Primjena blockchain tehnologije u poslovanju

Devunić, Tomislav

Sveučilište Jurja Dobrile u Puli
Fakultet ekonomije i turizma
„Dr. Mijo Mirković“

Tomislav Devunić

PRIMJENA BLOCKCHAIN TEHNOLOGIJE U POSLOVANJU

Završni rad

Pula, 2020.

Sveučilište Jurja Dobrile u Puli
Fakultet ekonomije i turizma
„Dr. Mijo Mirković“

PRIMJENA BLOCKCHAIN TEHNOLOGIJE U POSLOVANJU

Završni rad

Tomislav Devunić
JMBAG: 0303059806, redovan student
Studijski smjer: Informatički menadžment

Kolegij: Elektroničko poslovanje
Mentor: prof. dr. sc. Vanja Bevanda

Pula, rujan 2020.

IZJAVA O AKADEMSKOJ ČESTITOSTI

Ja, dolje potpisani Tomislav Devunić, kandidat za prvostupnika poslovne ekonomije ovime izjavljujem da je ovaj Završni rad rezultat isključivo mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na objavljenu literaturu kao što to pokazuju korištene bilješke i bibliografija. Izjavljujem da niti jedan dio Završnog rada nije napisan na nedozvoljen način, odnosno da je prepisan iz kojega necitiranog rada, te da ikoji dio rada krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za koji drugi rad pri bilo kojoj drugoj visokoškolskoj, znanstvenoj ili radnoj ustanovi.

Student

_____

U Puli, 21. rujna, 2020. godine

IZJAVA

o korištenju autorskog djela

Ja, Tomislav Devunić dajem odobrenje Sveučilištu Jurja Dobrile u Puli, kao nositelju prava iskorištavanja, da moj završni rad pod nazivom Primjena blockchain tehnologije u poslovanju koristi na način da gore navedeno autorsko djelo, kao cjeloviti tekst trajno objavi u javnoj internetskoj bazi Sveučilišne knjižnice Sveučilišta Jurja Dobrile u Puli te kopira u javnu internetsku bazu završnih radova Nacionalne i sveučilišne knjižnice (stavljanje na raspolaganje javnosti), sve u skladu s Zakonom o autorskom pravu i drugim srodnim pravima i dobrom akademskom praksom, a radi promicanja otvorenoga, slobodnoga pristupa znanstvenim informacijama.

Za korištenje autorskog djela na gore navedeni način ne potražujem naknadu.

U Puli, 21.9.2020.

Potpis

_____

Sadržaj

1. Uvod 1
2. Blockchain tehnologija 2
2.1 Struktura blockchaina 2
2.2 Povezivanje blokova 3
2.3 Novčanik 4
3. Vrste blockchaina 6
3.1 Javni blockchain 6
3.2 Privatni blockchain 7
3.3 Konzorcijski blockchain 7
4. Kriptografija u blockchain tehnologiji 9
4.1 HASH funkcije 10
4.2 Što radi SHA-256? 10
4.3 Primjer SHA-256 kriptiranja 10
5. Vrste konsenzusa 12
5.1 Proof-of-Work 12
5.2 Proof-of-Stake 13
5.3 Delegrirani Proof-of-Stake 14
5.4 Proof-of-Capacity 14
6. Primjena blockchain tehnologije u svakodnevnom poslovanju 16
6.1 Primjena u financijskom sektoru 17
6.2 Pametni ugovori 17
6.3.1 Moguće primjene pametnih ugovora 19
6.3 Distribuirana pohrana podataka u oblaku 20
6.3.1 Blockchain zasnovan na oblaku 21
6.3.2 Prednosti distribuirane pohrane podataka u oblaku 21

6.4 Autentikacija digitalnog identiteta 22
6.5 Primjena u medicini 24
7. Big Data i blockchain tehnologija 25
8. Problemi koji prate uvođenje blockchain tehnologije 27
9. Zaključak 30
Sažetak 31
Summary 32
Literatura 33
Popis slika 34

1. Uvod

U ovom završnom radu objasniti ću blockchain tehnologiju te njezinu primjenu u svakodnevnom poslovanju. Kako je blockchain tehnologija nastala za potrebe Bitcoina, njezine primjene su nadišle početnu ideju te se njenim razvojem počele primjenjivati na druga područja. Kako se blockchain temelji na sigurnosti i anonimnosti gotovo uvijek se njegova primjena povezuje sa ilegalnim aktivnostima.

