatiaľ čo Bitcoin nemá implementované riadenie

3.5 Ripple

3.5.1 Technológia verejného záznamu - Ripple Ledger

Ripple udržiava distribuovaný záznam s názvom Ripple ledger, ktorý sleduje všetky vykonané transakcie v systéme. Záznamy databázy sa vytvárajú každých pár sekúnd, a obsahujú zoznam transakcií, s ktorým väčšina validujúcich serverov súhlasí. To sa dosiahne pomocou protokolu Ripple, ktorý sa spúšťa medzi validujúcimi servermi. Ripple záznam pozostáva z nasledujúcich informácii:

- súbor transakcií
- informácie týkajúce sa účtu, ako napr. nastavenie účtu, celkový zostatok, vzťah dôvery
- časové pečiatky
- číslo databázy
- stavový bit indikujúci, či je kniha validovaná alebo nie

Najnovší platný záznam je označovaný ako posledný uzavretý záznam databázy. Na druhú stranu ak záznam databázy ešte nie je overený, tak sa blok databázy považuje za otvorený. Ripple ledger síce nie je blockchain, ale jeho záznamy sa uchovávajú na veľmi podobnom princípe.[29]

XRP Ledger je zdieľaný globálny záznam, ktorý je verejný pre všetkých. Jednotliví účastníci môžu dôverovať integrite záznamu bez toho, aby museli dôverovať akejkoľvek inštitúcii, na jej dosiahnutie. Softvér pre server s názvom rippled to dokáže tým, že spravuje databázu záznamov, ktorú je možné aktualizovať iba podľa veľmi špecifických pravidiel. Každá inštancia rippled uchováva úplnú kópiu celkového záznamu a sieť peer to peer serverov s rippled distribuuje transakcie kandidátov medzi sebou. Konsenzusový proces určuje, ktoré transakcie sa použijú pre každú novú verziu záznamu. [52]

Zdieľaný globálny záznam je vlastne séria samostatných záznamov alebo verzií záznamov, ktoré rippled uchováva vo svojej internej databáze. Každá verzia záznamu obsahuje index záznamu, ktorý identifikuje poradie, v ktorom sa vyskytujú záznamy. Každá verzia uzavretého záznamu má aj identifikačnú hodnotu hash, ktorá jednoznačne identifikuje obsah tohto záznamu. V akomkoľvek čase má rippled inštancia aktuálny otvorený záznam a niekoľko uzavretých záznamov, ktoré ešte neboli schválené konsenzom, a akýkoľvek počet historických záznamov, ktoré boli potvrdené konsenzom. Len potvrdené záznamy sú určite správne a nemenné. [52]

3.5.2 Operácie

Kryptomena Ripple vie pracovať iba s transakciami, ale v súčasnosti podporuje až šesť druhov transakcií, ktoré sú zaznamenané v nasledujúcej tabuľke č. 7.

Payment	Ide o najbežnejší typ transakcií a umožňuje účtovnej jednotke odosielať finančné prostriedky z jedného účtu na druhý.
AccountSet	Táto transakcia umožňuje účtovnej jednotke nastaviť možnosti relevantné pre svoj účet. Transakcia AccountSet umožňuje zrušenie transakcie s rovnakým sekvenčným číslom za predpokladu, že transakcia ešte nebola zapracovaná do validovanej databázy.
SetRegularKey	Táto transakcia umožňuje účtovnej jednotke zmeniť alebo nastaviť kľúč používaný subjektom na podpísanie budúcich transakcií.
OfferCreate	Táto transakcia vyjadruje zámer vymeniť meny.
OfferCancel	Táto transakcia odstráni ponuku z databázy.

TrustSet	Táto transakcia vytvára (alebo upravuje) dôveryhodné spojenie medzi dvomi účtami.

