Sveučilište u Rijeci – Odjel za informatiku

Odjel za informatiku – jednopredmetna informatika

Sven Živković

Blockchain tehnologija

Završni rad

Mentor: dr.sc. Božidar Kovačić

Rijeka, 23.8.2018.

SADRŽAJ

1.UVOD

Blockchain tehnologija se zasniva na ideji da se digitalna informacija razmjenjuje između svih čvorova koji sudjeluju u nekom određenom sustavu. Svaki pojedini čvor održava svoju kopiju svake relevantne informacije i na taj se način izbjegava potreba za središnjim autoritetom koji vrši kontrolu nad informacijama. Prvi blockchain koncept predstavljen je od strane Satoshia Nakamote 2008. godine. Naredne godine blockchain je implementiram u prvu digitalnu valutu Bitcoin, gdje će ta tehnologija biti glavna podloga koja će koristiti za sve transakcije na mreži, koje će biti zapisane u glavnoj knjizi (''ledger'').
U današnjem društvu znamo da informacije koje kolaju mrežom i razmjenjuju se među korisnicima, imaju veliku važnost. Samim time kako su računala postala nepohodna sredstva za obavljanje mnogih poslovnih djelatnosti, možemo zaključiti da je i komunikacija putem mreže postala svakodnevica za gotovo svaku osobu. Jasno nam je da iz tog razloga moramo očuvati integritet informacija. Jedni od uvjeta koje želimo zadovoljiti je da se informacije kreću sigurnom mrežom, te da ih nitko ne može izmjenjivat u trenutku zapisivanja niti nakon toga.
Blockchain će nam omogućiti maksimalnu zaštitu zapisa na način da koristi kriptografske funkcije. Svaki pojedini čvor u sustavu posjedovat će ekvivalentne informacije što je postignuto uz primjenu algoritma za postizanje konsenzusa. Najpoznatiji su proof-of-work i proof-of-stake, o kojima ćemo više reći kasnije.

U današnjem svijetu poslovanja, svaka tvrtka, organizacija ili korporacija želi zaštititi svoj integritet podataka u svojim bazama. Napadi na digitalne podatke danas postaju sve učestaliji i gotovo je nemoguće ne naći se na udaru jednog od njih, stoga mnogi danas ulažu velike resurse u što bolju zaštitu svojih podataka odnosno informacija. Biti žrtva jednog od takvih napada može uzrokovati velike financijske gubitke, a za neke organizacije može biti i pogubno. Blockchain tehnologija se nameće kao optimalno riješenje, te ćemo u nastavku shvatiti i zašto.

2. BLOCKCHAIN

2.1. ŠTO JE BLOCKCHAIN

Blockchain se sastoji od blokova koji su nanizani, odnosno povezani u lanac gdje svaki od blokova ima niz zapisa. Blokovi se povezuju algoritmom koji koristi hash funkciju. Vezu između blokova je vrlo teško krivotvoriti odnosno hakirati, jer je to ujedno algoritam koji koristi kriptografiju visoke razine. Kako smo i ranije spomenuli, Blockchain tehnologija nastala je prvenstveno kao ideja na kojoj će se zasnivati digitalna kriptovaluta Bitcoin. Danas, mnoge industrije prepoznaju kvalitetu same tehnologije te ju mnoge isto tako nastoje implementirat u svoje poslovanje. Na primjeru Bitcoina kao prve digitalne valute koja koristi hash funkcije i blockchain vidimo kako je postignut način sigurnih transakcija bez središnjeg autoriteta.

Napomenimo da svaki blok u lancu ima konačnu količinu podataka ili transakcija koju može pohraniti. U trenutku kada se blok popuni, kreira se novi koji će biti povezan s blokom koji mu prethodi i s onim koji će tek biti kreiran u budućnosti. Sigurnost tehnologije počiva na tome zato što ukoliko netko želi izmjeniti podatke u jednom bloku, trebao bi to napraviti u svima što je gotovo nemoguće. Podatak u trenutku kada je zapisan ne može se više mjenjati, sve naredbe i radnje su zapisane i ne može doći do manipulacije podacima.

2.2. STRUKTURA BLOKA

Kako i samo ime govori, blockchain se sastoji od niza blokova (Slika 1.1) koji su lančano povezani. Blok (Tabela 1.1) je struktura podataka koja sadrži informacije. Sastoji se od zaglavlja gdje su upisani meta-podaci i liste digitalnih informacije odnosno podataka određene dužine.