Kako bismo bolje razumjeli primjenu blockchain tehnologije, u ovom radu također sam se posvetio strukturi, vrstama i kriptografiji. Važna stavka za potpuno razumijevanje su algoritmi za postizanje konsenzusa od kojih su najpoznatiji proof-of-work i proof-of-stake algoritmi. Kod kriptiranja podataka koristi se SHA-256 način kriptiranja.

Također naglasak je stavljen na pametne ugovore kojima je ideja uklanjanje posrednika iz transakcija, samim time se smanjuju troškovi.

Struktura rada je sastavljena od 8 poglavlja. Osim uvoda i zaključka kao prvom i posljednjem poglavlju, govorimo o strukturi blockchaina i načinu povezivanja blokova u drugom poglavlju.. Treće poglavlje govori o vrstama blockchaina s obzirom na vlasništvo. Četvrto poglavlje govori o kriptografiji u blockchainu, objašnjenju hash funkcija te primjeru SHA 256 kriptiranja. Peto poglavlje objašnjava vrste konsenzusa dok šesto govori o mogućim primjenama blockchain tehnologije u svakodnevnom poslovanju. Naposlijetku u sedmom poglavlju su obrađeni problemi na koje se nailazi prilikom i tijekom implementacije.

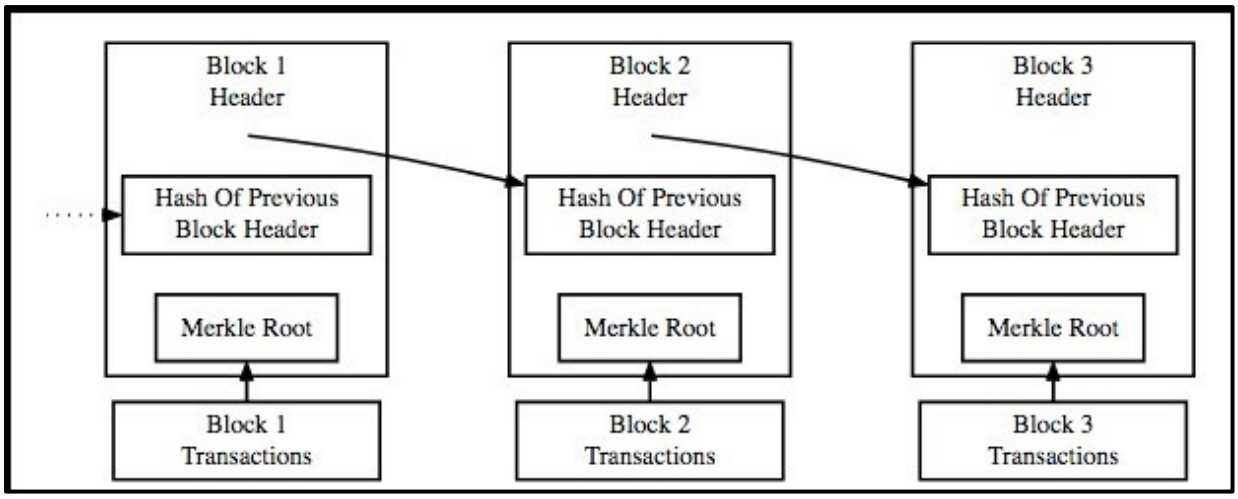
2. Blockchain tehnologija

Termin blockchain u doslovnom prijevodu na hrvatski znači lanac blokova. Kao što naziv kaže riječ je o blokovima podataka koji su povezani u jednosmjerni lanac gdje svaka nova karika (blok) zavisi o vrijednosti karike prije njega u nizu. Blockchain stavlja imperativ na sigurnost, kao općepoznato je da se u informatici sigurnost povezujemo s kriptografijom.

Iako prvi znanstveni radovi na temu kriptografski povezanih blokova podataka pojavljuju se još početkom 90-ih godina, blockchain kakav danas poznajemo opisan je i definiran 2008. godine. Kreator pod pseudonimom Satoshi Nakamoto podigao je web stranicu bitcoin.org te na njoj objavio rad na temu „Bitcoin: A Peer-to-Peer Electronic Cash System“. Rad se ubrzo proširio te izazvao velik interes.