TABUĽKA Č. 7 - TYPY TRANSAKCIÍ V RIPPLE.[28]

3.5.3 Konsenzus v Ripple

Kryptomena Ripple používa tiež konsenzusový mechanizmus typu proof of work. Avšak v tomto prípade funguje na mierne odlišnom princípe. Konsenzus v Ripple sa dosahuje hlasovaním serverov o validite záznamov. Tento proces vysvetlím bližšie pri vysvetlení validovania transakcií. [50]

Dôkaz práce môže byť vyžadovaný serverom, keď prijíma prichádzajúce spojenie. Keď server dostane nadmernú podozrivú záťaž, začne uzatvárať všetky odchádzajúce pripojenia, ktoré ho zaťažujú. Bude vyžadovať dôkaz o práci (Proof of Work) cez nové pripojenia a môže vyžadovať periodické dôkazy o práci z existujúcich pripojení na server. Servery prispôsobia náročnosť dokladu o práci, na takú akú vyžadujú. Útočník bude musieť skompletizovať dôkaz práce po každej malej sérii útokov. Oprávnení používatelia budú musieť dokončiť len jeden doklad o práci na server, ku ktorému sa chcú pripojiť. Server i klient budú musieť poskytnúť dôkaz o práci, keď spravia odchádzajúce pripojenia.[28]

3.5.4 Validácia operácií

Ťažba

Najväčším rozdielom od ostatných kryptomien je, že token XRP sa neťaží. XRP tokeny sú emitované spoločnoťou Ripple Labs. Je ich pevný počet 100 000 000 XRP. Z toho asi 60% má vo vlastníctve práve Ripple Labs a 40% je vypustených do obehu. [29]

Validácia záznamov

Každý verifikačný server overuje navrhované zmeny k poslednej databáze. Zmeny, s ktorými súhlasí aspoň 50% serverov sú združené do nového návrhu, ktorý je odoslaný na ostatné servery v systéme. Tento proces sa opakuje s rastúcimi požiadavkami na

hlasovanie aspoň 60%, 70% a 80%, po ktorých server zvaliduje zmeny a upozorní sieť na uzavretie poslednej časti databázy. V tomto bode je každá transakcia, ktorá bola vykonaná, ale nezobrazuje sa v Ripple ledger databáze bude vyradená a môže byť považovaná používateľmi Ripple za neplatnú. Každý validujúci server udržiava zoznam dôveryhodných serverov známy ako Unique Node List (Zoznam jedinečných uzlov, UNL). Servery berú do úvahy iba hlasy vydané takými servermi, ktoré sú obsiahnuté v ich UNL. V súčasnosti beh Ripple overovacích serverov sprostredkúva spoločnosť Ripple Labs. Ale treba však poznamenať, že každá entita môže spustiť svoj vlastný server. Týmto spôsobom, Ripple umožňuje iným inštitúciám (napr. bankám, ktoré prevádzkujú svoje vlastné servery) dosiahnuť konsenzus v súvislosti s osudom finančných transakcií. Napríklad, v septembri 2014 spoločnosť Ripple Labs uzatvorila dohodu o partnerstve s dvoma USA bankami, ktoré súhlasili s prijatím distribuovanej transakčnej open-source infraštruktúry spoločnosti Ripple. [28]

Čas validácie záznamu

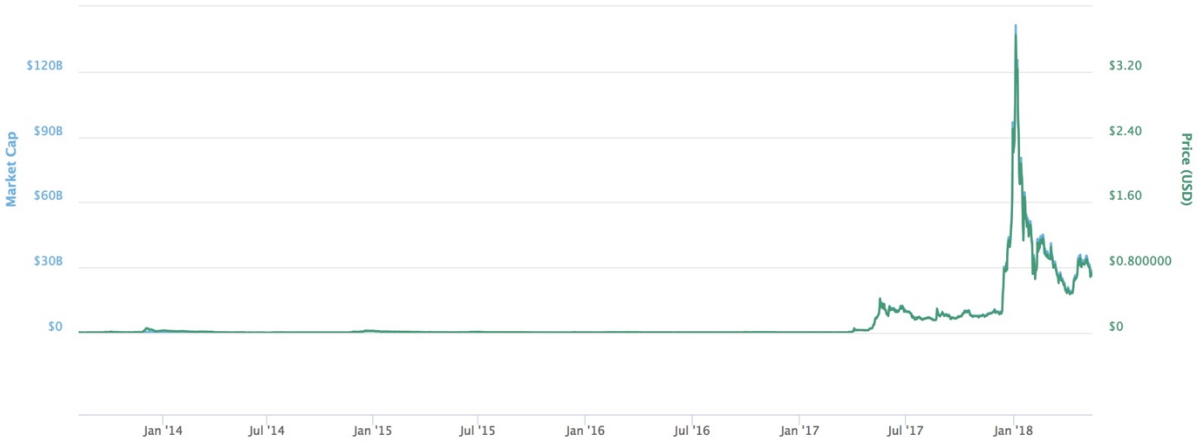
Transakcie sú naozaj veľmi rýchle, pričom validácia záznamu trvá v priemere asi 4 sekundy. To je jednou s najväčších výhod transakcií v Ripple. [29]

