BLOCKCHAIN TEHNOLOGIJA

Radovanac, Danijel

VELEUČILIŠTE U ŠIBENIKU

ODJEL MENADŽMENTA

STRUČNI STUDIJ INFORMATIČKI MENADŽMENT

Danijel Radovanac

BLOCKCHAIN TEHNOLOGIJE

Završni rad

Šibenik, 2020.

VELEUČILIŠTE U ŠIBENIKU

ODJEL MENADŽMENTA

STRUČNI STUDIJ INFORMATIČKI MENADŽMENT

BLOCKCHAIN TEHNOLOGIJE

Završni rad

Kolegij: Projektiranje i analiza informacijskih sustava

Mentor: Dr. Sc. Frane Urem, prof. v.š.

Student: Danijel Radovanac

Matični broj studenta: 1219055032

Šibenik, 2020.

Sadržaj

TEMELJNA DOKUMENTACIJSKA KARTICA

Veleučilište u Šibeniku Završni rad

Odjel menadžmenta

Preddiplomski stručni studij Menadžment

BLOCKCHAIN TEHNOLOGIJE

Radovanac Danijel

Magdalenićeva 14, 10410 Velika Gorica, dradovan@vus.hr

Sažetak rada

U današnje vrijeme kriptovalute se pojavljuju posvuda. U svijetu postoji preko 19.000 fizički prodajnih mjesta na kojima se mogu trošiti kriptovalute[1]. Hrvatska je također počela slijediti svjetske trendove modernizacije sustava plaćanja, te se svakog dana sve više poduzeća odlučuje implementirati ovaj sustav plaćanja u svoje poslovanje. Iza bilo koje kriptovalute nalazi se *blockchain* tehnologija, koja im daje sigurnost i funkcionalnost. Ona se opisuje kao baza podataka koja u sebi sadrži sve informacije o obavljenim transakcijama. S obzirom da se te informacije distribuiraju na više servera u mreži, svi sudionici imaju identične podatke zapisane kod sebe, što ovu tehnologiju čini decentraliziranom, odnosno ne može doći do prevare jer je svaka transakcija transparentna i vidljiva svakome. Osim toga, svaki blok u *blockchain*u je kronološki povezan sa prethodnim blokovima te je sinkroniziran sa mrežnim čvorovima, što znači da bi promjena podataka u jednom bloku značila preokret svih prethodnih blokova, a to čini prevaru i mijenjanje blokova gotovo nemogućim.

[1] https://coinmap.org/view/#/world/14.09395718/-13.71093750/2

Budući da *blockchain* može osigurati da podaci budu nepromjenjeni i transparentni, postoji ogroman potencijal za uklanjanje ne samo trećih strana, već i korupcije u različitim točkama lanca opskrbe. U radu se pobliže objašnjava *blockchain* tehnologija, njegova podjela, njegova svrha i njegov utjecaj na ukupan sustav plaćanja.

(35 stranica / 15 slika / 5 tablica / 16 literaturnih navoda / jezik izvornika: hrvatski)

Rad je pohranjen u: Knjižnici Veleučilišta u Šibeniku

Ključne riječi: *blockchain, kriptovaluta, blok, hash*

Mentor: Dr. Sc. Frane Urem, prof. v.š.

Rad je prihvaćen za obranu:

BASIC DOCUMENTATION CARD

Polytechnic of Šibenik Final paper

Department of Management

Professional Undergraduate Studies of Management

BLOCKCHAIN TECHONOLOGIES

Radovanac Danijel

Magdalenićeva 14, 10410 Velika Gorica, dradovan@vus.hr

Abstract

Nowadays cryptocurrency is appearing everywhere. There are over 19,000 physical outlets in the world where cryptocurrencies can be spent. Croatia has also started with the trends of modernization of the payment system, and every day more and more companies have decided to implement this payment system in their business. Behind any cryptocurrency is blockchain technology, which provides security and functionality. It is described as a database that contains all the information about the transactions performed. Since this information is distributed to multiple servers outside the network, all participants have identical data written to them, which makes this technology decentralized, i.e. it cannot be tampered with because every transaction is transparent and visible to everyone. In addition, each block is chronologically linked with previous blocks and is synchronized with network nodes, which means that changing the data in one block would mean reversing all previous blocks, making tampering with and changing blocks almost impossible.

Because blockchain can ensure that data is not tampered with and transparent, there is huge potential to remove not only third parties but also corruption at various points in the supply chain. In this paper blockchain technology is explained, as is its division, its purpose and its impact on the overall payment system.

(35 pages / 15 figures / 5 tables / 16 references / original in Croatian language)

Paper deposited in: Library of Polytechnic in Šibenik

Keywords: *blockchain, cryptocurrency, block, hash*

Supervisor: Dr. Sc. Frane Urem, prof. v.š.

Paper accepted:

1. Uvod

Trenutno, većina ljudi koriste pouzdanog posrednika, poput banke, prilikom obavljanja transakcija. S druge strane *blockchain(engl.)* omogućava potrošačima i dobavljačima da se izravno povežu, uklanjajući potrebu za trećom stranom. Izmišljena još 2008. godine, *blockchain* tehnologija oslikala je promjene koje mogu donijeti u različitim poslovnim područjima. Tehnologija je, čak i u svojim začecima, poremetila različite industrije i sektore. Različite značajke kao što su decentralizacija, transparentnost i nepromjenjivost čine ga privlačnim za poslovne sektore širom svijeta.

Decentralizacija – decentralizirana priroda *blockchain* tehnologije znači da se ne oslanja na središnju točku kontrole. Nedostatak jedinstvenog autoriteta čini sustav pravednijim i znatno sigurnijim. Umjesto oslanjanja na središnje tijelo za siguran rad s drugim korisnicima, *blockchain* koristi inovativne konsenzusne protokole preko mreže čvorova, za provjeru transakcija i bilježenje podataka na način koji se ne može korumpirati.

Transparentnost – transparentnost je jedna od najvećih prednosti *blockchain* tehnologije. Iako su algoritmi koji se nalaze u tehničkim detaljima vrlo zamršeni i kompliciran, cijeli koncept je jednostavan. Ako se neka transakcija obavi i spremi u decentraliziranu mrežu, *blockchain* će omogućiti da se izmijenjeni podaci odmah vide te se može utvrditi je li njima manipulirano.

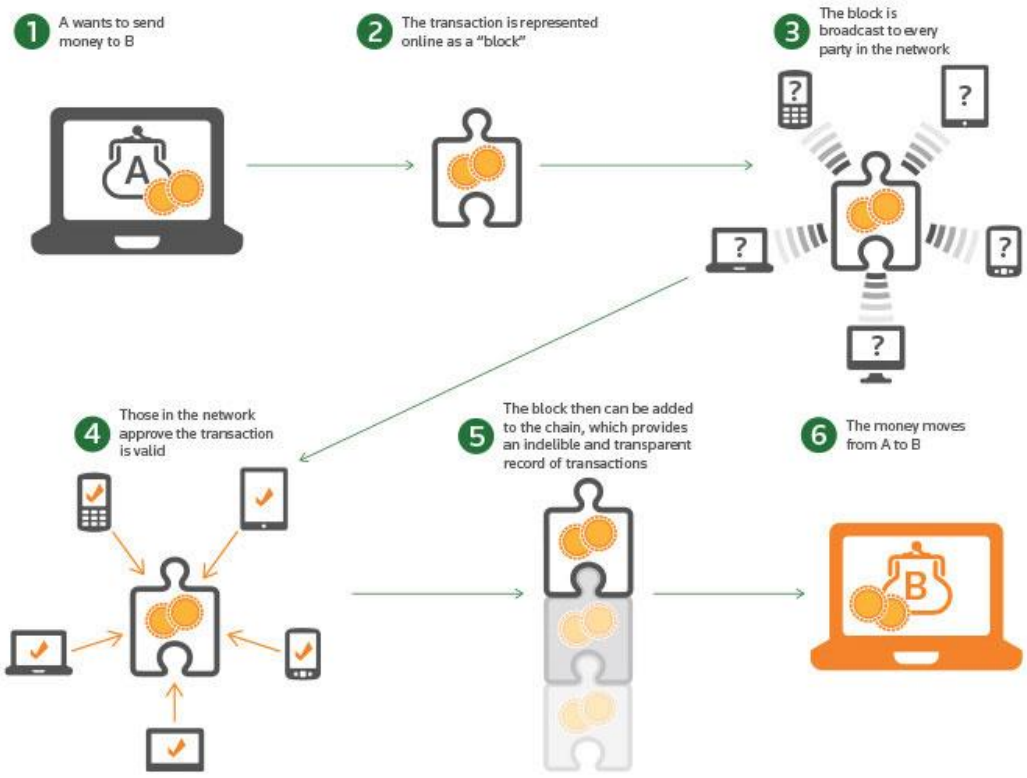
Kako se sustav ne oslanja na središnje tijelo, naknade koje organizacije obično naplaćuju više nisu čimbenik. Stoga se može pretpostaviti da je transakcija na *blockchainu* jeftinija, jer jedini troškovi koje sudionici imaju su nominalne naknade koje se koriste za nagrađivanje rudara ili krivotvorina koji vode čvor u mreži. Prema tvrdnji Harvard Business Review-a[2], *blockchain* će učiniti bankama ono što je Internet učinio za medije. Kada su u pitanju banke i financijske organizacije današnjeg dana, *blockchain* ima potencijal riješiti puno problema. *Blockchain* tehnologija posjeduje sve privlačne karakteristike potrebne pouzdanom tehnologijom koja uključuje novac. Siguran je, zaštićen, transparentan, decentraliziran, i relativno jeftiniji.

Prvobitno nastala kao podloga za potrebe kriptovalute *Bitcoin*, *blockchain* tehnologije danas imaju puno širu primjenu. Iako je trenutno najznačajnija za financijski sektor, *blockchain* tehnologija se

[2] https://hbr.org/2017/03/the-blockchain-will-do-to-banks-and-law-firms-what-the-internet-did-to-media

može primijeniti u nizu brojnih sektora koji bi nam omogućili ne samo niže troškove i čekanje u raznoraznim redovima na šalterima, već i lakšu svakodnevicu.