Tabela 1.1 (Struktura bloka)

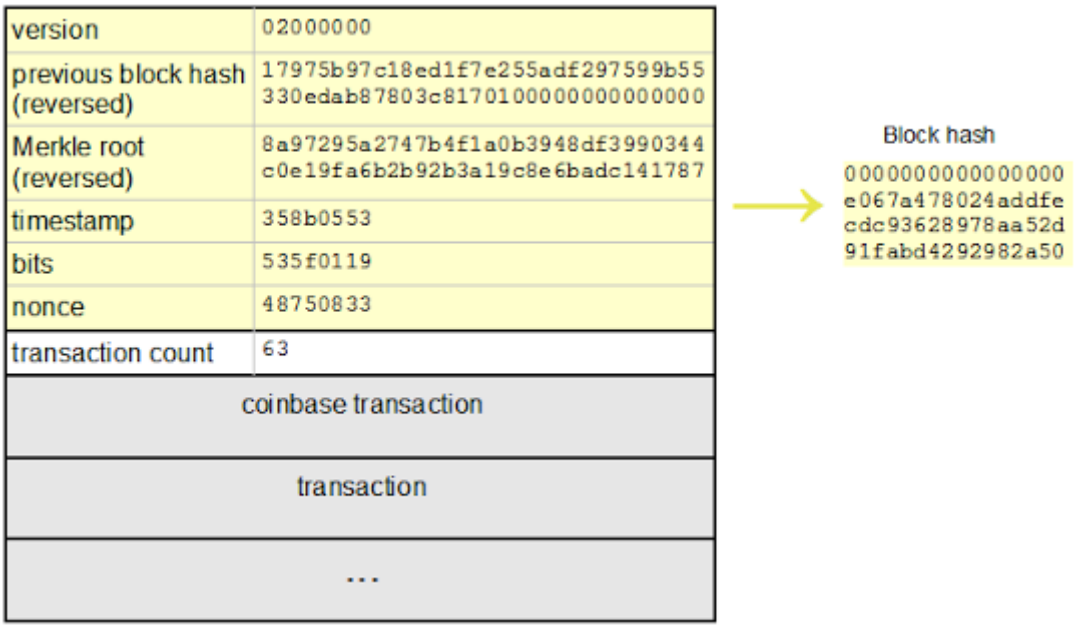
VELIČINA	NAZIV	OPIS
4 BAJTA	VELIČINA BLOKA	VELIČINA BLOKA U BAJTOVIMA
80 BAJTOVA	ZAGLAVLJE BLOKA	META-PODACI
1-9 BAJTOVA	BROJAČ ZAPISA	KOLIKO ZAPISA SADRŽI BLOK
VARIJABILNO	ZAPISI	ZAPISI POHRANJENI U BLOKU

Kako bi shvatili šta se točno dešava sa svakim pojedinim blokom, potrebno je detaljnije promotriti zaglavlje bloka (Tabela 2.1.).

Tabela 2.1 (Zaglavlje bloka)

VELIČINA	NAZIV	OPIS
4 BAJTA	VERZIJA	VERZIJA PROTOKOLA
32 BAJTA	HASH PRETHODNOG BLOKA	REFERENCA NA BLOK KOJI PRETHODI
4 BAJTA	KORIJEN BINARNOG STABLA	HASH KOJI IMA INFORMACIJE O SVIM ZAPISIMA U BLOKU
4 BAJTA	VREMENSKA OZNAKA	VRIJEME KADA JE BLOK NASTAO
4 BAJTA	TEŽINSKA OZNAKA	TEŽINA ALGORITMA ČIJE JE RIJEŠENJE POTREBNO ZA UKLJUČIVANJE BLOKA
4 BAJTA	NONCE	BROJ POMOĆU KOJEG JE RIJEŠEN ALGORITAM

U samom zaglavlju bloka susrećemo se s tehničkim informacijama o njemu samom i sa svim informacijama vezanim uz povezivanje s drugim blokovima koji su također dio blockchaina. Hash prethodnog bloka je konačni dobiveni izlazni rezultat nakon dvostruke primjene hash funkcije SHA- 256. Napomenimo kako hash samog bloka nije dio strukture bloka, on se uobičajeno računa samo kada ima potrebe za takvom akcijom, tada se izračun izvrašava na strani svakog čvora. 4 bajta koja su predviđenja za vremensku oznaku, sadržavaju informaciju o tome kada je blok dodan u lanac. Korijen binarnog hash stabla ima u sebi informaciju koju je preuzeo od svih zapisa u bloku. Težinska oznaka i nonca su meta-podaci, njihova primjena je vidljivo isključivo kod dodavanja pojedinog bloka u blockchain.