3.5.5 Iné odlišnosti a inovácie

Samotná kryptomena Ripple je určitým druhom inovácie a odlišnosti vo svete kryptomien. Zatiaľ čo väčšina vzniknutých kryptomien sa rozhodla ísť vyšliapanou cestičkou Bitcoinu, XRP išla svojou vlastnou cestou a tak ako od BTC tak aj od ostatných mien sa odlišuje najviac. Ripple dokázal, že sa to dá robiť aj inak. Tým nechcem povedať, že jedna mena je lepšia ako druhá alebo opačne. Len tým chcem poukázať na diverzitu, napriek ktorej sa obom menám sa darí relatívne dobre.

3.5.6 Kapitalizácia trhu a cena Ripple

Na obrázku č.9 môžeme vidieť vývoj trhovej kapitalizácie a cien Ripple vpriebehu času, vyjadrené v amerických dolároch.



OBRÁZOK Č. 9 - VÝVOJ TRHOVEJ KAPITALIZÁCIE A VÝVOJ CIEN RIPPLE V PRIEBEHU ČASU VYJADRENÝCH V AMERICKÝCH DOLÁROCH [39]

Ripple prišiel na trh v roku 2012. Najväčšiu hodnotu táto kryptomena získala 4.januára 2018 kedy dosiahla cenu 3.84 $. Avšak už ku koncu januára mala hodnotu iba 1.16 $. To je dosť výrazný pád a čiastočne sa dá tento mesiac nazvať nestabilným z hľadiska kapitalizácie trhu. Momentálna hodnota XRP je 0.743117 $. Kapitalizáciou trhu je patrí tretia priečka hneď za Bitcoinom a Ethereom dosahujúc hodnotu 26 905 951 074 $. So sľubnou finančnou technológiou pre budúcu a rozrastajúcu sa sieť bánk, vyzerá kryptomena Ripple ako sľubná dlhodobá investícia. S viac investormi, ktorí si uvedomujú XRP a rastúce povedomie o tejto technológii, sa očakáva, že hodnota XRP bude narastať aj v roku 2018. [29]

3.5.7 Súhrn rozdielov Ripple voči BTC

- Najväčším rozdielom oproti mene Bitcoin je to, že Ripple nefunguje priamo na blockchainovej technológii, aj keď princípy sú podobné. Používa svoju vlastnú technológiu s názvom Ripple ledger.
- Transakcie sú validované servermi, ktoré mali vo vlastníctve najprv výlučne Ripple Labs, v súčasnosti však existujú aj validujúce servery, ktoré sú vydané inými inštitúciami. Na rozdiel od ostatných spomínaných kryptomien, Ripple je jedinou menou, ktorá nefunguje na princípe ťažby. Existuje 100 000 000 XRP tokenov z čoho 60% má vo svojich rukách Ripple Labs.

- Rozdiel je tiež v dosahovaní konsenzu. Obe kryptomeny síce používajú rovnaké mechanizmy, avšak v Ripple je implementované hlasovanie serverov, zatiaľ čo v BTC platí pravidlo : Najdlhšia reťaz vyhráva.
- Validácia záznamov je oveľa rýchlejšia ako pri BTC. Pri Ripple je to v priemere pár sekúnd, zatiaľ čo pri BTC je to až 10 minút.
- Decentralizácia Ripple nie je na takej úrovni ako je to pri BTC. To je spôsobené hlavne väčšinovým vlastníctvom validačných serverov spoločnosťou Ripple Labs.
- Pri BTC sú sledované iba transakcie. Pri XRP však môžu byť sledované aj iné typy dát, týkajúcich sa používateľov.

3.6 Vytvorenie jednoduchého záznamu reťazcov na blockchainovom princípe

Počas komparácie daných kryptomien sme síce zistili veľa odlišností, ale vo veľa vlastnostiach a technológiách sú podobné. Jednou z technológií, ktoré sa vo väčšine kryptomien vyskytuje je technológia blockchain. A práve blockchain som sa rozhodol naprogramovať a interpretovať niektoré jeho vlastnosti.