Slika 1.: Prikaz rada blockchain tehnologije



Izvor: *https://www.iotforall.com/blockchain-explained/*

Iako *blockchain* ima ogroman potencijal za stvaranje novih financijskih, dobavljačkih lanaca i digitalnih identitetskih sustava, to je još uvijek tehnologija u razvoju s malo proizvodnih sustava, a tu se javljaju i problemi upravljanja i ranjivosti. U ovom radu ćemo se osvrnuti na sve prednosti i mane *blockchain* tehnologije te ćemo pomnije promotriti nastanak i princip rada ove tehnologije. Također ćemo govoriti o raznim primjenama *blockchain* tehnologije, fokusirajući se na kriptovalute, koje su svakim danom sve popularnije i sve više prisutnije u svakodnevnom životu.

2. Blockchain

Sama riječ *blockchain* se može doslovno prevesti kao 'lanac blokova'. Radi se o podatkovnim blokovima koji su povezani u jednosmjerni lanac gdje svaki novi blok ovisi o prvom, odnosno ranijem, bloku. Ova tehnologija se temelji na kriptografiji. Svaki blok u lancu je konačan, što znači da ima određenu količinu podataka ili transakcija koju može pohraniti. Nakon što se blok popuni kreira se novi blok koji je povezan s prethodnim blokom i s onim koji će tek biti kreiran u budućnosti. Sigurnost *blockchaina* se nalazi u tome što ako netko želi izmijeniti podatke u jednom bloku, trebao bi izmijeniti podatke u svima što je skoro pa nemoguće. Podatak se u trenutku zapisa ne može se više mijenjati te se ne može doći do manipulacije istih.

2.1. Povijest blockchaina

Ideja koja stoji iza *blockchain* tehnologije opisana je već 1991. godine, kada su znanstvenici Stuart Haber i W. Scott Stornetta predstavili računalno praktično rješenje za vremensko žigosanje digitalnih dokumenata kako ih se ne bi moglo krivotvoriti. Sustav je koristio kriptografski osiguran lanac blokova za pohranjivanje vremenski označenih dokumenata, a 1992. godine Merkle-ovo stablo ugrađeno je u dizajn, što je učinilo cijeli proces učinkovitijim dopuštajući prikupljanje nekoliko dokumenata u jedan blok.

Ipak, *blockchain* kakvog poznajemo danas, opisan je i definiran 2008. godine kada je jedna neidentificirana osoba pod pseudonimom Satoshi Nakamoto digao web stranicu zvanu „*'Bitcoin*: *A Peer-to-Peer Electronic Cash System',* gdje je taj sistem opisao kao 'ravnopravna *peer-to-peer* verzija elektroničke gotovine koja bi omogućila izravno slanje online plaćanja s jedne stranke na drugu bez prolaska kroz financijsku instituciju.'[3]

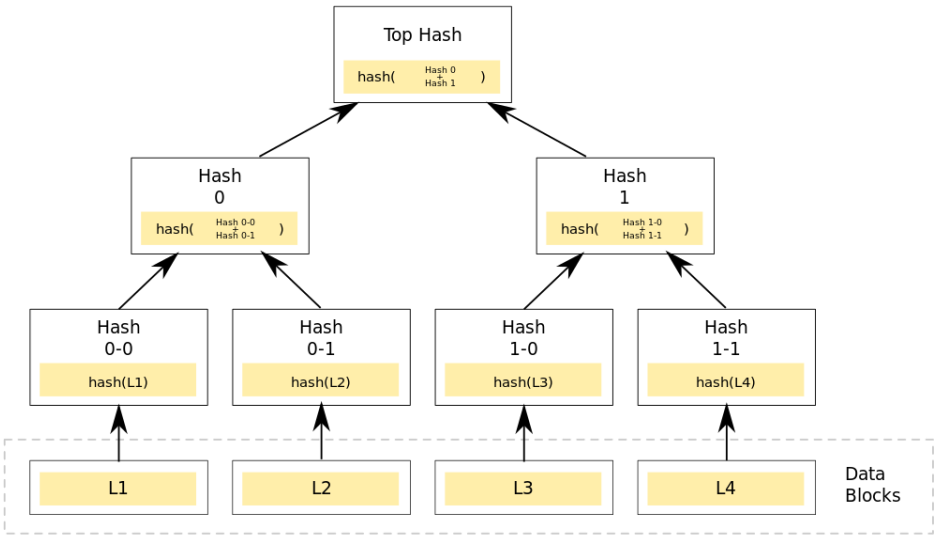
Blockchain pruža alternativu klasičnom sustavu te zaobilazi treću stranu, odnosno centraliziranog posrednika. U *blockchainu*, taj posrednik se zamjenjuje decentraliziranom mrežom anonimnih računala koji potvrđuju transakcije na bazi algoritma. Iza računala se nalazi bilo koji pojedinac koji potvrđivanjem transakcije bude nagrađen, odnosno „rudari“ *bitcoin* ili bilo koju drugu kriptovalutu koja se „rudari“.

[3] https://nakamotoinstitute.org/bitcoin/

2.1.1. Merkleovo stablo

„Merkleovo stablo je kriptografska stablasta struktura u kojoj je svaki čvor koji nije list, obilježen *hashem labela* njegove djece-čvorova. Nazvana su po Ralphu Merkleu koji je prvi predložio takav koncept. Podaci koji se trebaju kriptirati, razbijaju se u blokove te se ti blokovi zatim *hashiraju* i ti *hashevi* predstavljaju listove stabla. Iduća se razina stabla dobiva konkateniranjem (spajanjem) parova listova te njihovim *hashiranjem*. Postupak se ponavlja sve dok na kraju ne ostane samo jedan čvor, takozvani Merkleov korijen.“[4]

Slika 2.: Binarno hash stablo-“Merkle-ovo stablo”



Izvor: *https://bitcoin.com.au/what-is-a-merkle-tree-and-how-does-it-help-organize-data-on-the-bitcoin-blockchain/*

2.2. Vrste blockchaina

Postoje tri primarna tipa blok-lanaca; javna, privatna i konzorcijska.

[4] http://btc-croatia.blogspot.com/2014/04/merkleovo-stablo.html

2.2.1. Javni blockchain

Javni blokovi su *open source*. Dopuštaju svakome da sudjeluje kao korisnici, rudari, programeri ili članovi zajednice. Sve transakcije koje se odvijaju na javnim blokovima su potpuno transparentne, što znači da svatko može pregledati pojedinosti transakcije. Ova vrsta *blockchaina* omogućila je i nagradu (ekonomske poticaje) za one koji koriste jedan od vrsta *proof-of-stake* ili *proof-of-work* algoritma.

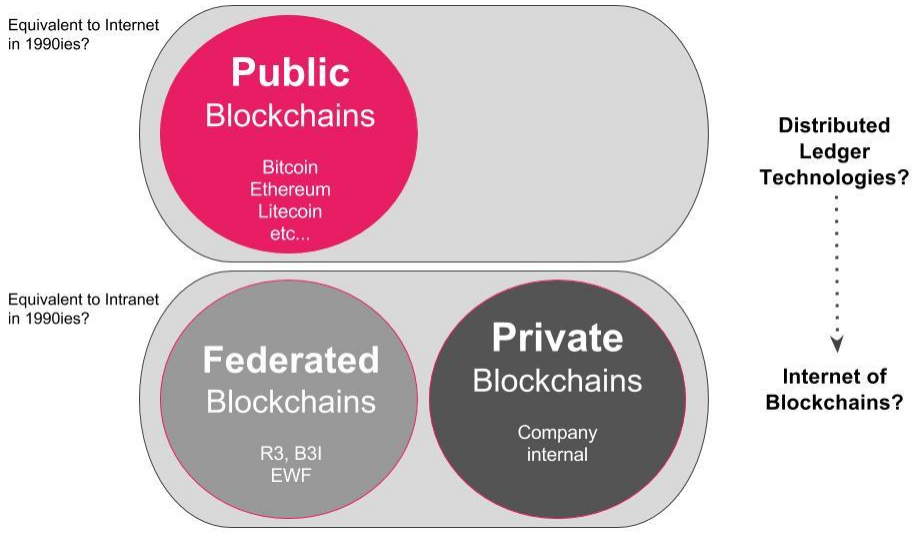
2.2.2. Privatni blockchain

Privatni blok-lanci, također poznati kao dopušteni blok-lanci, posjeduju brojne značajne razlike od javnih blokova. Svaki sudionik ovakve mreže mora biti prvotno pozvan odnosno odobren od strane administratora. Privatni blok-lanci su dragocjeni za poduzeća koja žele surađivati i dijeliti podatke, ali ne žele da njihovi osjetljivi poslovni podaci budu vidljivi na javnom *blockchainu*. Privatni blok-lanci mogu ili ne moraju imati token povezan s lancem.

2.2.3. Konzorcijski blockchain

Za konzorcijski *blockchain* se često kaže da je sustav koji je "polu-privatan" i ima kontroliranu skupinu korisnika, ali djeluje u različitim organizacijama. Ovakav pristup ima iste prednosti kao i privatni blok-lanac i može se smatrati potkategorijom privatnih blok-lanaca, za razliku od zasebnog tipa lanca.

Slika 3.: Podjela blockchaina



Izvor: *https://blockchainhub.net/blockchains-and-distributed-ledger-technologies-in-general/*

2.3. Struktura bloka

„*Blockchain* se kao što mu samo ime govori sastoji od blokova. Blok je struktura podataka u kojoj su zapisane digitalne informacije koje se dijele putem *blockchaina*. Iz tablice vidimo da se jedan blok sastoji od zaglavlja u kojem su upisani meta-podaci te liste digitalnih informacija varijabilne dužine:“[5]

Tablica 1.: Struktura bloka

Veličina	Naziv	Opis
4 bajta	Veličina bloka	Veličina bloka u bajtovima
80 bajtova	Zaglavlje bloka	Meta-podaci o bloku
1-9 bajtova	Brojač zapisa	Koliko zapisa sadrži blok
Varijabilno	Zapisi	Zapisi pohranjeni u bloku

[5] https://skolakoda.org/struktura-blockchain-bloka

2.3.1. Zaglavlje bloka

Zaglavlje svakog bloka sastoji se od 80 bajtova podataka koji služe kao dodatne tehničke informacije o bloku i povezivanju blokova u lanac. Struktura zaglavlja bloka dana je u tablici 2..