Slika 1.1. Primjer bloka

2.3. POVEZIVANJE BLOKOVA

Svaki blok u lancu možemo zamisliti kao svaku pojedinu stranicu u knjizi. Svaka stranica knjige se nalazi u nekom poglavlju i ima svoj numerirani broj na dnu stranice, pa tako i zaglavlje bloka sadrži tehničke informacije, i ima referencu na pretohdni blok. Ti podaci su svakako vrlo bitni u oba slučaja, za svaki blok u lancu ili stranicu u knjizi, trebamo znati gdje pripada i u kojem redoslijedu. Kada bi došlo do narušavanja tog redoslijeda, naprimjer uslijed nekog pokušaja napada na blockchain, vrlo lako bi pomoću referenci na prethodni blok uredili razmještaj na prvotno stanje. Korištenjem hash funkcije dobivamo i validaciju podataka. Svaki korisnik koji ima pristup podacima nekog bloka ili barem samo zaglavlju tog pojedinog bloka koristeći kriptografske funkcije, u mogućnosti je odrediti hash tog bloka. Kako je već spomenuto, blok koji nastaje kasnije u lancu, sadržava u sebi hash bloka koji je nastao neposredno prije njega. Ukoliko bi netko pokušao napraviti izmjenu u podacima odredjenog bloka, morao bi mjenjati sve hasheve od tog trenutka nadalje.

2.4. VRSTE BLOCKCHAINA

Trenutno postoje tri vrste blockchain mreže, to su javna, privatna i konzorcijska.

2.4.1. JAVNI BLOCKCHAIN

Javni blockchain nema apsolutno nikakvih ograničenja pristupa. Svatko tko ima pristup internetskoj mreži može slati transakcije pa tako može postati i validator, odnosno može sudjelovati u izvršavanju koncsenzusnog protokola. Inače, ovakva vrsta blockchaina nudi ekonomske poticaje (nagradu), za one koji osiguravaju mrežu i koriste jedan od vrsta proof-of-stake ili proof-of-work algoritam. Trenutno jedni od najpoznatijih javnih blockchainova su Bitcoin, Ethereum itd.

2.4.2. PRIVATNI BLOCKCHAIN

U ovom primjeru blockchaina susrećemo se s ograničenjima za sudionika i validatora. Svaki sudionik ovakve mreže mora biti prvotno pozvan odnosno odobren od strane administratora. Privatni blockchain možemo smatrati kao podloga koju koriste koje su zainteresirane za samu tehnologiju koju blockchain pruža, ali nisu zadovoljni s razinom kontrolne koju nudi javna mreža. Svodi se na implementaciju tehnologije za neke računovodstvene i evidencijske postupke unutar organizacije, bez ugrožavanja svoje autonomije ili mogućnosti da određeni podaci ili informacije budu izložene javnosti.

2.4.3. KONZORCIJSKI BLOCKCHAIN

Za konzorcijski blockchain se često kaže da je polu-decentraliziran. Umjesto da ga kontrolira jedna organizacija kao što smo vidjeli na primjeru privatnog blockchaina ovdje više različitih organizacija ima dozvoljen pristup lancu i svaka može kreirati čvor u takvoj mreži. Administratori takvog blockchaina ograničavaju korisnikova prava na čitanje pojedinih dijelova lanca kako oni to smatraju optimalnim, i dozvoljavaju da samo nad ograničem brojem pouzdanih čvorova izvršavaju konsenzusni protokol.

3. HASH FUNKCIJE

Argument hash funkcija su podaci proizvoljne duljine, ali rezultat je fiksne. Cijela blockchain tehnologija se zasniva na iskorištavanju svojstva hash-eva. Hash nekog bloka je vrlo lako izračunati ali je vrlo teško, odnosno nije niti moguće otkriti koji se podaci kriju u pozadini izračunatog hasha. Dovoljno je da nekoj ulaznoj informaciji ili rečenici izmjeniti samo jedno slovo, hash te informacije će izgledati u cijelosti drugačije. Kako bi dokazali prethodne tvrdnje navest ćemo nekoliko poruka i njihovu izlaznu vrijednost hash funkcije SHA-256.

3.1. SHA-256

Kriptografske hash funkcije su matematičke operacije koje se izvode nad digitalnim podacima.
SHA-256 spada u SHA-2 kriptografske funkcije čije je standarde osmislila NSA (National security agency). Broj 256 u imenu funkcije označava broj bitova, dok je SHA kratica za Secure hash Algorithm. SHA-256 može biti izgeneriran iz bilokojeg ulaznog podatka ili poruke, ali poruka ne može ne može biti izgenerirana iz hasha.