Na vytvorenie záznamu reťazcov fungujúceho na blockchainovom princípe som si zvolil programovací jazyk Java. Na tvorbu tohto jednoduchého programu som si zvolil prostredie InteliJ IDEA. Výsledný program je typu konzolovej aplikácie.

Zdrojový kód je rozdelený do dvoch tried :

- Block.java
- Main.java

Block.java obsahuje triedu blok, ktorá bude interpretovať súbor reťazcov. Reťazec v rámci kryptomien býva zväčša transakcia. Formát však v mojom príklade nie je dôležitý, princíp blockchainu a šifrovania dát interpretujem preto na reťazcoch.

Main.java obsahuje hlavnú funkciu Main, pomocou ktorej sa spúšťa konzolová aplikácia. Je v nej obsiahnuté vytvorenie blokov aj následný výpis zašifrovaných textov - hashov.

Tu je zdrojový kód triedy block.java:

Block.Java

```
import java.util.Arrays;
public class Block
    {
    private int previousHash;
    private String[] transactions;
    private int blockHash;

    public Block(int previousHash,String[] transactions)
        {
        this.previousHash = previousHash;
        this.transactions = transactions;

        Object[] contens = {Arrays.hashCode(transactions), previousHash};
        this.blockHash = Arrays.hashCode(contens);
        }

    public int getPreviousHash()
        {
        return previousHash;
        }

    public String[] getTransactions()
        {
        return transactions;
        }

    public int getBlockHash()
        {
        return blockHash;
        }
    }
```

Trieda blok obsahuje tri súkromné premenné s názvami previousHash, transactions a blockHash.

previousHash - je celočíselná premenná, ktorá obsahuje hash predchádzajúceho bloku.

transactions – je pole reťazcov napr. transakcií, ktoré budeme uchovávať v blokoch

blockhash – je celočíselná premenná, ktorá vytvorí zo súboru reťazcov hash

Ďalej v kóde nasleduje verejný parametrický konštruktor blokov s parametrami: previousHash a transactions. Z toho vyplýva, že nový blok bude konštruovaný vždy z hashu predchádzajúcich reťazcov a reťazcov obsiahnutých v novom bloku.
V nasledujúcich riadkoch sa potom kalkuluje hash kód transakcií a následne priradí k premennej blockHash.

V nasledujúcej časti kódu sa nachádzajú tzv. getter funkcie, pomocou ktorých dostaneme hodnotu chcenej premennej obsiahnutej v našej triede. Napr.getPreviousHash nám vráti hodnotu hashu predchádzajúceho bloku reťazcov.

Tu môžete vidieť zdrojový kód triedy main.java:

Main.java

```
import java.util.ArrayList;
import java.util.Arrays;

public class Main {

    ArrayList<Block> blockchain = new ArrayList<>();

    public static void main(String[] args) {
        String[] genesisTransactions={"Sender:Tomas, Recipient: Fero, Amount:15
BTC"};
        Block genesisBlock=new Block(0,genesisTransactions);

        String[] block2Transactions={"Sender: Fero, Recipient: Tomas, Amount:45
BTC","Sender: Igor, Recipient: Michal, Amount:23 BTC"};
        Block block2=new Block(genesisBlock.getBlockHash(),block2Transactions);

        String[] block3Transactions={"Sender: Majo, Recipient: Miko, Amount:13
BTC","Sender: Tomas, Recipient: Igor, Amount:1000 BTC"};
        Block block3=new Block(block2.getBlockHash(),block3Transactions);

        System.out.println("Hash of Genesis block:");
        System.out.println(genesisBlock.getBlockHash());
        System.out.println("Hash of second block:");
        System.out.println(block2.getBlockHash());
        System.out.println("Hash of third block:");
        System.out.println(block3.getBlockHash());
    }
}
```

Ako prvé vytvoríme pole reťazcov genesisTransactions, ktoré budú uchovávať reťazce v prvom bloku. Ďalej vytvoríme prvý blok s názvom genesisBlock. Keďže je to prvý blok vôbec, nemá žiaden predchádzajúci blok. Preto za hash predchádzajúceho bloku dosadím číslo 0. Po vytvorení bloku genesis sa genesisTransactions nachádzajú v tomto bloku a majú vytvorený unikátny hash, ktorý zaručí že aj najmenšia zmena vo vstupe reťazca zmení hash kód na nepoznanie.