Tablica 2.: Struktura zaglavlja bloka

Veličina	**Naziv**	**Opis**
4 bajta	Verzija	Verzija protokola u vrijeme nastajanja bloka (specifično za Bitcoin)
32 bajta	Hash prethodnog bloka	Referenca na prethodni blok u lancu koji još nazivamo roditelj bloka
32 bajta	Korijen binarnog hash stabla	Kriptografski hash koji sadrži informacije o svim zapisima u bloku
4 bajta	Vremenska oznaka	Vrijeme kada je blok kreiran i uključen u *blockchain*
4 bajta	Težinska oznaka	Težina algoritma čije je rješenje potrebno za uključivanje bloka u *blockchain*
4 bajta	*Nonce*	Broj pomoću kojeg je riješen algoritam za uključivanje bloka u *blockchain*

„*Hash* prethodnog bloka predstavlja rezultat dvostruke primjene SHA-256 *hash* funkcije nad zaglavljem prethodnog bloka u lancu. *Hash* bloka, koji je zapravo *hash* zaglavlja bloka, je jedinstveni identifikator svakog pojedinog bloka. Primijetimo, *hash* bloka zapravo nije dio strukture bloka. On se izračunava na strani svakog čvora kada čvor ima potrebe za time, na primjer kada primi novi blok koji je uključen u lanac. Također, u svrhu vremenske uštede čvor može održavati zasebnu bazu podataka u kojoj su spremljeni *hash*-evi blokova.

Vremenska oznaka predstavlja kada je blok dodan u lanac.

Težinska oznaka i ***nonce*** su meta-podaci koji se koriste prilikom dodavanja u lanac.

Korijen binarnog *hash* stabla predstavlja informaciju dobivenu od svih zapisa u bloku.“[6]

2.4. Decentralizirani sustav ravnopravnih partnera

Sustav ravnopravnih partnera građen prema modelu ravnopravnih partnera (eng. *peer-to-peer*) sastoji se od velikog broja istovrsnih procesa, takozvanih partnera (eng. *peer*). Partneri obavljaju zadaće prema potrebama svojih korisnika. Ako je partneru pri obavljanju neke zadaće potrebna pomoć on stupa u komunikaciju sa svojim susjedima, a ti susjedi sa svojim susjedima i tako se komunikacija odvija na razini cijelog sustava.

Cijeli decentralizirani sustav zasniva na ideji ravnopravnih partnera. Općenito, sustav ravnopravnih partnera pruža najbolji i najjeftiniji način da veliki broj korisnika dođe do neke datoteke, a troškovi takve komunikacije postaju relativno mali i dijele se među korisnicima.

U privatnim *blockchain* sustavima, svaki od partnera će obavljati sve od navedenih funkcija, dok ćemo u javnim prema funkcijama koje partneri obavljaju i razlikovati samu vrstu partnera. Partneri se dijele na; *miner* (rudar), potpuni partner, *blockchain* partner i novčanik.

[6] https://skolakoda.org/struktura-blockchain-bloka

Slika 4.: Zadaće i vrste partnera u sustavu

Izvor: *https://repozitorij.veleri.hr/islandora/object/veleri%3A1594/datastream/PDF/view*

2.4.1. Blockchain partner

Blockchain partner održava *blockchain* sa svim zapisima, počevši od prvog bloka koji se naziva generički blok na koji se nadovezuju svi ostali blokovi sve do zadnjeg kreiranog. Za razliku od jednostavnog novčanika *blockchain* partner nema potrebe za oslanjanjem na ostale partnere u svrhu pretraživanja *blockchaina* ili provjere integriteta podataka.[7]

[7] https://repozitorij.veleri.hr/islandora/object/veleri%3A1594/datastream/PDF/view

2.4.2. Jednostavni novčanik

„U javnim sustavima koji koriste *blockchain* zbog velike količine podataka svaki korisnik nema mogućnost pohraniti cijeli *blockchain*. Takav korisnik tada u sustavu sudjeluje kao jednostavan novčanik i na slici 4 prepoznajemo ga po tome što u svojim zadaćama nema crveni krug pod nazivom održavanje *blockchain*-a. Glavna zadaća koju jednostavni novčanik obavlja je kreiranje novih zapisa u skladu s protokolom koji propisuje sustav.“[8]

2.4.3. Rudar

„Partneri rudari preuzimaju nove zapise koje su kreirali novčanici, formiraju ih u blokove i dodaju u *blockchain*. U *blockchain* protokolu dodavanje novih zapisa iziskuje korištenje računalnih resursa. Kada rudar pronađe blok u *blockchain*-u, rješavajući algoritam pod nazivom '*proof-of-work*' i koristeći svoje računalne resurse, tada sve transakcije u tom bloku postaju potvrđene i zapisuju se u *blockchain*, a rudar kao nagradu za korištenje svojih računalnih resursa dobiva određeni broj digitalne valute za svoj doprinos mreži. Povećanjem broja rudara koji sudjeluju u mreži, povećava se i sigurnost same mreže. Veći broj rudara omogućuje više različitih lokacija, na kojim se može zapisati blok u *blockchainu* i nikad se ne zna koji rudar će pronaći blok i zapisati ga. Time se postiže velika sigurnost, jer se ne zna lokacija zapisa i samim time ne može se utjecati na nju.“ [9]

[8] Ibid

[9] Ibid

3. Hash funkcije

Osnovna ideja *hash*-funkcija je da *hash* služi kao digitalni otisak ulazne vrijednosti i da se ne može dobiti pomoću neke druge ulazne vrijednosti. Cijela *blockchain* tehnologija se zasniva na iskorištavanju svojstva *hash*-eva. *Blockchain* tehnologija iskorištava važna svojstva *hash*-eva. Relativno je lako proizvesti *hash* iz podataka kao što je *bitcoin* blok, no gotovo je nemoguće otkriti koji su to podatci putem *hasha*.

Općenito, *hash* funkcija je bilo funkcija koja za ulaz ima podatke proizvoljne veličine, a kao izlaz vraća podatke fiksne veličine. Kriptografske *hash* funkcije su jednosmjerne odnosno nemaju inverz. Jedini način da se kreiraju ulazni podaci kriptografske *hash* funkcije iz izlaza je pokušati pretraživanje *brute-force* algoritmom.

Hash funkcija je svaka funkcija koja se može upotrijebiti za mapiranje podataka proizvoljne veličine u vrijednosti fiksne veličine. Vrijednosti koje je vratila *hash* funkcija nazivaju se *hash* vrijednosti ili *hash* kodovi. *Hash* funkcije se često koriste u kombinaciji s *hash* tablicom, a one ubrzavaju pretraživanje tablice ili baze podataka otkrivanjem dupliciranih zapisa u velikoj datoteci.

Hash funkcije su dio suvremenih metoda informacijske sigurnosti. Osim enkripcije i digitalnog potpisa, oni su sastavni dio sigurne komunikacije, primjerice putem interneta. Ovdje je nebitno je li korišteni komunikacijski kanal nesiguran: moderna informacijska sigurnost također mora jamčiti sigurnost u nezaštićenim kanalima, koji su u najgorem slučaju dostupni svima.

3.1. Hash tablica

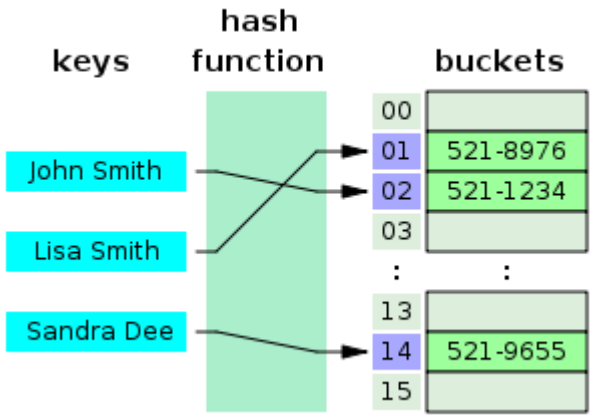
„*Hash* tablica je podatkovna struktura koja rabi *hash* funkciju za učinkovito preslikavanje određenih ključeva (na primjer imena ljudi) u njima pridružene vrijednosti (na primjer telefonske brojeve). *Hash* funkcija se koristi za transformiranje ključa u indeks (*hash*) to jest mjesto u nizu elemenata gdje treba tražiti odgovarajuću vrijednost.

U najboljem slučaju *hash* funkcija preslikava svaki mogući ključ u zaseban indeks, ali je to u praksi gotovo nemoguće. Većina implementacija *hash* tablica podrazumijeva da su *hash* kolizije – parovi

različitih ključeva s istim *hash* vrijednostima – obična pojava, i na neki način se brine da se ovaj problem svlada.“[10]

„U dobro dimenzioniranoj *hash* tablici, prosječna cijena (broj računalnih naredbi) svakog pronalaženja ne ovisi o broju elemenata uskladištenih u tablici. Mnoge implementacije *hash* tablica također omogućuju proizvoljna unošenja i brisanja parova ključeva i vrijednosti uz konstantnu prosječnu (amortiziranu) cijenu po operaciji.“[11]

Slika 5. Telefonski imenik kao hash tablica



Izvor: *https://hr.wikipedia.org/wiki/Hash_tablica*

3.2. SHA-256 kriptografska hash funkcija

SHA-256 spada u SHA-2 kriptografske funkcije čije je standarde osmislila NSA (National security agency). To je kriptografska *hash* funkcija koja uzima ulaz kao 20 bajtova i prikazuje *hash* vrijednost u heksadecimalnom broju, dugačkih otprilike oko 40 znamenki.

U osnovi, koristi se u sigurnosne svrhe, kao što su stvaranje digitalnog potpisa, sustavi za provjeru datoteka i druge vrste provjere autentičnosti. Ova tehnologija se također koristi u *blockchain* tehnologiji za stvaranje kripto valute. MD5 je popularni algoritam raspršivanja koji se koristi od strane većine programera za integriranje sigurnosti u različite tipove algoritama.