3.2. Kako radi SHA-256?

Podatak koji će ulaziti u funkciju prvo treba proširiti na način da će njegova duljina biti djeljiva s 512. Duljinu podatka (d) proširit ćemo tako da nadodajemo bit „1“ na kraj podatka. Zatim, k puta nadodajemo bit suprotne vrijednosti „0“, gdje k označava najmanje nenegativno rješenje jednadžbe koja glasi → $d+1+k = 448 \bmod 512$. Poslije ovih operacija, dodaje se 64-bitni blok koji je ujedno ranije spomenutu duljinu podatka ali u binarnom zapisu.
Kada je proširenje podatka završeno, tada će se podatak podjeliti na blokove $P^{(1)}$, $P^{(2)}$, $P^{(3)}$, $P^{(4)}$,...,$P^{(n)}$ od kojih svaki ima veličinu od 512 bitova.

Rekurzivna formula koja prikazuje rad SHA funkcije glasi:

$$H^{(i)} = H^{(i-1)} + KOM_{P(i)}(H^{(i-1)})$$

KOM → komprecijska funkcija
$H^{(i)}$ → Pojedini hash duljine 256 bita
$H^{(n)}$ → Traženi rezultat
+ → operator
$H^{(0)}$→ Vrijednost rekurzije na samom početku

Dakle, KOM, ranije spomenuta funkcija kompresije djelovat će nad 512 i 256-bitnim blokovima. Pri računanju hash vrijednosti nekog podatka ili poruke koriste se i neke pomoćne funkcije, no finalni izračun hash poruke može se prikazati na sljedeći način:

$$H_1^{(i)} \leftarrow a + H_1^{(i-1)}$$
$$H_2^{(i)} \leftarrow b + H_2^{(i-1)}$$
$$H_3^{(i)} \leftarrow c + H_3^{(i-1)}$$
$$\cdots\cdots$$
$$H_8^{(i)} \leftarrow h + H_8^{(i-1)}$$

$H^{(n)} = (H_1^{(n)}, H_2^{(n)}, H_3^{(n)},..., H_8^{(n)})$ predstavlja finalnu hashiranu vrijednost podatka.

Primjer 1.
SHA-256("Ja sam sven i student sam jednopredmetne informatike u Rijeci**")**

Vrijednost hash-a →
0d619f0ab1eea497910fa4f472cdf01f546aaa30933f9195d4f0379391978e38

SHA-256("Ja sam sven, student sam jednopredmetne informatike u Rijeci**")**

Vrijednost hash-a →
1d1fe84592cad7d301b96862a6f168c59b1560daf82e128729959d5123928600

Primjer 2.

SHA-256("hash funkcija je moćan alat**")**

Vrijednost hash-a → 18613d31ae80e30c72ccc892fb0ec78b49e90d32c875520cc0ed96afca584bcd

SHA-256("hash funkcija je moćan alaT**")**

Vrijednost hash-a → 1f7cdb911e0704d18b6a4d4cd15e852064fde377aa14520b4d44d8a1f7e5aeba

Primjer 3.

SHA-256("a**")**

Vrijednost hash-a → ca978112ca1bbdcafac231b39a23dc4da786eff8147c4e72b9807785afee48bb

SHA-256("A**")**

Vrijednost hash-a → 559aead08264d5795d3909718cdd05abd49572e84fe55590eef31a88a08fdffd

Iz prethodno navedenih primjera, vidimo kako i samo najmanja promjena u ulaznoj poruci koja se podvrgava kriptografskoj hash funkciji SHA-256, ima kompletno drugačiji izlazni rezultat.

4. BLOCKCHAIN PARTNERI

Kada govorimo o blockchainu, onda moramo znati kako se cijeli decentralizirani sustav zasniva na ideji ravnopravnih partnera. Postoje centralizirani i decentralizirani sustavi, kod centraliziranih sustava koristimo poslužitelja za povezivanje klijenata radi njihove daljnje komunikacije. Analogono tome, jasno je da decentralizirani sustav počiva na ideji da nije potreban poslužitelj već će sustav biti sačinjen od velikog broja partnera koji obavljaju određene zadatke prema potrebama korisnika. Dakle, kod decentraliziranih sustava koji koriste blockchain razmjena informacija odnosno podataka kroz neku mrežu će se vršiti direktno među korisnicima, a ne preko poslužitelja.

Postoje četiri funkcije koje partneri mogu obavljati u sustavu blockchaina, to su :

- Wallet (novčanik)
- Network routing (mrežno usmjeravanje)
- Mining (rudarenje)
- Održavanje blockchaina

Napomenimo da u privatnim (private blockchain) sustavima gdje koristimo blockchain, svaki od partnera će obavljati sve od navedenih funkcija, dok ćemo u javnim (public blockchain) prema funkcijama koje partneri obavljaju i razlikovati samu vrstu partnera. Vrste partnera su :

- Potpuni partner
- Rudar (miner)
- Novčanik
- Blockchain partner

Funkciju mrežnog usmjeravanja će obavljati svaki od navedenih partnera. Kako je i ranije rečeno, govorimo o decentraliziranom sustavu ravnopravnih partnera pa se zato i postavlja potreba za time da svaki od partnera uspostavlja vezu s ostalima u sustavu. Uz mrežno usmjeravanje, partneri će također biti zaduženi za validaciju novih zapisa u lancu. Napomenimo samo da potpuni partner može obavljati funkcije svih prethodno navedenih partnera, dok ćemo svakog od ostalih pobliže objasniti.