Následne vytváram ďalší súbor reťazcov s názvom block2Transactions. Tie budem vkladať do druhého bloku, ktorý vytváram hneď v ďalšom riadku. Blok je vytvorený pomocou hashu predchádzajúceho bloku a reťazcov vkladaných do neho.

V ďalších riadkoch robím presne to isté, vytváram nový blok pomocou hashu predchádzajúceho a transakcií, ktoré majú byť v aktuálnom bloku obsiahnuté.

```
/Library/Java/JavaVirtualMachines/jdk1.8.0_161.jdk/Contents/Home/bin/java ...
Hash of Genesis block:
1658233479
Hash of second block:
-1194067566
Hash of third block:
-221309343

Process finished with exit code 0
```

OBRÁZOK Č. 10 - PÔVODNÝ VÝSTUP Z KONZOLOVEJ APLIKÁCIE PO SPUSTENÍ MAIN.JAVA

Na obrázku č.10 sa nachádza výstup z naprogramovanej konzolovej aplikácie. Vidíme 3 bloky jedinečne zahashované v podobe digitálneho podpisu.

Teraz zmením vstup prvého bloku, aby som interpretoval nemožnosť meniť obsah reťazcov bez povšimnutia. napr. pridám transakciu : „Sender: Jano, Recipient: Strapo, Amount:13 BTC“. Obrázok č.11 ukazuje, že sme zmenili kód a pridali ďalšiu transakciu.

```
import java.util.ArrayList;
import java.util.Arrays;

public class Main {

    ArrayList<Block> blockchain = new ArrayList<>();

    public static void main(String[] args) {
        String[] genesisTransactions={"Sender:Tomas, Recipient: Fero, Amount:15 BTC",
                                      "Sender: Jano, Recipient: Strapo, Amount:13 BTC"};
        Block genesisBlock=new Block( previousHash: 0,genesisTransactions);

        String[] block2Transactions={"Sender: Fero, Recipient: Tomas, Amount:45 BTC","Sender: Igor, Recipient: Michal, Amount:23 BTC"};
        Block block2=new Block(genesisBlock.getBlockHash(),block2Transactions);

        String[] block3Transactions={"Sender: Majo, Recipient: Miko, Amount:13 BTC","Sender: Tomas, Recipient: Igor, Amount:1000 BTC"};
        Block block3=new Block(block2.getBlockHash(),block3Transactions);

        System.out.println("Hash of Genesis block:");
        System.out.println(genesisBlock.getBlockHash());
        System.out.println("Hash of second block:");
        System.out.println(block2.getBlockHash());
        System.out.println("Hash of third block:");
        System.out.println(block3.getBlockHash());
    }
}
```

OBRÁZOK Č. 11– ZMENA ZDROJOVÉHO KÓDU TRIEDY MAIN.JAVA

Výstup z takto zmenených vstupov vyjadruje obrázok č.12.

```
/Library/Java/JavaVirtualMachines/jdk1.8.0_161.jdk/Contents/Home/bin/java ...
Hash of Genesis block:
845286529
Hash of second block:
-2007014516
Hash of third block:
-1034256293

Process finished with exit code 0
```

OBRÁZOK Č. 12. – VÝSTUP KONZOLOVEJ APLIKÁCIE PO ZMENE ÚDAJOV V PRVOM BLOKU GENESIS

Toto je priamy dôkaz toho, že nemožno zmeniť obsah bloku bez toho aby sme nezmenili digitálny podpis vo všetkých nasledujúcich blokoch. Na tomto princípe funguje blockchainova technológia. Samozrejme toto je veľmi zjednodušený príklad fungovania tejto technológie, avšak toto je jedna z najdôležitejších vlastností, ktorú blockchain obsahuje.

Záver

Platobné systémy zažívajú v dnešnej dobe evolúciu čo spôsobilo, že je stále viac a tento trend zatiaľ napreduje. Platobné systémy sú zároveň digitálnymi menami, pomocou ktorých sa obchoduje stále viac. Je to spôsobené stále sa vytvárajúcimi novými výhodami týchto systémov. Transakcie sú vďaka nim oveľa rýchlejšie, lacnejšie a súkromnejšie. Vznik nových kryptomien prináša zo sebou väčšiu slobodu v spôsoboch platieb ale aj možnosti zárobku v podobe ťaženia týchto kryptografických peňazí, čo predstavuje proces validovania transakcií.