2.1 Struktura blockchaina

Blok sadrži informacije kao zaglavlje bloka i transakcije. Blokovi su strukture podataka čija je svrha spajanje skupova transakcija i repliciraju se na sve čvorove u mreži. Blokove u blockchainu stvaraju rudari (engl. Miners). Iskopavanje (engl. Mining) je postupak stvaranja valjanog bloka koji će biti prihvaćen od ostatka mreže. Čvorovi uzimaju transakcije na čekanju, provjeravaju kriptografsku točnost i pakiraju ih u blokove koji će se pohraniti u blockchain.



Slika 1. Struktura blockchaina izvor: https://revistadigital.inesem.es/informatica-y-tics/blockchain/ (Datum pristupanja: 18.9.2020.)

Na slici 1. vidljivo je kako je u bloku svake transakcije hash funkcija povezana preko pokazivača sa hash funkcijom iz prethodnog bloka. Blok još sadrži zaglavlje i *Merkle root*[1] .

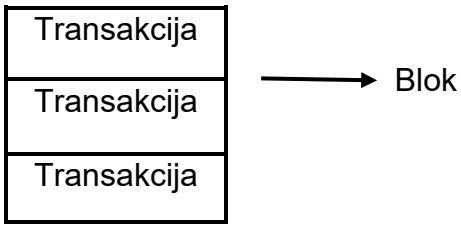
Zaglavlje bloka sadrži metapodatke koji pomažu u provjeri valjanosti bloka.
Metapodaci uključuju:

- Vremensku oznaku
- hash prethodnog bloka
- Nonce[2]
- Verzija bloka - Opisuje strukturu podataka unutar bloka

2.2 Povezivanje blokova

Struktura blockchaina povezana je preko tzv. back-linked[3] transakcija više blokova. Iz tog razloga, svaki blok sadrži hash, koji je stvoren uz pomoć SHA-256 kriptografskog algoritma hash funkcija. Svaki blok prisutan na blockchainu odnosi se na neposredno prethodni blok, koji se ponekad naziva i nadređeni blok.

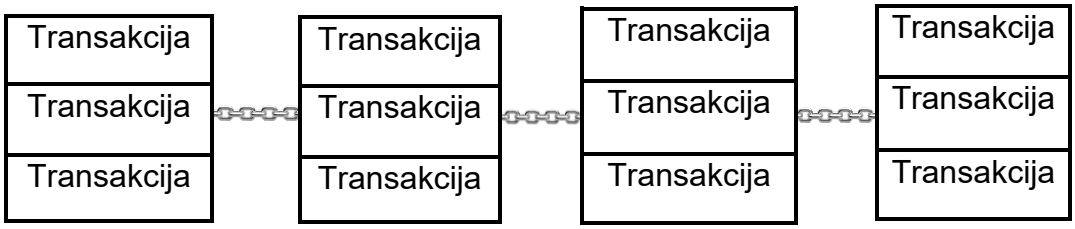
Kod upotrebe SHA-256 kriptografskog algoritma ispostavlja se da rezultat od 32 bajta ne možemo preokrenuti, jer je funkcija jednosmjerna.



Slika 2. Transakcije grupirane u blok, vlastita izrada

Transakcije su grupirane u blokove tako da se mogu učinkovito provjeriti i zatim sinkronizirati s ostalim računalima na mreži. Nakon provjere bloka dodaju se posljednjem bloku u blockchain, kao što je prikazano na slici 3.

[1] Merkle root se koristi kod kriptovaluta kako bi se osiguralo da su blokovi podataka koji se prosljeđuju između peer-ova na peer-to-peer mreži cjeloviti, neoštećeni i nepromijenjeni
[2] Nonce ili "broj koji se koristi samo jednom" odnosi se na prvi broj koji rudar blockchaina treba otkriti prije rješavanja bloka u blockchainu
[3] Back-linked označava pojam kada se svaki sljedeći blok u lancu odnosi na onaj prethodni