4.1. NOVČANIK

U javnim decentraliziranim sustavima, cijeli lanac odnosno blockchain ima ogormnu količinu podataka pa samim time svaki korisnik ne može pohraniti sve podatke, zato je i osmišljen novčanik. Korisnik koji je u sustavu predstavljen kao novčanik će imati za svoju glavnu funkciju da kreira nove zapise prema protokolu samog sustava. Da bi se potvrdila vjerodostojnost neke transakcije, informacije ili nekog drugog podatka, novčanik će pohraniti odnosno čuvati informaciju tako da pohranjuje javne i privatne kriptografske ključeve. Javni ključ koristi na način da se iz njega generira svojevrsna adresa čija je svrha primanje transakcija nekog drugog korisnika. Privatni ključ se koristi za samo pristupanje adresi i sredstvima koja se nalaze u novčaniku. Sami privatni ključevi imaju funkciju kao identifikacija, recimo kao lozinka bankovne kartice.

Novčanik također vrši validaciju novonastalih zapisa u lancu, samo on to radi na nešto drugačiji način iz razloga jer ne pohranjuje cijeli blockchain odredjenog sustava. To znači da će pohranjivat samo zaglavlja blokova a ne cijelovite zapise unutar lanca. Kako sami novčanici nemaju pregled nad cijelovitim blockchainom, tada će se pritom validacije poslužiti ostalim partnerima koji će im omogućiti uvid u traženi dio blockchaina. Novčanici rade na način da verificiraju lance blokova bez transakcija, i tek poslije toga će lanac povezati sa transakcijama. Veza koja se dešava između transakcije i jednog bloka u lancu će se uspostaviti preko puta u binarnom hash stablu. Novčanik će saznati u kojem je bloku tražena transakcija koju želi validirati, ali pritome čeka da rudari odrade svoju zadaću. Njihova je zadaća dodavanje još 6 blokova u lanac, kako bi korisnik-novčanik znao da je transakcija sigurna i da je provjerena od ostatka mreže.

4.2. BLOCKCHAIN PARTNER

Glavna funkcija blockchain partnera je ta da održava cijeli lanac sa svim zapisanim podacima u njemu krenuvši od prvog do posljednjeg bloka u blockchainu koji u tom odredjenog trenutku postoji. Ukoliko je potrebno validirati neku odredjenu transakciju ili provjeriti vjerodostojnost neke odredjene transakcije koje je zapisana u blockchain, tada blockchain partner može provjeriti jesu li sredstva koja su dio te transakcije stvarno od tog korisnika. Sam taj proces će se obaviti na jednostavan način tako da će se povezati nova transakcija sa svim onim transakcijama od te osobe do samog početka lanca, tj. do prvog bloka u blockchainu, kojeg ujedno zovemo i generički blok.

4.3. RUDAR (MINER)

Funkcija rudara je ta da prihvaća nove zapise koji su napravljeni sa strane novčanika, kreira blokove od tih zapisa i smješta ih u blockchain. Na primjeru bitcoina, način kako se upisuju novi zapisi u lanac potrebno je iskorištavanje računalnih resursa. Pod iskorištavanjem računalnih resursa, mislimo na rješavanje algoritma koji se zove proof-of-stake. Dakle, novi blokovi se dodaju u blockchain pomoću rješavanja algoritma, kada se transakcije validiraju rudar koji je obavio tu zadaću i utrošio svoje resurse na izvršenje iste, biva nagradjen s odredjenim udjelom bitcoina. U prosjeku se svakih 10 minuta kreira novi blok u lancu, što znači ako je odredjeni bitcoin poslan nekom klijentu, transakcija će biti validirana nakon u prosjeku 10 minuta.

5. ALGORITMI

Svaki se blockchain sustav zasniva na nekom algoritmu odnosno na načinu na koji se postiže konsenzus. Postoje razne vrste algoritama, prvi algoritam koji je napisan u tu svrhu je Proof-of-work pomoću kojeg se realizira konsenzus kod Bitcoina. Konsenzus je postupak donošenja odluke koji počiva na suglasnosti većine korisnika koji za funkciju imaju verifikaciju transakcija.