Popularitu a úspech kryptomien možno vyčísliť v hodnote za ich jednotku či trhovú kapitalizáciu danej meny. Kapitalizáciu len tých najúspešnejších môžeme počítať v stovkách biliónoch dolároch. O kryptomenách momentálne môžeme hovoriť ako o jednom s najväčších trendov informatickej či finančnej spoločnosti.

Z hľadiska využitia daného systému by som za najviac pokročilú považoval Ethereum, ktorý sa dá považovať za niečo viac než digitálnu menu. Z hľadiska súkromia a rýchlych transakcií výrazne vytŕča z radu kryptomena Dash. Úplne nový pohľad nám priniesla kryptomena Ripple, ktorá funguje na odlišných princípoch, no napriek tomu dosahuje úspech, keď už teraz implementovala svoj systém do rôznych bankových systémov a z hľadiska kapitalizácie zatiaľ dosahuje bronzovú tretiu priečku. Bitcoin považujem za pôvodcu všetkých týchto úspechov, keďže vďaka svojmu úspechu akceleroval celkový vývoj tejto oblasti.

Jednou z najdôležitejších technológií, ktorú zo sebou Bitcoin priniesol je technológia blockchain. Tú používa drvivá väčšina všetkých kryptomien ako technológiu verejného distribuovaného záznamu. Táto technológia sa začína využívať vo veľkom a to nie len v oblasti kryptografických mien.

Pomocou programovacieho jazyka Java sa mi podarilo interpretovať vlastnosť nemožnosti zmeny záznamov v blockchaine bez povšimnutia. Konzolová aplikácia dokáže pridávať reťazce do blokov a tie sú naprogramované tak, aby pri zmene akéhokoľvek údaja v bloku, bol zmenený digitálny podpis aktuálneho bloku a všetkých blokov nasledujúcich po ňom. A presne túto vlastnosť má aj blockchain.

Raketový štart kryptografických mien je poháňaný inováciami, ktoré sú v nich implementované a naďalej vyvíjané. Ich veľké množstvo na trhu svedčí aj o prvkoch originality , o ktoré sa každá z nich snaží. Asi väčšina kryptomien používa veľmi podobné technológie a napriek tomu vznikajú stále nové. To je spôsobené hlavne tým, že aj napriek veľkým podobnostiam navonok, je každá z nich vzácna práve tým čím sa odlišuje. To bolo dokázané aj v tejto bakalárskej práci.

Zoznam bibliografických odkazov

[1] VONDRUŠKA, Pavel. 2006. Kryptologie, šifrování a tajná písma. Praha: Albatros nakladatelství, a.s., 2006. 335 s. ISBN 80-00-01888-8.

[2] MENEZES, Alfred.-VAN OORSCHOT, Paul-VANSTONE, Scott. A. Handbook of applied cryptography. Vyd. 5. Boca Raton : CRC Press, 2001. str. 816. ISBN 08-493-8523-7.

[3] STANEK, Martin. Kryptológia: Pragmatický pohľad. Katedra informatiky FMFI UK, 2013. 19 s. Dostupné na internete:
<http://www.dcs.fmph.uniba.sk/~stanek/Kryptologia%20v1b.pdf>

[4] LEE KUO CHUEN, David. Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data. Singapore: Elsevier, 2015. ISBN 978-0-12-802117-0.

[5] KUCHÁŘ, Miloš. *Bezpečná síť : Jak zajistíte bezpečnost vaší sit*ě. Praha : Grada publishing, 1999. 148 s. ISBN 80-7169-886-5.

[6] DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. Computer Press, 2004. 190 s. ISBN 80-251-0106-1.

[7] SCHNEIDER, Bruce. *Applied Cryptography*. Wiley, 1996. 758 s. ISBN 0471128457.

[8] KUROSE, James. F. - ROSS, Keith. W. Počítačové sítě. Computer press, 2014. 624 s. ISBN 9788025138250

[9] CHOHAN, Usman. W. Cryptocurrencies: A Brief Thematic Review, University of New South Wales, 2017, 9 s.

[10] GUTTMANN, Benjamin. The Bitcoin Bible Gold Edition: Books On Demand. 2014. ISBN 978-3732296965.