[10] https://hr.wikipedia.org/wiki/Hash_tablica
[11] Donald Knuth (1998.). *The Art of Computer Programming'*, 2. izd., str. 513.–558., Addison-Wesley

Njegov radni proces je prilično složen, najprije mapira podatke slučajne veličine i te ih onda pretvara u *hash* kod, gdje je *hash* alfanumerički niz koji je kriptografska konverzija podataka.

Poruku čiju *hash* vrijednost želimo izračunati prvo:

(1) proširimo tako da je konačna dužina u bitovima djeljiva sa 512, a zatim

(2) podijelimo u blokove duzine 512 bitova $M^{(1)},M^{(2)},...,M^{(N)}$.

Blokovi poruke se obrađuju jedan po jedan: Počevši sa predodređenom početnom *hash* vrijednošću $H^{(0)}$, slijedno se računa

$$H^{(i)} = H^{(i)} + C_M{}^{(i)}(H^{(i-1)}),$$

gdje je C SHA-256 kompresijska funkcija, a '+' je word-wise mod 2^{32} zbrajanje. $H^{(N)}$ je *hash* vrijednost poruke M.

Izračunavanje *hash* vrijednosti počinje pripremanjem poruke; označimo ukupnu duljinu poruke P s d;

(1) Proširivanje poruke: Pretpostavimo da je duljina poruke M, u bitovima l. Dodajemo bit '1' na kraj poruke, i zatim k nula bitova, gdje je k najmanje ne negativno rješenje jednadžbe l + 1 + k = 448 mod 512. Na to se dodaje 64-bitni blok koji je jednak broju l zapisanom binarno. Na primjer, poruka "abc" (u 8-bitnom ASCII kodu) ima dužinu 8 * 32 = 24 pa se proširuje prvo sa '1' i zatim sa 448 – (24 + 1) = 443 nula bitova, nakon čega dobijemo prošireno poruku od 512-bitova

(2) Podijelimo poruku na N 512-bitnih blokova $M^{(1)},M^{(2)},...,M^{(N)}$. Prvih 32 bita i-tog bloka su označena sa $M_0^{(i)}$, sljedećih 32 bita su $M_1^{(i)}$, i tako do $M_{15}^{(i)}$. Koristi se isključivo big-endian zapis.

Tablica 3.: Pregled operatora

$\oplus$	**Bitwise XOR**
$\wedge$	Bitwise AND
$\vee$	Bitwise OR
$\neg$	Bitwise complement
+	Zbrajanje mod 2^{32}
$SHR^n(x)$	Pomak u desno za n bitova
$ROTR^n(x)$	Rotacija u desno za n bitova

Svi operatori djeluju nad 32-bitnim riječima.

Početna *hash* vrijednost $H^{(0)}$ je slijedeći niz 32-bitnih riječi:

Tablica 4.: Hash vrijednosti

$H_1^{(0)}$ = 6a09e667
$H_2^{(0)}$ = bb67ae85
$H_3^{(0)}$ = 3c6ef372
$H_4^{(0)}$ = a54ff53a
$H_5^{(0)}$ = 510e527f
$H_6^{(0)}$ = 9b05688c
$H_7^{(0)}$ = if83d9ab
$H_8^{(0)}$ = 5be0cd19

To su ostaci korijena prvih osam prim brojeva.

3.3. Hash vrijednosti nekih poruka

Hash vrijednost 24-bitne poruke "abc" u heksadecimalnom zapisu je:

ba7816bf 8f01cfea 414140de 5dae2223 b00361a3 96177a9c b410ff61 f20015ad

Hash vrijednost 448-bitne poruke:

“abcdbcdecdefdefgefghfghighijhijkijkljklmklmnlmnomnopnopq”

248d6a61 d20638b8 e5c02693 0c3e6039 a33ce459 64ff2167 f6ecedd4 19db06c1.

4. Algoritmi za postizanje konsenzusa

„Konsenzus ili sporazumna jednoglasna odluka je postupak donošenja odluka koji se ne zasniva na "vladavini većine" već na najvećoj mogućoj suglasnosti unutar skupine. U svijetu kriptovaluta, pojam konsenzusa se odnosi na princip verifikacije transakcija. Konsenzus je metoda kojim se razlikuju ispravne od 'lažnih', malicioznih transakcija."[12]

Konsenzusni algoritam može se definirati kao mehanizam putem kojeg *blockchain* mreža postiže konsenzus. Javni (decentralizirani) *blockchainovi* grade se kao distribuirani sustavi i, budući da se ne oslanjaju na središnje tijelo, distribuirani čvorovi trebaju se dogovoriti o valjanosti transakcija. Tu se pojavljuju konsenzusni algoritmi. Uvjeravaju da se poštuju pravila protokola i jamče da se sve transakcije događaju na pouzdan način, tako da se novčići mogu potrošiti samo jednom.

4.1. Problem usuglašavanja bizantskih generala

„Problem Bizantinskih generala u kojem je grupa generala dio bizantske vojske okružila Grad s kraljem na čelu. Ti generali žele formulirati plan napada na grad. U svom najjednostavnijem obliku, generali moraju samo odlučiti hoće li se napasti ili povući. Neki generali možda preferiraju napad, a neki se više vole odstupiti. Za primjer ćemo uzeti da se unutar dvorca nalazi 300 vojnika i neka dvorac okružuje 5 vojnih jedinica s po 100 vojnika. Jedino general koji vodi 3. vojnu jedinicu je izdajnik, nazovimo ga G3. Prema tome, generali G1, G2, G4 i G5, odani su kralju. Ako generali G1, G2, G4 i G5 izvedu napad na dvorac, postoji šansa da poraze 300 vojnika koji brane dvorac, čak i uz to da se general G3 pridruži obrani dvorca, ali to trebaju izvesti istovremeno i koordinirano."[13] Cilj generala G3 je izbjeći istovremeni napad jedinica G1, G2, G4 i G5 a to će izvesti ovako:

[12] https://www.kriptovaluta.hr/tutorials/sto-je-konsenzus-i-koje-sve-vrste-postoje/
[13] The Byzantine Generals' Problem, (2015), Dug Campbell,str.396., 8.8.2018.

(1) G1 šalje poruku "Napad u 18 sati." prema G2,

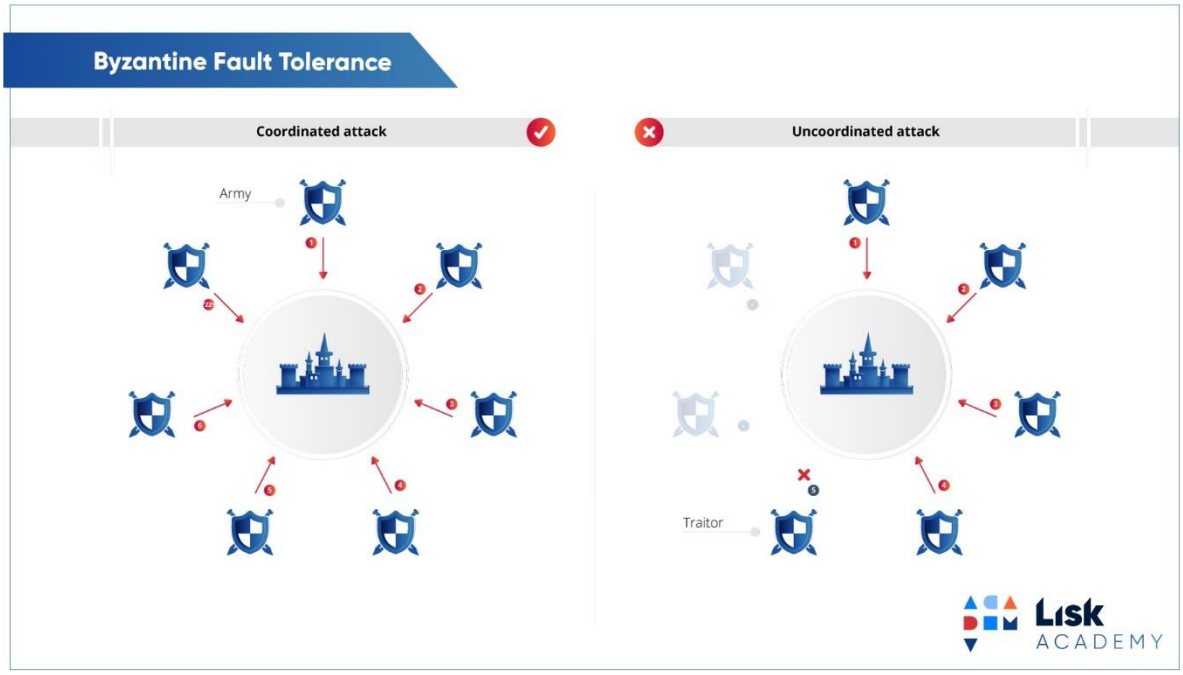
(2) G2 šalje tu istu poruku "Napad u 18 sati." prema G3,

(3) G3 je izdajica, on mijenja sadržaj poruke u "Napad u 17 sati." i šalje je prema G4,

(4) G4 šalje poruku "Napad u 17 sati." prema G5.

Nakon izmjene poruka vojska generala G4 i G5 napadaju dvorac s kombiniranih 200 vojnika u 17 sati, misleći da će im se ostatak vojske pridružiti. Budući da generali G1 i G2 misle da je napad u 18 sati ne priključuju se napadu u 17 sati. Vojna jedinica generala G3 se može u bilo kojem trenutku priključiti obrani dvorca i tada 400 vojnika brani dvorac. 200 vojnika G4 i G5 nemaju šanse protiv vojnika koji brane svoj dvorac te gube bitku. U 18 sati generali G1 i G2 gube bitku od brojčano moćnije obrambene vojske. Ovaj primjer možemo primijeniti i u *blockchain* tehnologiji gdje nam generali predstavljaju partnere u distribuiranom sustavu. Digitalni podaci koje želimo upisati u *blockchain* su poruke među generalima. Pojedini partner ne zna broj ostalih partnera kao ni koji od njih su partneri izdajnici (njima je u interesu upisati podatke koji nisu ispravni niti istiniti). Algoritmi za postizanje konsenzusa omogućuju partnerima da u ovakvim uvjetima budu sigurni da su svi podaci koji upisuju u nove blokove nepromjenjivi i istiniti.