Slika 3. Povezivanje blokova radi formiranja blockchaina, vlastita izrada

„Kada netko pošalje primjerice bitcoin s jedne adrese na drugu adresu, transakcija je vremenski obilježena i zabilježena kod svakog sudionika sustava. Nitko ne može prevariti sustav i poslati nešto što nema u vlasništvu, jer je stanje računa javno, sinkronizirano s ostalim sudionicima sustava i evidencijom transakcija, a pravila su definirana na početku i implementirana kroz programski kod. Na ovaj način, Satoshi Nakamoto je prvi dokazao da problem dvostruke potrošnje (eng. double spending problem) može biti riješen bez treće strane, odnosno posrednika kojem obje strane vjeruju. Nakon što se transakcija odobri, posebni čvorovi šalju podatke po cijeloj mreži o transakciji i svaki server transakciju zapisuje kod sebe.“[4]

2.3 Novčanik

Blockchain novčanik (engl. Wallet) digitalni je novčanik koji korisnicima omogućuje pohranu i upravljanje njihovom digitalnom valutom te omogućuje transakcije u kriptovalutama i mogućnost njihovog ponovnog pretvaranja u fiat[5] valutu.

U novčanik se zapisuju sve transakcije. Kriptografija kod svake transakcije koristi asimetričnu kriptografiju te se za to koriste dvije vrste ključa: **Javni i privatni ključ**

Vrijednosti ovih ključeva nisu jednake. Javni ključ u pravilu možemo davati bilo kome odnosno može se poistovjetiti sa IBAN brojem koji imam u banci, dok privatni ključ trebamo držati na sigurnom mjestu te se on poistovjećuje s PIN-om. Kada nam netko želi poslati digitalni novac na naš račun, on će potpisati tu transakciju našim javnim ključem. Novac će sjesti baš na naš račun jer je privatni ključ zapisan unutar novčanika, Isključivo osoba koja ima pristup privatnom ključu može potvrditi javni. Kada se oni potvrde, transakcija se zapisuje u blockchain, a novac se dodjeljuje nama.

[4] Analiza tehnologije Blockchain, Pejčić Lovro, 2018, str 2. Datum pristupanja (7.9.2020)
[5] Fiat valuta je općeprihvaćeno sredstvo plaćanja (euro, američki dolar itd.)

„Binarno hash stablo omogućuje novčanicima provjeru kojem bloku u blockchainu pripada određena transakcija. S obzirom da novčanik poznaje sadržaj transakcije vrlo lako može saznati i hashiranu vrijednost te transakcije, koju onda predaje binarnom hash stablu. Vrste novčanika:

- Desktop novčanik
- Novčanik za mobilne uređaje
- Hardware novčanik
- Novčanik u oblaku

1) Desktop novčanik je novčanik instaliran na naše računalo ili laptop. Ova vrsta novčanika je sigurnija od novčanika u oblaku. Potrebno je imati dobar antivirusni program, te je potrebno ponekad povezati se na internet kako bi se ažurirali podaci o transakcijama u blockchainu.

2) Novčanik za mobilne uređaje je lagana verzija novčanika pogodna za instaliranje na mobilni uređaj ili tablet. Također važno je na uređaju imati dobru zaštitu kako bi se zaštitili od krađe digitalnog novca sa našeg novčanika.

3) Hardware novčanik je najsigurniji novčanik. Novčanik nije potrebno povezivati na Internet, a bez obzira na to on i dalje može potpisivati transakcije.

4) Novčanik u oblaku pruža najjednostavniju, ali i najrizičniju mogućnost korištenja novčanika. Za kreiranje je dovoljna email adresa i lozinka. Činjenica da je novčanik u oblaku i da je internetska veza konstantno u upotrebi dovela je do velikog broja lažnih internetskih stranica sa jako sličnim sučeljem, gdje naivni korisnik unosi svoju email adresu i lozinku misleći da je na pravoj stranici, te nakon toga ostaje bez svega što je posjedovao u svom novčaniku. Postoje razni načini kako se osigurati od prijevare i gubitka digitalno novca. Neki od novčanika nude mogućnost odabira 12 riječi koje će kasnije služiti kao mogućnost dohvaćanja zaboravljene lozinke, postavljanje podsjetnika za lozinku (engl. Password hint), prevencija od neautoriziranog pristupa novčaniku kreiranjem dva-faktora autorizacije (engl. Two-factor authentication) koja omogućuje spremanje broja mobilnog uređaja, na koji onda 12 dobivamo jednokratnu lozinku za pristup. Najbitnije je sačuvati privatni ključ jer u slučaju gubitka ili krađe istoga, ostajemo bez svega.“[6]

[6] Škegro Andrej, Primjena blockchain tehnologije u prehrambenoj industriji, Zagreb, 2019. str.10-11

3. Vrste blockchaina

Kako su se razvile različite potrebe korisnika tako su se razvile različite vrste blockchain tehnologije. U početku su bile dvije najpoznatije i najraširenije vrste, javni i privatni blockchain. Uz navedene dvije vrste, razvio se i konzorcijski[7] blockchain. U nastavku ću svaki pojedino objasniti.