5.1. PoW (PROOF-OF-WORK)

PoW, ujedno i prvi algoritam za postizanje konsenzusa je osmišljen od strane Satoshija Nakamota. To je proces u kojem računala koja zovemo rudari, rješavaju komplicirane matematičke zadatke nakon čega bivaju nagrađeni nekim udjelom kriptovalute. Ono šta se po završetku izračuna dešava jest da se u blockchain dodaje novik blok i transakcije koje mu pripadaju. Proof-of-work počiva na sistemu ''najduži lanac pobjeđuje''. Kako svi rudari rudare na istom blockchainu, u trenutku kada se pokušava postaviti lažni blok uslijed nekog napada, stvara se novi lanac i odlučuje se koji je ispravan, i to je onaj duži. Znači da lanac na koji je utrošeno minimalno 51% ukupne snage računala za rudarenje se postavlja kao ispravan. U prevedenom, dok god nije 51% računalne snage u mreži u rukama jedne ili par osoba, Bitcoin i sve kriptovalute koje počivaju na tom principu se smatraju sigurnima.
Svakako, Pow ima svojih prednosti i mana kao i svi drugi algoritmi.

Prednosti:

- U proizvodnju novih sredstava ulažu se struja i računalna oprema
- Svatko može rudariti
- Povoljno za lokacije s puno neiskorištene električne energije

Nedostaci :

- Mreža postaje spora ako je koristi veliki broj korisnika
- Velika potrošnja energije
- Rudarenje je postalo isplativo samo za one s profesionalnom opremom

5.2. PoS (PROOF-OF-STAKE)

Proof of stake (dokaz ulogom) počiva na totalno drugačijoj ideji od PoW-a. Ne kreiraju se novi blokovi pomoću klijenta rudara, već se tvorac novovg bloka u lancu određuje sa svojim udjelom na računu, to nazivamo ulog. Kod stvaratelja novog bloka uzimamo dva bitna kriterija, to su koliko novaca se nalazi na računu i koliko dugo ga ima. Primjerice, uzmimo za primjer Kriptovalutu Cardano i da imamo dva korisnika od kojih Klijent K1 ima 15 000 ADA jedinica, dok K2 ima 8 000 ADA jedinica. Mnogo je veća vjerojatnost da će kao tvorac novog bloka biti izabran K1 u odnosu na K2, pogotovo u slučaju ako korisnik K1 ima vremenski duže taj iznos na računu od korisnika K2.
Za razliku od PoW-a ovdje kreator novog bloka biva nagrađen na nešto drugačiji način, u trenutku kada je neki korisnik odabran za tvorca novog bloka, provizija transakcije koju je korisnik validirao odlazi na njegov račun. PoS sustav je također visoke sigurnosti, jer ako se desi da tvorac novog bloka odnosno validator transakcija pokušava validirati lažne transakcije, on istovremeno riskira sav svoj ulog i vrijednost same kriptovalute. Kako bi neki napadač preuzeo kontrolu cijele mreže, on mora posjedovati 51% valute. Iako niti tada korisnik nema interesa u narušavanju integriteta sustava, jer samom manipulacijom valute riskira cijelu svoju vrijednost.

Prednosti:
- Brza obrada transakcija (nema potrebe za rješavanjem teških matematičkih problema)
- Nema velike potrošnje električne energije
- Nema potrebe za zahtjevnim hardverom

Nedostaci:
- Bogatiji se obogaćuju
- U slučaju udruživanja velikih grupacija dovodi se do kontroliranja i moguće manipulacije sustava

5.3. DPoS (DELEGIRANI PROOF-OF-STAKE)

Daniel Larimer, blockchain stručnjak na temelju načina kako bitcoin funkcionira i kako postiže konsenzus, shvatio je kako je ogromna količina energije utrošne na rudarenje te kako bi rudarenje moglo postati centralizirano preko velikih udruženja (mining pools), i samim time kontrolitati valutu. U želji da se izbjegne ta mogućnost razvio je sustav brzine 100 000 transakcija unutar jedne sekunde, što bitcoin nikako ne može postići. DPoS sustav funkcionira na način da cijela zajednica odnosno svi klijenti odabiru delegat u rasponu od 20-101 članova, to su računala koja će se koristiti za validaciju transakcija. Kao i kod običnog PoS-a, oni dobijaju svoju naknadu na principu provizije od transakcija. Članovi delegata se biraju glasanjem koje je stalno aktivno. Svaki korisnik koji u svojem novčaniku ima neki udjel kriptovalute ima i pravo da sudjeluje u glasanju. Važnost (''težina'') glasa je je ekvivalentna sa sredstvima u novčaniku. Dakle, što korisnik ima više udio u nekoj valuti, to će njegov glas imati veći značaj za odluku pri odabiru delegata. Članovi delegata nemogu modificirati same transakcije, ali ih mogu odbijati odnosno osporavati da budu pridodane određenom bloku.