Slika 6.: Primjer napada samo lojalnih generala i napada s izdajicama



Izvor: *https://lisk.io/academy/blockchain-basics/how-does-blockchain-work/byzantine-fault-tolerance-explained*

4.2. Proof-of-work (PoW)

Proof-of-work u Bitcoinu funkcionira kao alat koji se koristi za obradu blokova transakcija i njihovo dodavanje u *blockchain*. Drugim riječima, PoW se koristi za stvaranje blokova. Proces generiranja ispravnih dokaza kako bi se blok dodao *blockchainu* poznat je kao „rudarenje“, a pojedinci koji sudjeluju u procesu poznati su kao „rudari“. Prva primjena distribuiranog i nepovjerljivog algoritma konsenzusa je Bitcoinov PoW algoritam. PoW od rudara zahtijeva da riješe složene kriptografske zagonetke prije nego što mogu dodati blok u *blockchain*.

U zamjenu za rješavanje zagonetke, rudari se nagrađuju BTC-om. Važno je napomenuti da svaki blok koji je dodan u *blockchain* mora slijediti određeni skup pravila konsenzusa. Da bi došli do bloka rudari se moraju međusobno natjecati kako bi pronašli ispravan *hash* za svaku *hash* funkciju. Postoji poteškoća s mrežom koja se dinamički prilagođava ovisno o tome koliko je rudarima teško pronaći ispravne *hashove*. Čim rudar naiđe na ispravnu *hash* vrijednost, svi ostali čvorovi u sustavu provjeravaju ispravnost prije izvršavanja transakcije za kreiranje novog bloka.

Algoritam konsenzusa PoW funkcionira kao alat koji se koristi za obradu blokova transakcija i njihovo dodavanje u *blockchain*. Čvorovi unutar mreže provjeravaju svaki blok prije nego što je dodan u *blockchain*.

Slika 7.: Prikaz PoW

Izvor: *https://wolfcone.com/proof-of-work-and-proof-of-stake-explained/*

4.3. Proof-of-stake (PoS)

Algoritam konsenzusa PoS je relativno drugačiji i nov način generiranja blokova unutar *blockchaina* od algoritma PoW. Uz PoW, rudarima koji pronađu ispravan *hash* omogućeno je generiranje novih blokova i za to su nagrađeni. Međutim, uz PoS sistem, pojedinci koji su izabrani za stvaranje bloka, koji se nazivaju *validatori*, ovise o različitom skupu kriterija. Specifični kriteriji razlikuju se ovisno o PoS sistemu, ali u većini sustava izabran je *validator* za generiranje novog bloka na temelju njihovog ekonomskog udjela u mreži. Tako su, na primjer, *validatori* odabrani za generiranje novog bloka s vjerojatnošću koja je proporcionalna količini kovanica koje *validator* posjeduje. Dakle, što više kovanica *validator* ima u svojem novčaniku, to je veća vjerojatnost da će biti izabran za stvaranje bloka.

Pojedini PoS sistemi uzimaju u obzir i duljinu vremena koje je *validator* držao kovanice u svom novčaniku. Taj se kriterij obično naziva „starost kovanica“ (*coin age*). Starost kovanice definiran je kao iznos kovanica pomnožen s brojem dana koliko su se kovanice držali u novčaniku. Stoga je vjerojatnije da će biti izabran *validator* koji posjeduje kovanice u dužem vremenskom razdoblju za generiranje novog bloka. PoS se vidi kao superiorniji mehanizam za stvaranje blokova u odnos na PoW zbog razloga koji se primarno odnose na potrošnju energije. PoW sistem za Bitcoin zahtijeva ogromnu količinu energije. Procijenjeno je da bi se otprilike 6,5 milijuna američkih kućanstava moglo pogoniti energijom koja se trenutno troši na *Bitcoin*. Umjesto trošenja električne energije na proizvodnju bezbroj *hasheva* za pravo generiranje bloka, kao što se zahtijeva u PoW sistemima, *validatori* u PoS sistemima su odabrani za stvaranje blokova na temelju njihovog ekonomskog udjela u mreži, a to je sustav koji zahtijeva znatno manje računalnih resursa za rad. Kao takav, smatra se mnogo pouzdanijim i energetski učinkovitijim sustavom.

Algoritam PoS koristi *validatore* koji se odabiru na temelju kriterija koji uključuju starost novca i ekonomski ulog. Također zahtijeva znatno manje energije zahvaljujući svojim kriterijima za odabir *validatora*.

Algoritam konsenzusa PoW se smatra jednim od najboljih rješenja problema bizantskih generala, koji je omogućio stvaranje Bitcoina kao dio sustava problema usuglašavanja bizantskih generala. To znači da je Bitcoin *blockchain* vrlo otporan na napade, poput 51% napada (većinski napad). Ne

samo zato što je mreža decentralizirana, već i zbog PoW algoritma. Remećenje mreže i visoki troškovi „rudarenja“ čine ulaganje vlastitih sredstva rudara vrlo teškim i malo vjerojatnim.

Slika 8.: Prikaz PoS

Izvor: *https://wolfcone.com/proof-of-work-and-proof-of-stake-explained/*

Algoritmi konsenzusa ključni su za održavanje integriteta i sigurnosti mreže kriptovaluta. Omogućuju sredstva distribuiranih čvorova koji postižu konsenzus o tome koja je inačica *blockchaina* stvarna. Dogovaranje o trenutnom stanju *blockchaina* bitno je za ispravan rad digitalnog ekonomskog sustava.

5. Upotreba blockchaina

Prvobitno nastala kao podloga za potrebe kriptovalute Bitcoin, *blockchain* tehnologije danas imaju puno širu primjenu. Iako je trenutno najznačajnija za financijski sektor, *blockchain* tehnologija se može primijeniti u nizu brojnih sektora koji bi nam omogućili ne samo niže troškove i čekanje u raznoraznim redovima na šalterima, već i lakšu svakodnevicu.

5.1. Kriptovaluta

Kao što smo već napomenuli, *Bitcoin* je postao prva kriptovaluta ikada kada je objavljena 2009. Međutim, tek nekoliko godina kasnije, kada se stvorilo sve više i više kriptovaluta, ljudi su počeli trgovati, Ideja je stvarno jednostavna; trguje se jednom kripto valutom za drugu, uz nadu da novčić koji kupite poveća svoju vrijednost. Koncept je isti kao na burzi. Kada ljudi trguju, trebaju koristiti razmjenu kriptovaluta. Tako se kupci i prodavači mogu podudariti. Na primjer, posjedujemo *Bitcoin* i želimo ga prodati za *Ethereum*, razmjena će nam pomoći naći prodavača *Ethereuma* s kojim možete trgovati. Burze će nam naplatiti naknadu za to, što obično košta oko 0,1% za svaku razmjenu. Trgovanje kriptovalutama sada je zaista popularno, jer se dnevno kupuju i prodaju u vrijednosti milijarde dolara.

Kriptovaluta je u osnovi digitalni način zadržavanja i prijenosa vrijednosti „online“. To je internetski medij razmjene koji koristi kriptografske funkcije za obavljanje financijskih transakcija. Kriptovalute podupiru *blockchain* tehnologiju za postizanje decentralizacija, transparentnosti i nepromjenjivosti. Dostupno je nekoliko desetaka različitih kriptovaluta, a najveće i najpoznatije su *Bitcoin* i *Ethereum.*

Vrijednost bilo koje kriptovalute u bilo kojem trenutku ovisi o ponudi i potražnji. Obično je u bilo kojem trenutku dostupan fiksni iznos bilo koje valute, pa što je više ljudi želi iskoristiti, to je viša cijena. Na primjer, krajem 2017. godine, cijena jednog *bitcoina* porasla je otprilike 20 000 USD, a zatim je pala na cijenu od oko 4000 USD.

Odnos državnih institucija prema *Bitcoinu* varira od zemlje do zemlje. U Njemačkoj *Bitcoin* ima status privatnog novca, u Danskoj i Ujedinjenom Kraljevstvu se na trgovanje *bitcoinom* ne plaća

porez, a u većini zemalja EU se bitcoin slobodno koristi.[14] [15] No, neke vlade su neprijateljski nastrojene prema *bitcoinu*; Rusija je zabranila korištenje *bitcoina*, a u Kini kupnja *bitcoina* podliježe određenim ograničenjima, na primjer kineske banke ne smiju poslovati s *bitcoin* tvrtkama).

Tablica 5.: 5 kriptovaluta s najvećom tržišnom vrijednosti na dan 25.08.2020.

Redni broj	Naziv kriptovalute	Oznaka	Vrijednost u američkim dolarima (USD)	Promjene vrijednosti u zadnjih 24 sata(%)
1.	Bitcoin	BTC	11,522.17	-2.24
2.	Ethereum	ETH	390.08	-4.04
3.	Ripple	XRP	0.2828	-2.46
4.	Bitcoin Cash	BCH	283.16	0.07
5.	Litecoin	LTC	60.09	-2.55

5.1.1. Bitcoin

Nedugo nakon pokreta „zauzmimo Wall Street“[16] pojavio se *Bitcoin*, nakon što su građani optužili velike banke za zloupotrebu novca zajmoprimaca, varanje klijenata, lažiranje sustava i naplaćivanje nevjerojatnih naknada. Pioniri *Bitcoina* su htjeli staviti prodavača na glavno mjesto, ukloniti posrednika, otkazati kamate i imati transparentne transakcije, pobiti korupciju i smanjiti naknade. Stvoren je decentralizirani sustav, gdje sami kontroliramo svoja sredstva i znamo tijek događanja u svakom trenu. *Bitcoin* je stigao daleko u relativno kratkom vremenu. Po cijelom svijetu tvrtke su, od privatne bolnice u Varšavi[17] do velikih poduzeća kao što su *Dell*, *PayPal* i *Microsoft,* prihvatile valutu. Na web stranicama se sve više promovira, publikacije poput *Bitcoin*

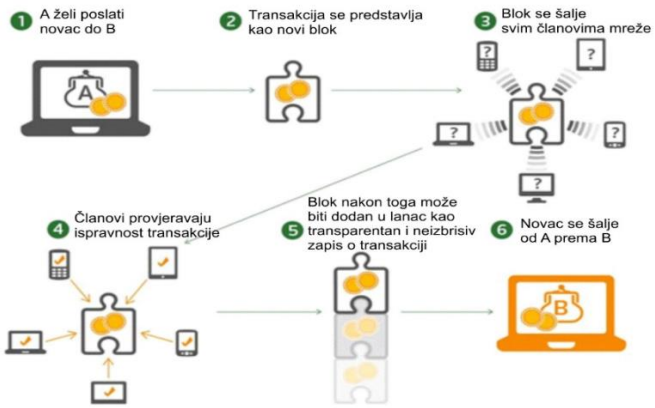
[14] https://crobitcoin.com/danska-ukinula-porez-na-bitcoin/
[15] https://crobitcoin.com/uk-pdv-bitcoin-trgovanje/
[16] https://hr.wikipedia.org/wiki/Occupy_Wall_Street
[17] https://www.coindesk.com/patients-can-pay-surgery-polish-hospital-bitcoin

Magazina objavljuju novosti, forumi raspravljaju o kriptovaluti i trguju svojim kovanicama. Ima svoje sučelje za programiranje aplikacija (*API – application programming interface*), indeks cijena i tečaj.