3.1 Javni blockchain

Javni blockchain je otvorena mreža gdje se svatko može pridružiti podacima i pristupiti im, a bilo tko može slati transakcije u javni blockchain i sudjelovati u procesu provjere valjanosti transakcija. Za primjer se može uzeti javna cesta koju svako može koristiti bez obzira da li je vozač automobila, biciklista ili pješak.

Javni blockchain osiguran je kriptoekonomikom, što je kombinacija ekonomskih poticaja i kriptografske provjere koji koriste mehanizme poput „Proof of Work“ ili „Proof of stake“, slijedeći opće načelo da stupanj do kojeg netko može imati utjecaja u proces konsenzusa proporcionalan je količini ekonomskih resursa koje mogu donijeti. Ova vrsta blockchaina obično smatra "potpuno decentraliziranom."

Prednosti javnih blockchaina dolaze iz otvorenosti i decentralizacije protokola:

- Ne postoji središnje tijelo, što javni blockchain čini dobrom opcijom za suradnju neovisnih poslovnih partnera.
- Transparentnost - svi podaci o javnim blockchainima su javni (iako je uobičajeno sakriti identitet sudionika), što pruža mogućnost oduprijeti se hakiranju ili kontroli kapitala iz opresivnih režima[8].
- Otvorenost - budući da su javni blockchaini otvoreni, vjerojatno će ih koristiti veliki broj subjekata.
- Mrežni učinak - vjerojatno će ljudi početi koristiti nove javne blockchain aplikacije jer koriste drugi softver temeljen na istom blockchainu, koji proširuje korisničku bazu ovog blockchaina.

Nažalost, trošak nije uvijek vrijedan koristi. Jedan od nedostataka javnih blokova je velika količina računalne snage koja je potrebna za verificiranje transakcija.

[7] tzv. Decentralizirani blockchain

[8]' tlačni režim (engl. oppressive regime), odnosi se na države u kojima postoje "zakoni i običaji“. ili prakse koje sustavno proizvode nejednakosti; koje tlače određene grupe unutar društva

Primjeri javnih blockchaina uključuju Bitcoin, Ethereum, Dash, Monero, Stellar, Neo i dr. Broj slučajeva korištenja javnih blockchain-ova brzo raste. Osim za prijenos novca, oni se mogu koristiti i za:

- Pohranjivanje hasheva dokumenta ili čitave dokumente.
- Spremanje glavnih knjiga poslovanja koje bi trebale biti javne, odgovorne i transparentne.
- Kodificiranje[9] ugovora između stranaka.
- Stvaranje digitalnih sredstava i prijenos istih između subjekata na mreži
- U logistici za dokazivanje porijekla robe.

Poduzeća također mogu koristiti blockchain poput Bitcoina ili Dash-a kako bi svojim klijentima omogućili prihvaćanje plaćanja u tokenima (npr. Plaćanje u Bitcoin-u). To omogućava brze i jednostavne prekogranične transakcije i praćenje svih transakcija radi veće sigurnosti od mogućih prijevara.

3.2 Privatni blockchain

Privatna blockchain mreža zahtijeva pozivnicu i mora je potvrditi osnivač mreže ili skup pravila koja je uspostavio osnivač mreže. Jednom kada se subjekt pridruži mreži, on će igrati ulogu u održavanju blockchaina na decentralizirani način. Kod privatnog blockchaina pojedinačna organizacija ili vlast imaju kontrolu nad mrežom. Ovaj tip blockchaina odgovarao bi organizacijama jer čitanje i zapisivanje podataka nije dozvoljeno bez dopuštenja.

Po dizajnu, blockchain je decentralizirana tehnologija, ali u slučaju privatnog blockchaina ona je centralizirana. Svaki blok obično sadrži hash, vremensku oznaku kao i podatke o transakcijama, što je u pravilu isto kao i kod javnog blockchaina.