Svaka akcija koju delegat radi je javno dostupna, pa tako bilo koje ponašanje koje je neprihvatljivo, rezultirat će time da će računalo/korisnik biti izbačen iz kruga delegata i biti zamijenjen sljedećim kandidatom.

Prednosti:
- Brza validacija i obrada transakcija
- Ukoliko nastane nepravilnost u sustavu, detektira se unutar 1-2 minute
- Nema velikog utroška energije
- Sustav je djelomično centraliziran ali počiva na viskoj razini demokracije među korisnicima

Nedostaci:
- Ukoliko se većina članova delegata udruže, mogu manipulirati mrežom
- Manji je broj ljudi koji validiraju transakcije u mreži pa je samim time lakše izvršiti 51% napad na mrežu.

6. PRIMJENA BLOCKCHAINA

Kako je i ranije spomenuto, blockchain tehnologija je nastala prvnstveno kao podloga na kojoj će se primjenjivat Bitcoin. Naravno, s godinama sve više industrija prepoznaje kvalitetu i sigurnost koju pruža sama blockchain tehnologija, pa tako su se razvile ideje implementacije blockchaina u raznim granama industrije poput industrije plaćanja (kriptovalute), nekretnina, medicina, politika i razne druge grane s kojima se svakodnevno susrećemo.

6.1. PAMETNI UGOVORI

Pametni ugovori (Smart contracts) su možda najrevolucionarnija ideja zasovana na blockchain tehnologiji. Nick Szabo je 1994. Godine, dakle i prije samog nastanka blockchain tehnologije i kriptovalta uopće, predložio koncept pametnih ugovora. Za njih kažemo da su automatski, odnosno ''samo-izvršavajući '' digitalni ugovori. Papirnati ugovori su na taj način prevedeni u programski kod i čuvaju se u okviru cijele mreže.
Napredak blockchain donosi je taj da potpuno uklanja treću stranu odnosno posrednika čak i u ugovorima između korisnika, poput klasničnih ugovora definirana su pravila i kazne ukoliko jedna strana ne ispoštuje pravila ugovora, ali automatski se provode kazne i sankcije.
Jednom kada je pametni ugovor postavljen na blockchain, svaki korisnik koji sudjeluje u mreži prihvaća pravila koja su u njemu definirana. Bitno je reći kako pravila ugovora više nisu pravno obavezujuća, već putem algoritma. Jednom kada se ugovor potpiše tj. validira od više strana, on je automatski izvršen.

Neke od bitnih karakteristika pametnog ugovora :

- POVJERLJIVOST I SIGURNOST → podaci jednom zapisani u blockchain, zauvijek su na mreži i gotovo ih je nemoguće promjeniti.

● BRZINA I CIJENA → automatsko izvršavanje transakcija i pametnih ugovora nemjerljivo je brža od današnje birokracije, eliminiranjem treće strane kao posrednika nudi ogromnu količinu uštede.
● TRANSPARENTNOST → svi ugovoreni korisnici su se usuglasili oko jasnih pravila definiranih u ugovoru te kasnije to ne mogu poricat.

6.2. KRIPTOVALUTA

Kriptovalutu treba shvatiti kao vrstu digitalne valute koja će funkcionirati na temelju kriptografskih algoritama. Neovisna je, što znači da ne postoji glavni autoritet ili neka institucija koja vrši kontrolu nad njom i upravlja ili odobrava njene transkacije. Zasniva se dakle na ideji blockchaina i potpuno je decentralizirana. Kako je objašnjeno u poglavlju ranije, nove jedinice kriptovalute (u većini slučajeva) nastaju rudarenjem. Moguće je naravno putem neke od mjenjačnica na internetu kupiti željenu kriptovalutu te kasnije njome trgovati ili kupovati druge usluge, ovisno o želji pojedinog korisnika. Uz Bitcoin koji je ranije spomenut i koji je ujedno i prva kriptovaluta, ima još mnogo interesantnih kriptovaluta od kojih ćemo spomenuti samo neke :

● Ethereum

● Ripple

● Litecoin

6.2.1. ETHEREUM

Platforma i operacijski sustav Ethereuma su otvorenog koda, zasnovani su na blockchainu te imaju funkcionalnost pametnih ugovora. Ether je kriptovaluta čiji blockchain generira platforma Ethereuma, on se može razmjenjivati između korisnika putem njihovih računa odnosno novčanika i koristiti kao kompenzacija između rudara radi izrađenih izračuna. Ethereum se još uvijek bazira na principu proof-of-worka, no najvljuje se prelazak na proof-of-stake.