Kao što smo već objasnili, *Bitcoin* radi na *blockchainu*, gdje su sve potvrđene transakcije uključene u takozvane 'blokove'. Kako svaki blok ulazi u sustav, on se emitira na ravnopravnu mrežu, vršnjačka računalna mreža korisnika radi provjere valjanosti. Na taj su način svi korisnici svjesni svake transakcije, koja sprječava krađu i dvostruko trošenje, gdje netko troši istu valutu dva puta. Proces također pomaže da *blockchain* korisnici vjeruju u sustav.

Iskopavanje ili obrada osiguravaju sigurnost *Bitcoin* procesa kronološkim dodavanjem novih transakcija (ili blokova) u lanac i držanjem u redu čekanja. Blokovi se odrezuju kako se svaka transakcija finalizira, šifre se dekodiraju, a *bitcoinovi* prosljeđuju ili razmjenjuju. Rudari također mogu generirati nove *bitcoine* pomoću posebnog softvera za rješavanje kriptografskih problema. To pruža pametan način izdavanja valute i također daje poticaj ljudima da se rude. Kompenzaciju dogovaraju svi u mreži, ali uglavnom je 12,5 bitcoina kao i naknade koje plaćaju korisnici koji šalju transakcije. Da biste spriječili inflaciju i održali sustav upravljivim, do 2040. u opticaju ne može biti više od fiksnog ukupnog broja od 21 milijuna *bitcoina* (ili BTC-ova), pa je „zagonetku“ sve teže riješiti. Trenutno postoji nešto više od 18400000[18] izrudarenih *bitcoina*, a jedini način da se stvori novi bitcoin je rudarenje. Novi blok se izrudari približno svakih 10 minuta.

Slika 9.: Funkcioniranje bitcoina



Izvor: https://www.ucionica.net/internet/sto-su-bitcoin-blockchain-i-kriptovaluta-4199/

[18] https://www.buybitcoinworldwide.com/how-many-bitcoins-are-there/

5.1.2. Litecoin

Litecoin, lansiran 2011. godine, bio je među početnim kriptovalutama nakon *Bitcoina* i često ga nazivaju "srebrom za *bitcoinovo* zlato". Stvorio ga je Charlie Lee, diplomirani MIT-ovac i bivši *Googleov* inženjer. *Litecoin* se temelji na globalnoj mreži plaćanja otvorenog koda koju ne kontrolira nijedno središnje tijelo i koristi "skriptu" kao dokaz rada, koji se može dekodirati uz pomoć *CPU-a* potrošačke razine. Iako je *Litecoin* na mnogo načina sličan *bitcoin*-u, on ima bržu stopu stvaranja bloka i stoga nudi bržu potvrdu transakcije. Osim programera, sve je veći broj trgovaca koji prihvaćaju *Litecoin*. Isto kao i *Bitcoin*, prvi rudar koji uspješno provjeri blok je nagrađen s 25 *litecoina*. Broj litecoina nagrađenih za takav zadatak s vremenom se smanjuje. U listopadu 2015. prepolovljena je, a ono će se nastaviti u pravilnim razmacima sve dok ne bude izrudaren 84 000 000. *litecoin*. Taj proces se događa svake četiri godine, a prošle godine se dogodio 05.08. Iduće smanjenje će se dogoditi 04.08.2023. godine.[19]

5.1.3. Ripple

„*Ripple* (XRP) jest kriptovaluta osmišljena 2012. godine. *Ripple* u užem smislu riječi u biti ne predstavlja kriptovalutu, već protokol za prijenos novaca. Osmišljen je kao protokol za internacionalna plaćanja između banaka. Osnovna ideja jest zamijeniti stare principe rada poput *SWIFT-a* (koji je razvijen 1972. g. i dalje se koristi). On nastoji surađivati s aktualnim financijskim svijetom, a cilj mu je biti globalna mreža, platforma koja će omogućiti svakome da prenese novac u bilo kojoj valuti u bilo koju valutu u nekoliko sekundi. Slično *Bitcoinu,* koristi tehnologiju distribuirane mreže (*blockchain*). No u usporedbi s *Bitcoinom,* transakcije u *Ripple* mreži su brže, provizije za transakcije su daleko niže.“[20]

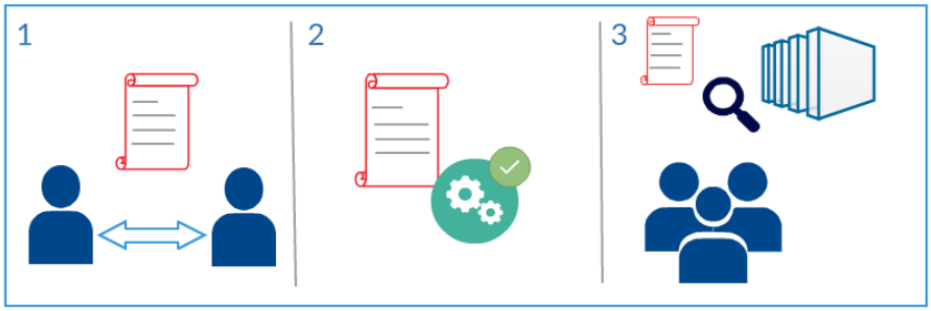
[19] https://www.litecoinblockhalf.com/
[20] https://www.kriptovaluta.hr/altcoin/sto-je-ripple-xrp-te-isplati-li-se-ulagati/

5.2. Pametni ugovori

Pametni ugovori u ovom se vremenu mogu nazvati najkorištenijom primjenom *blockchain* tehnologije. Koncept pametnih ugovora uveo je Nick Szabo, pravni znanstvenik i kriptograf 1994. Zaključio je da se bilo koja decentralizirana knjiga može koristiti kao ugovori koji su kasnije nazvani pametnim ugovorima. Ovi digitalni ugovori mogu se pretvoriti u kodove i dopustiti im da se izvode na *blockchainu*. Iako je ideja pametnih ugovora nastala davno, trenutni svijet u kojem živimo djeluje na papirnim ugovorima. Čak i ako se koriste digitalni ugovori, uključivanje pouzdane treće strane iz sustava ne može se isključiti. Iako smo definirali sustav funkcioniranja ovom metodom; ne možemo sa sigurnošću reći je li uvijek glatka. Uključivanje treće strane moglo bi dovesti do sigurnosnih pitanja ili lažnih aktivnosti zajedno s povećanom naknadom za transakcije.

"Pametni ugovor predstavlja kod u nekom programskom jeziku koji olakšava razmjenu novca, nekretnina, dionica ili bilo kakvih vrijednosti. Možemo reći da pametni ugovori služe za reguliranje nekog poslovnog odnosa između stranaka među kojima ne postoji uzajamno povjerenje. Takav kod se može zapisati na *blockchain* i izvršavati na bilo kojem računalu u distribuiranoj mreži. Pametan ugovor se automatski izvršava kada su zadovoljeni specifični uvjeti."[21]

Slika 10.: Pametni ugovor



Izvor: *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3195066*

[21] https://skolakoda.org/pametni-ugovori

„Slika prikazuje proces kreiranja pametnih ugovora. Koraci su sljedeći:

(1) Moguća razmjena dobara između dva ili više partnera zapisuje se kao programerski kod i pohranjuje na *blockchain*. Partneri ostaju anonimni, no sadržaj pametnog ugovora javno je dostupan svim partnerima u sustavu.

(2) Varijable poput datuma ili određene količine novca potiču izvršavanje ugovora prema pravilima definiranim u kodu

(3) Ostali korisnici sustava mogu pretražiti *blockchain*, kako bi razumjeli aktivnosti definirane ugovorom ili provjerili rezultat izvršavanja ugovora.“[22]

5.2.1. Primjer upotrebe pametnog ugovora

- Naručili ste robu putem internetske trgovine. Vaša uplata za robu je zabilježena u *blockchainu*, a tek nakon potvrde kurirske službe da je roba koju ste uzeli i zadovoljni njenom kvalitetom, novac ide prodavaču.
- Tijekom glasanja, ako bi se svi glasovi pohranili na *blockchain*, bilo bi je gotovo nemoguće hakirati i dekodirati. Pored toga, automatizirana priroda pametnih ugovora može učiniti zamorni proces glasanja mnogo jednostavnijim i potpuno online. To čak može potaknuti nisku izlaznost koju Amerika obično dobije.
- Primjer bi mogla biti tarifa osiguravajućeg društva koja se temelji na načinu na koji klijenti upravljaju svojim vozilima. Vozila bi bila ona koja ove podatke prijavljuju osiguravajućim društvima, te se po tome računa njihova rata.
- Pretpostavimo da svoj stan iznajmite na tjedan putem *airbnb*-a, osim što je ovo verzija *airbnb*-a koja postoji na *blockchainu* u kojoj možete platiti u kripto valuti. Nakon plaćanja, dobivate digitalni račun kao što je to diktirano u kodu pametnog ugovora. Pametni ugovor prati primate li "digitalni ključ" ili ne. Ako ne primite taj ključ do određenog datuma, pametni ugovor vam automatski izvršava povrat novca.