[11] Difficulty (Cryptocurrencies). [online]. In: investopedia.com [cit. 23.4.2018]. Dostupné na internete: < https://www.investopedia.com/terms/d/difficulty-cryptocurrencies.asp>

[12] Explaining Hash Rate Or Hash Power In Cryptocurrencies. [online] In:coinsutra.com [cit. 1.5.2018]. Dostupné na internete: <https://coinsutra.com/hash-rate-or-hash-power/>

[13] Market Capitalization. [online]. In: investopedia.com [cit. 5.5.2018]. Dostupné na internete: **<**https://www.investopedia.com/terms/m/marketcapitalization.asp>

[14] Bitcoin mining pools. [online] In: buybitcoinworldwide.com [cit. 18.4.2018]. Dostupné na internete: <https://www.buybitcoinworldwide.com/mining/pools/>

[15] How to Set Up a Bitcoin Miner. [online] In: coindesk.com [cit. 12.4.2018]. Dostupné na internete: < https://www.coindesk.com/information/how-to-set-up-a-miner/>

[16] Consensus Mechanism (Cryptocurrency). [online] In: investopedia.com [cit. 19.4.2018]. Dostupné na internete: < https://www.investopedia.com/terms/c/consensus-mechanism-cryptocurrency.asp >

[17] Proof of Stake (PoS). [online] In: investopedia.com [cit. 5.4.2018]. Dostupné na internete: < https://www.investopedia.com/terms/p/proof-stake-pos.asp >

[18] Proof of Work. [online] In: investopedia.com [cit. 5.4.2018]. Dostupné na internete: < https://www.investopedia.com/terms/p/proof-work.asp>

[19] NAKAMOTO, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System. [online] In: bitcoin.org [cit. 17.1.2018]. Dostupné na internete: < https://bitcoin.org/bitcoin.pdf >

[20] Descriptions of SHA-256, SHA-384, and SHA-512. [online] In: iwar.org.uk [cit. 1.4.2018]. Dostupné na internete: <http://www.iwar.org.uk/comsec/resources/cipher/sha256-384-512.pdf>

[21] RUDLANG, Marit. Comparative Analysis of Bitcoin and Ethereum. 2017, 103 s. [online] In: brage.bibsys.no [cit. 11.3. 2018]. Dostupné na internete : <https://brage.bibsys.no/xmlui/bitstream/handle/11250/2451325/17050_FULLTEXT.pdf>

[22] Smart Contracts. [online] In: investopedia.com [cit. 14.3.2018]. Dostupné na internete: < https://www.investopedia.com/terms/s/smart-contracts.asp >

[23] Ethereum. [online] In: ethereum.org [cit. 16.1.2018]. Dostupné na internete: <https://www.ethereum.org/>

[24] Ethereum White Paper. [online] In: github.com [cit 16.1.2018]. Dostupné na internete: < https://github.com/ethereum/wiki/wiki/White-Paper>

[25] Keccak implementation overview. [online] In: keccak.team [cit. 12.5.2018] Dostupné na internete: <https://keccak.team/files/Keccak-implementation-3.2.pdf>

[26] SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions. [online] In: nvlpubs.nist.gov [cit. 1.5.2018]. Dostupné na internete: < https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf >

[27] Dash. [online] In: dashmasternode.org [cit. 16.4.2018]. Dostupné na internete: <http://dashmasternode.org/>

[28] ARMKNECHT, Frederik et al. Ripple: Overview and Outlook, 2015. 19 s. [online]

In: researchgate.net [cit. 15.2.2018]. Dostupné na internete:
< https://www.researchgate.net/publication/281631024_Ripple_Overview_and_Outlook >

[29] Ripple. [online] In: ripple.com [cit. 14.4.2018]. Dostupné na internete: <https://ripple.com/>

[30] HILEMAN, Garrick. – RAUCHS, Michel. Global cryptocurrency benchmarking study. 2017 [online] In: jbs.cam.ac.uk [Cit. 5.5.2018]. Dostupné na internete: <https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf>

[31] Menový pár. [online] In: xtb.com [cit. 17.4.2018]. Dostupné na internete: <https://www.xtb.com/sk/menovy-par-kb>

[32] BERENTSEN, Aleksander – SCHÄR, Fabian. A Short Introduction to the World of Cryptocurrencies, 2018, 16 s. Dostupné na internete :
< https://files.stlouisfed.org/files/htdocs/publications/review/2018/01/10/a-short-introduction-to-the-world-of-cryptocurrencies.pdf >