6.2.2. RIPPLE

Predmet usporedbe za Ripple će nam biti Bitcoin. Analize su pokazale da bitcoinu u prosjeku treba oko 168 minuta, dakle nešto manje od 3 sata kako bi se prenio s jednog računa na drugi. Ripple za takvu transakciju između dva korisnika zahtjeva tek nešto više od 3 sekunde. Nailazimo na mnogo sličnih karakteristika kod obje valute, ali ima i nekoliko bitnih razlika

● Ripple se ne rudari, on koristi iterativni proces konsenzusa
● Nije decentraliziran

● Ripple je transakcijska mreža (koja ima svoje coine), nije digitalna valuta.

Ripple je svakako skrenuo pažnju mnogim bankama i korporacijama, jer je proizvod nastao na blockchain tehnologiji koji svakako vidi dalekosežnu primjenu što u financijskom sektoru, što u ostalima.

6.2.3. LITECOIN

Litecoin je peer-to-peer kriptovaluta i možemo ju predstaviti kao pojednostavljeni bitcoin. Prednosti je najlakše uočiti na isti način kao i ranije, usporedivši ga s Bitcoinom. Litecoin ne koristi SHA-256 algoritam za šifriranje, već koristi Scrypt. Scrypt je tip algoritma veoma sličan SHA-256 ali bitna razlika je da onemogućuje da se izračuni mogu prvoditi paralelno, već se moraju izvršavati serijski. Kada bi kod rudarenja htjeli npr. Proces A i B provoditi paralelno, potrebe za memorijom bi bile ogormne. Scrypt je po tome i dobio ime kao ''memorijski težak problem'', više nemamo onaj osnovni problem kao kod Bitcoina da je ograničenje kod rudarenja jačina procesora nego u ovom slučaju količina memorije. Paralelno pokretanje više procesa zahtjevat će uređaje s ogromnom memorijom, postaje iznimno skupo. Dolazimo do dvije bitne posljedice ovog algoritma

● Prosječan korisnik se može natjecati s korisnicima koji imaju ogromnu količinu procesora

● Proizvodnja memorije je mnogo skuplja od proizvodnje SHA-256 procesora

Scrypt je i dizajniram s ciljem ovih posljedica, jer na taj način rudarenje postaje demokratsko, i većini dostupno.

7. ZAKLJUČAK

Za blockchain tehnologiju možemo s pravom reći da je još uvijek u svojim začecima, jer njenu prvu pravu implementaciju vidimo tek 10-ak godina unazad.
Digitalne valute su svjedočile početku blockchain tehnologije, no sam potencijal je vidljiv i mnogo dalje. Samim time kako je manipulacija podacima unutar lanca onemogućena dobrom podlogom od strane tehnologije, u budućnosti bi se u školstvu i raznim drugim institucijama mogla naći ova tehnologija kao sastavni dio svakodnevice. Primjerice, kroz povijest mnogih država zna se kako je bilo poteškoća i manipulacija u procesima prebrojavanja izbornih rezultata, blockchain će u potpunosti ukloniti tu mogućnost. Također kao primjer može se uzeti kako medicinskoj industriji dijeljenje ili gubitak zdravstvenih informacija dovodi do problema i nepovjerljivosti između korisnik i pružatelja usluga, pomoću blockchaina razmjena informacija između korisnika bi bila u potpunosti sigurna i lišena svih takvih ili sličnih anomalija u sustavu. Ovo su dakle samo trivijalni primjeri u kojima spomenuta tehnologija nudi revolucionarna i trenutno optimalna rješenja, no sama budućnost blockchaina i vrijeme koje će biti potrebno da se ono implementira u razne industrijske sustave, to će biti vidljivo u narednim godinama.

8. LITERATURA

Arunović, Denis. »Što je u stvari blockchain i kako radi?« *Denis Arunović* (2018). <https://www.bug.hr/tehnologije/sto-je-u-stvari-blockchain-i-kako-radi-3011>.

Badurina, Leon. »Blockchain: Za razliku od ljudi, imun je na manipulaciju, korupciju, diktaturu….« *Leon Badurina* (2017). <https://www.netokracija.com/sto-je-blockchain-132284>.

Deželić, Vanja. »Što je blockchain, koje su njegove prednosti i mane?« (2017). <https://www.ictbusiness.info/kolumne/sto-je-blockchain-koje-su-njegove-prednosti-i-mane>.

Milinković, Nikola. »Uvod u blockchain.« *Nikola Milinković* (2017). <https://startit.rs/uvod-u-blockchain/>.

Tyle, Mohit Kaushal & Sheel. »The Blockchain: What It Is and Why It Matters.« (2015). <https://www.brookings.edu/blog/techtank/2015/01/13/the-blockchain-what-it-is-and-why-it-matters/>.

Wikipedia. n.d. <https://en.wikipedia.org/wiki/Blockchain>.

9. POPIS SLIKA I TABELA