[22] Ibid

5.2.2. Ethereum

Godine 2013. Vitalik Buterin, programer i suosnivač *Bitcoin Magazina*, izjavio je da je *Bitcoinu* potreban skriptni jezik za izgradnju decentraliziranih aplikacija. Ne uspijevajući postići dogovor u zajednici, Vitalik je započeo razvoj nove distribucijske računalne platforme temeljene na *blockchainu*, *Ethereum*, koja je sadržavala pametne ugovore. Ponovimo, pametni ugovori su programi ili skripte koji se raspoređuju i izvršavaju na *Ethereum blockchainu*, a mogu se koristiti na primjer za obavljanje transakcije ako su ispunjeni određeni uvjeti. Pametni ugovori pišu se na određenim programskim jezicima i sastavljaju se u bajt kod, koji je decentralizirani Turingov kompletni virtualni stroj zvan *Ethereum* virtualni stroj (EVM) koji zatim može čitati i izvršiti.

Programeri također mogu kreirati i objavljivati aplikacije koje se izvode unutar *Ethereum blockchaina*. Te se aplikacije obično nazivaju *DApps* (decentralizirane aplikacije) i već postoje stotine *DApps-ova* koji rade u bloku *Ethereum*, uključujući platforme društvenih medija, igre za kockanje i razmjenu financija.

Kripto valuta *Ethereuma* naziva se *Ether*, može se prenositi između računa i koristiti za plaćanje naknada za računsku moć koja se koristi prilikom izvršavanja pametnih ugovora.

5.2.2.1. Ether

Ether je temeljni token koji napaja *Ethereum blockchain*, ali služi malo drugačijoj svrsi nego što *bitcoin* to čini na *Bitcoin blockchainu*. Iako se *etherom* trguje na javnim tržištima i ima aprecijaciju cijena sličnu *bitcoinu*, po dizajnu su prilično različite. *Ether* nije namijenjen kao jedinica valute na *peer-to-peer* mreži plaćanja; radije djeluje kao "gorivo" ili "plin" koji pokreće *Ethereum* mrežu.

Na najvišoj razini, *Ethereum* je platforma otvorenog koda koja vodi pametne ugovore. Kad se pametni ugovori izvode na *blockchainu*, oni se izvršavaju kada se ispune određeni uvjeti. Izvršenje pametnih ugovora zahtijeva računske resurse koji se moraju na neki način platiti: tu dolazi *ether*.

Ether je kripto-gorivo koji omogućuje pokretanje pametnih ugovora. To pruža poticaj čvorovima da provjere blokove na *Ethereum blockchainu*, koji sadrži kod pametnog ugovora. Svaki put kada se blok provjerava, stvara se 5 *ethera* i dodjeljuju se uspješnom čvoru. Novi blok se širi otprilike

svakih 15–17 sekundi. Neki čvorovi mogu pronaći ispravno rješenje za blok bez uključivanja u mrežu. Mreža *Ethereum* nagrađuje takve čvorove s 2–3 etera.

Slika 11.: Ether

Izvor: *http://kripto-portal.com/sto-je-ethereum-eth/*

5.3. Prednosti, nedostaci i nestabilnost kriptovaluta

"Investiranje u kriptovalute najčešće se povezuje uz *Bitcoin*, čija je cijena općeniti pokazatelj kretnji tržišta, pa se ponegdje naziva i "digitalnim zlatom". No, danas postoje stotine drugih kriptovaluta i gotovo svakodnevno se pojavljuju nove. Neke opstaju i rastu, neke se gase, no rast kripto tržišta je ustrajan. Stoga niti ne čudi kako sve više internetskih trgovina nudi plaćanje i kriptovalutama, a vlasnici "digitalnih novčanika" žele ponude u kojima svoje kriptovalutne jedinice mogu mijenjati za proizvode ili usluge."[23]

Niz je elemenata koji pozitivno utječu na ulaganje u kriptovalute:[24]

- Hakiranje *Blockchain*-a težak je posao, jer zahtijeva istovremeno hakiranje nekoliko tisuća računala, što je gotovo nemoguće;
- Ima ozbiljan potencijal da zamijeni trenutni novčani sustav u svijetu, jer broj korisnika kriptovaluta raste;

[23] https://ec.europa.eu/croatia/cryptocurrencies_and_blockchain_all_you_need_to_know_hr
[24] https://sh.wikipedia.org/wiki/Kriptovaluta

- Zbog ograničene količine kovanica, otporan je na inflaciju, a kreiranje novca zahtjeva ulaganje u hardver i električnu energiju.

Uz mnoge prednosti kriptovalute imaju i mane. Polovicom 2018. Godine znanstvenici sa Sveučilišta Texas u Austinu su uvjerljivo pokazali da je nedavni eksplozivni rast cijena (kao i strmoglavi pad) posljedica manipulacije.[25] Nedostatci kriptovaluta su: [26]

- Transakcije kriptovaluta su nepovratan proces nakon nekoliko potvrda transakcije;
- Jedna od stvari koje kriptovalute nemaju u odnosu na standardne kreditne kartice je zaštita korisnika od prijevare;
- Mnoge banke ne pružaju usluge kriptovalutama i njihovim korisnicima, također odbijajući suradnju s digitalno-valutnim kompanijama;
- Mogu biti zauvijek izgubljene/uništene zbog nekog štetnog softvera ili gubitka podataka na internetu.

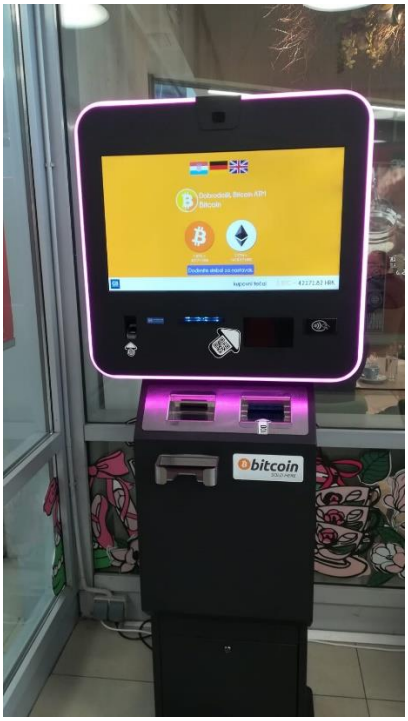
5.4. Pretvorba kriptovaluta u pravi (fizički novac)

Prvi *Bitcoin* bankomat je instaliran u listopadu 2013. godine u Vancouveru u Kanadi. Danas se u Hrvatskoj nalaze čak 4 *Bitcoin* bankomata, 2 u Zagrebu, 1 u Splitu i 1 u Rijeci, a nedavno je u Splitu otvorena i prva *Bitcoin* mjenjačnica.

„Od 15. srpnja svi domaći i strani korisnici svoje kriptovalute mogu promijeniti u kune u zadarskim poštanskim uredima, priopćeno je danas iz Hrvatske pošte. Rezultat je to provođenja pilot-projekta u sklopu većeg procesa digitalizacije poslovanja, što je jedna od razvojnih strategija Hrvatske pošte. Pilot-projekt ostvaruje se u suradnji s hrvatskom tvrtkom *Electrocoin* , koja već pet godina vodi servis *bitcoin-mjenjacnica.hr*, provodi se u tri poštanska ureda u Zadru, a pokazat će interes tržišta za ovakvu vrstu usluge.“[27]

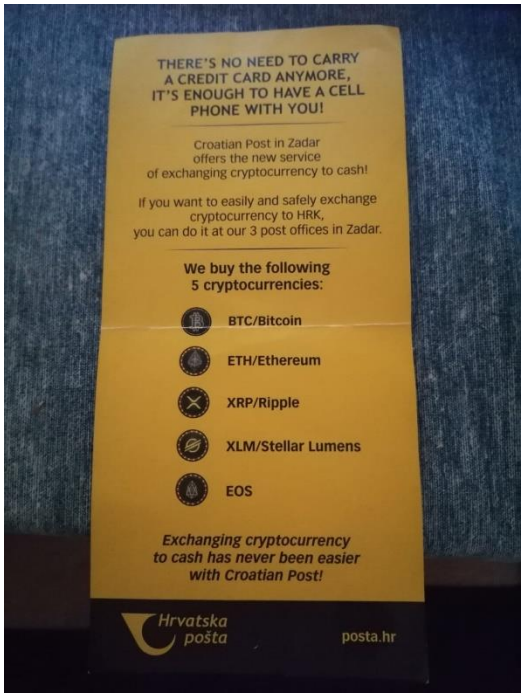
[25] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3195066
[26] Ibid
[27] https://www.bug.hr/kriptovalute/hrvatska-posta-kroz-pilot-projekt-postaje-mjenjacnica-kriptovaluta-10655

Slika 12.: Bitcoin bankomat u Zagrebu



Izvor: *Fotografija autora*

Slika 13. i 14.: Dvostrani letak Hrvatske Pošte za izmjenu kriptovaluta



Izvor: *Fotografije autora*

6. Rudarenje

Rudarstvo se naziva rudarstvom, jer je to proces u kojem dobrovoljci ulažu veliki napor u nadi da će dobiti „zlatnik“. Najveća briga za rudare oduvijek je bila sve veća poteškoća računalnih zagonetki uključenih u osiguravanje blokova. Kako je riješeno više zagonetki, težina sljedeće zagonetke uvelike se povećava, ponekad čak i eksponencijalno. Da bi rudarstvo bilo isplativo, organizacije su uložile mnogo u istraživanje i razvoj naprednijih algoritama rješenja i učinkovitijih dijelova hardvera. Neke su organizacije otišle toliko daleko da su svoje rudarske uređaje premjestile u zemlje u kojima je opskrba električnom energijom jeftinija. U pogledu hardvera, neke organizacije sa značajnim kapitalom investirale su u ASIC-ove ili integrirane sklopove specifične za aplikaciju. Ova klasa hardvera dizajnirana je za dovršavanje vrlo specifičnih zadataka, točnije rudarstva.