[33] Cryptocurrency statistics. [online] In: bitinfocharts.com [cit. 19.2.2018]. Dostupné na internete: < https://bitinfocharts.com/>

[34] Bitcoin Block Reward Halving Countdown. [online] In: bitcoinhalf.com [cit. 12.3.2018]. Dostupné na internete: < http://www.bitcoinblockhalf.com/>

[35] Bitcoin Mining Block Reward (Halving). [online] In: etherworld.co [cit. 30.4.2018]. Dostupné na internete: < https://etherworld.co/2017/04/05/bitcoin-mining-block-reward-halving/ >

[36] SCHIRRIFF, Ken. : Bitcoin mining the hard way: the algorithms, protocols, and bytes [online]. Dostupné z: http://www.righto.com/2014/02/bitcoin-mining-hard-wayalgorithms.html

[37] Bitcoin. [online]. In: bitcoin.com [cit. 15.1. 2018]. Dostupné na internete: <https://www.bitcoin.com/>

[38] Hashrate. [online]. In: cahts.bitcoin.com [cit. 15. 3. 2018]. Dostupné na internete: <https://charts.bitcoin.com/chart/hash-rate>

[39] Top 100 Coins by Market Capitalization. [online]. In: coinmarket.com [cit. 15.3.2018]. Dostupné na internete: < https://coinmarketcap.com/coins/>

[40] STROUKAL, Dominik. – SKALICKY, Jan. Bitcoin peníze budoucnosti, Praha: Ludwig von Mises Institut CZ&SK. 176 s. ISBN: 978-80-87733-26-4

[41] BITCOIN PRICE CHART WITH HISTORIC EVENTS. [online] In: 99bitcoin.com [cit. 14.3. 2018]. Dostupné na internete: <https://99bitcoins.com/price-chart-history/>

[42] How to mine Ethereum. [online]. In: coindesk.com [cit. 15.4. 2018]. Dostupné na internete: < https://www.coindesk.com/information/how-to-mine-ethereum/>

[43] Ethereum network hashrate chart. [online] In: coinwarz.com [cit. 15.4.2018]. Dostupné na internete: <https://www.coinwarz.com/network-hashrate-charts/ethereum-network-hashrate-chart>

[44] KHATWANI, Sudhir. Top 7 Profitable Proof Of Stake (POS) Cryptocurrencies. [online] In: coinsutra.com [cit. 14.4.2018]. Dostupné na internete: <https://coinsutra.com/proof-of-stake-cryptocurrencies/>

[45] MAHALINGAM, Vakeesan. DASH Mining Guide: How to Mine DASH Cryptocurrency. [online] In: cryptovest.com [cit. 14.4. 2018]. Dostupné na internete: < https://cryptovest.com/education/dash-mining-guide-how-to-mine-dash-cryptocurrency/>

[46] Dash Network Hashrate Chart and Graph. [online] In: coinwarz.com [cit. 14.3.2018]. Dostupné na internete: <https://www.coinwarz.com/network-hashrate-charts/dash-network-hashrate-chart >

[47] TSIHITAS, Theo. Dash vs Bitcoin: Has Dash Successfully Overcome Bitcoin's Shortcomings. 2017. [online] In: coincentral.com [cit. 14.4.2018]. Dostupné na internete: < https://coincentral.com/dash-vs-bitcoin-comparison/ >

[48] DUFFIELD, Evan. – DIAZ, Daniel. Dash: A Privacy-Centric Crypto-Currency. [online] In: github.com [cit. 14.3.2018]. Dostupné na internete: < https://github.com/dashpay/dash/wiki/Whitepaper>

[49] PrivateSend. [online]. In: docs.dash.org [cit. 14.3.2018]. Dostupné na internete:

<https://docs.dash.org/en/latest/introduction/features.html#privatesend>

[50] SCHWARTZ, David – YOUNGS, Noah – BRITTO, Arthur. The Ripple Protocol Consensus Algorithm. Ripple Labs Inc, 2014. [online] In: ripple.com [cit. 14.5.2018]. Dostupné na internete: <https://ripple.com/files/ripple_consensus_whitepaper.pdf>

[51] Ledger Data Formats. [online] In: ripple.com [cit. 14.4.2018]. Dostupné na internete: <https://ripple.com/build/ledger-format/>

Zoznam obrázkov

Zoznam tabuliek