Digitalne se informacije mogu reproducirati relativno lako, tako da kod bitcoina i drugih digitalnih valuta postoji rizik da jedan potrošač može kopirati svoj bitcoin i poslati ga drugoj strani dok još uvijek drži original. Recimo da je netko pokušao duplicirati račun od 20 kuna kako bi original i krivotvorinu potrošio u prodavaonici. Da je prodavač znao da kupci dupliciraju novac, sve što bi trebao učiniti je pogledati serijske brojeve računa. Da su brojevi identični, službenik bi znao da je novac dupliciran. Ova analogija je slična onome što radi bitcoin rudar kada provjeravaju nove transakcije.

S čak 600.000 kupovina i prodaja u jednom danu provjera svake od tih transakcija može biti puno posla za rudare. Kao što smo rekli, kao naknadu za svoj trud, rudari dobivaju bitcoin kad god dodaju novi blok transakcija u *blockchain*. Količina novog bitcoina oslobođenog svakog miniranog bloka naziva se "nagrada na bloku". Nagrada za blok se prepolovljava na svakih 210.000 blokova ili otprilike svake 4 godine. 2009. godine bilo je 50 BTC-a. U 2013. godini bilo je 25 BTC-a, u 2018. 12,5 BTC-a, a negdje sredinom 2020. prepolovit će se na 6,25. Po ovoj brzini prepolovljenja, ukupni broj *bitcoina* u optjecaju približit će se ograničenju od 21 milijun, što valutu čini vremenom oskudnijom i vrjednijom, ali i skupljom za proizvodnju rudarima.

Da bi rudari *bitcoinom* zapravo mogli zaraditi 1 BTC od provjere transakcija, moraju se dogoditi dvije stvari. Prvo, moraju potvrditi transakcije u vrijednosti od 1 megabajta (MB), koje teoretski mogu biti manje od 1 transakcije, ali češće nekoliko tisuća, ovisno o tome koliko podataka pohranjuje svaka transakcija. Ovo se smatra jednostavnijim djelom. Drugo, kako bi dodali blok transakcija u *blockchain*, rudari moraju riješiti složeni računalni problem iz matematike, koji se naziva i '*PoW- Proof-of-work*'. Ono što zapravo rade je pokušavaju smisliti 64-znamenkasti heksadecimalni broj, nazvan "*hash*", koji je manji ili jednak ciljanom *hashu*. U osnovi, rudarsko računalo izbacuje *hasheve* brzinom od megahaše u sekundi (MH / s), gigahaše u sekundi (GH / s) ili čak terahaše u sekundi (TH / s), ovisno o jedinici, pogađajući sve moguće 64- znamenke brojeva dok ne stignu do rješenja. Drugim riječima, to je kockanje. Razina težine najnovijeg bloka u vrijeme pisanja iznosi oko 6.061.518.831.027. To jest, vjerojatnost da računalo stvori *hash* ispod cilja je 1 na 661 618 831.027 - manje od 1 na 6 trilijuna. Ta se razina prilagođava svakih 2016 blokova ili otprilike svaka 2 tjedna, a cilj je da se stopa iskopavanja konstantno zadrži. Odnosno, što se više rudara natječe za rješenje, problem će postajati još teži. Točno je i suprotno. Ako se računska snaga isključi s mreže, poteškoća se prilagođava te se smanjuje kako bi olakšala rudarstvo.

Slika 15. „Mining“

Izvor: *http://younesscrypto-currency.blogspot.com/2016/06/swisscoin-cryptocurrency-how-does.html*

7. 6 značajki blockchain tehnologije

1) Povećani kapacitet

Najistaknutija stvar *blockchain* tehnologije je ta što povećava kapacitet cijele mreže. Zbog razloga što puno računala radi zajedno, što ukupno nudi veću snagu u odnosu na malo uređaja na kojima su stvari centralizirane.

2) Bolja sigurnost

Blockchain tehnologija ima bolju sigurnost jer ne postoji ni jedna mogućnost za gašenje sustava. Čak i najviša razina financijskog sustava podložna je hakiranju. *Bitcoin* u drugu ruku nikada nije bio hakiran.

3) Nepromjenljivost

Stvaranje nepromjenjivih glavnih knjiga jedna je od glavnih vrijednosti *blockchaina*. Svaka baza podataka koja je centralizirana podliježe hakiranju i zahtijeva povjerenje treće strane radi čuvanja baze podataka.

4) Brže podmirivanje

Tradicionalni bankarski sustavi mogu biti spori, jer im je potrebno puno vremena za namirenje, a to obično traje danima. To je jedan od glavnih razloga zašto određeni bankarski instituti trebaju nadograditi svoje bankarske sustave. Ovaj problem možemo riješiti pomoću *blockchaina* jer se tako može podmiriti prijenos novca u stvarno velikim brzinama. To u konačnici štedi puno vremena i novaca ovim institucijama, a potrošaču također pruža udobnost.

5) Decentralizirani sustav

Prije nego što su se pojavili *blockchain* tehnologije, bili smo naviknuti na centralizirane usluge. Ideja je vrlo jednostavna, imate centralizirani entitet koji pohranjuje sve podatke i morat ćete isključivo komunicirati s tim entitetom da biste dobili sve potrebne podatke. Drugi primjer centraliziranog sustava su banke. Pohranjuju sav vaš novac, a jedini način na koji možete nekome platiti je prolazak kroz banku. U decentraliziranom sustavu informacije ne pohranjuje samo jedan entitet. Zapravo, svi u mreži posjeduju informacije.

U decentraliziranoj mreži, ako želite komunicirati sa svojim prijateljem, to možete učiniti izravno, bez prolaska kroz treću stranu. To je glavna ideologija koja stoji iza *Bitcoina,* mi i samo mi sami upravljamo svojim novcem. Svoj novac možete poslati bilo kome što želite, a da ne morate prolaziti kroz banku.

6) Konsenzus

Svaki *blockchain* uspijeva zbog algoritama konsenzusa. Arhitektura je pametno dizajnirana, a algoritmi konsenzusa su jezgra ove arhitekture. Svaki *blockchain* ima konsenzus za pomoć mreži u donošenju odluka. Jednostavno rečeno, konsenzus je postupak odlučivanja za grupu čvorova koji su aktivni na mreži. Ovdje se čvorovi mogu brzo i relativno brže dogovoriti. Kad milijuni čvorova provjeravaju transakciju, konsenzus je apsolutno neophodan za nesmetano funkcioniranje sustava. Čvorovi možda ne vjeruju jedni drugima, ali mogu vjerovati algoritmima koji se nalaze u osnovi jezgre. Kako bi se održala decentralizacija, svaki *blockchain* mora imati algoritam konsenzusa, inače će se izgubiti njegova osnovna vrijednost.

8. Zaključak

U današnjem svijetu poslovanja, svaka organizacija ili korporacija želi zaštititi svoje podatke u svojim bazama. Napadi na digitalne podatke danas postaju sve češći i gotovo je nemoguće ne naći se na udaru jednog od njih, stoga mnoge organizacije ulažu u što bolju zaštitu protiv istih. Ako se ipak nađemo na udaru jednog takvog napada, posljedice mogu biti ogromne, ako ne i, za neke manje organizacije, pogubne. Stoga se *blockchain* tehnologija nameće kao optimalno rješenje. U radu smo razjasnili kako bitcoin nije *blockchain* tehnologija, nego je temeljenoj na njoj. Bitcoin je trenutno najbolje stojeća kriptovaluta, gdje 1 BTC vrijedi oko 11.000 američkih dolara. On je prvi pokušaj održavanja decentralizirane javne knjige bez ikakve formalne kontrole ili upravljanjem. Digitalne valute su svjedočile početku *blockchain* tehnologije, no sam potencijal je vidljiv i mnogo dalje.

Blockchain tehnologija je tek na svojim začecima, s obzirom ne to da smo njenu prvu pravu implementaciju vidjeli prije jedno desetljeće. S razvojem informatičkih tehnologija kriptovalute su postale sve važniji faktor u ekonomiji te su svojim sve većim razvojem počele zabrinjavati centralne banke koje su morale reagirati na njihov rast. Decentraliziranost i neregularnost sustava smatra se najvećom prednosti kriptovaluta, ali se pokazalo i kao glavni uzrok velike volatilnosti jer cijena bitcoina i ostalih kriptovaluta ovisi isključivo o odnosu ponude i potražnje.

Samim time kako je manipulacija podacima unutar lanca onemogućena dobrom podlogom od strane tehnologije, *blockchain* bi se, u budućnosti u školstvu i drugim raznim institucijama mogla naći kao sastavni dio svakodnevice. Primjena *blockchain* tehnologije te realizacija direktnih umjesto centraliziranih transakcija može uvelike uvesti promijene u društveno-ekonomski svijet.

Literatura

1. Blockchain for dummies, IBM Limited Edition,(2017), Manav Gupta

2. Blockchain Basics, A Non-Technical Introduction in 25 Steps, Daniel Drescher, 2017

3. Donald Knuth (1998.). 'The Art of Computer Programming', 2. izd., Addison-Wesley

4. Swan M. (2015): Blockchain: Blueprint for a New Economy

5. Luka Grubišić, Robert Manger, Mreže Računala, predavanja, PMF, Zagreb, 2009.

6. Robert Manger, Miljenko Marušić, Strukture podataka i algoritmi, predavanja, PMF, Zagreb, 2003.

7. Maria Grazia Vigliotti, Haydn Jones, The Executive Guide to Blockchain, 2020.

8. https://prviplan.hr/analize-i-komentari/deset-godina-blockchaina-tehnologije-koja-mijenja-svijet/

9. https://blockchainhub.net/blockchains-and-distributed-ledger-technologies-in-general/

10. https://en.wikipedia.org/wiki/Blockchain

11. https://crobitcoin.com/bitcoin/transakcije/

12. https://www.coindesk.com/information/what-is-blockchain-technology

13. https://crobitcoin.com/altcoin/ethereum/

14. https://pcchip.hr/ostalo/tech/uvod-u-blockchain-tehnologiju/

15. http://younesscrypto-currency.blogspot.com/2016/06/swisscoin-cryptocurrency-how-does.html

16. https://wolfcone.com/