Privatni blockchain je suprotnost javnom blockchainu. Mnoge funkcije koje su dozvoljene svima u javnom blockchainu nisu dozvoljene u privatnom blockchainu.

3.3 Konzorcijski blockchain

Konzorcijski blockchain je vrsta blockchain tehnologije u kojoj nekoliko organizacija upravlja platformom, umjesto da to radi jedna organizacija. Dakle, sama po sebi nije

[9] (engl. to codify) organizirati nešto, poput zakona ili pravila, u neki sustav

javna platforma. Entiteti mogu ostvariti članstvo u mreži samo glasovanjem ili prethodnim odobrenjem.

Kod konzorcijskog blockchaina svaki od sudionika ima jednaku važnost. Organizacije su postavile takav sustav da ubrzaju konsenzus među njima. Konzorcijski blockchain prikladan je za grupe koje nisu velike. U takvim skupinama nema problema s prepoznavanjem sudionika.

Konzorcijski blockchain sa sobom donosi neke prednosti pred javnim blockchainom. Neki od njih su:

- Veća brzina - budući da je broj korisnika ograničen, oni mogu brže i s manje napora postići konsenzus.
- Privatnost - Podaci u domeni ostaju unutar korisnika. Budući da nije javno objavljeno, osigurana je privatnost podataka.
- Veći izlaz - Budući da korisnici postižu konsenzus u mnogo kraćem vremenu, mogu obrađivati više transakcija po jedinici vremena, povećavajući na taj način učinak.

4. Kriptografija u blockchain tehnologiji

Kriptografija je metoda korištenja naprednih matematičkih principa za pohranu i prijenos podataka u određenom obliku tako da ih mogu čitati i obrađivati samo oni kojima je namijenjen. Kriptografiju ljudi koriste tisućama i tisućama godina za prenošenje poruka bez otkrivanja. U stvari, najranije korištenje kriptografije uočeno je u grobu preuzetom iz Starog kraljevstva u Egiptu, oko 1900. godine prije Krista.[10]

U originalnoj verziji Blockchaina koristi se kriptografski hash poznat pod nazivom SHA-256. Siguran je, ali toliko neefikasan da je stvoren specijalizirani hardver, koji se naziva mining rings[11], posebno za obavljanje poslova obrade transakcija.

Svaki riješeni hash predstavlja jedan blok - snop obrađenih transakcija koje mogu biti prenesene na sve važeće čvorove. Kriptografske informacije o svakom bloku zapisa temelje se na podacima povezanim s posljednjim blokom i sadrže jedinstvenu vremensku oznaku, zbog čega vizualizacije blockchaina izgledaju kao poveznice u lancu.

U stvari, pojam "blockchain" polazi od ideje da je lanac blokova kriptografski osiguran. Ovaj lanac blokova olakšava otkrivanje pokušaja lažnog dodavanja zapisa u lanac. U slučaju da dođe do situacije da netko odabere poveznice u sredini lanca i počinje dodavati svoje veze na postojeću vezu, lanac bi se počeo račvati. Takva situacija se dogodila 2013. prilikom neispravnog ažuriranja te su Bitcoin razvojni programeri istu uočili i ispravili što dovodi do toga da je lančano povezivanje blokova sigurno iz razloga jer netko tko želi lažno urediti postojeći zapis u lancu odmah bude prepoznat i „skinut“ s lanca.

Ovo može postati uobičajena taktika sa svakim koji želi lažno izmijeniti ugovor, djelo ili vlasništvo. Ako pokušaju razbiti lanac te u istom nisu razotkriveni, blockchain ne bi mogao sloviti kao siguran.

[10] What is Cryptocurrencies Cryptography? (2017.) Dostupno na www.blockgeeks.com/guides/cryptocurrencies-cryptography (datum pristupanja: 26.6.2020)

[11] Mining rings - računala posebno dizajnirana za verifikaciju transakcija u blockchain kriptovalutama poput Etheriuma ili Bitcoina. Takva računala su najčešće nekoliko umreženih procesora (CPU) ili grafičkih kartica (GPU)

4.1 HASH funkcije

Hash funkcije dobivaju svoju kriptografsku snagu ne od nemogućnosti invertiranja, već od problema na koji kod koji invertira hash traje vrlo dugo vremena da bi odgovor - recimo milijun godina. Hash funkcije nije nemoguće invertirati, već je vrlo nepraktično za izvesti.

„Prvi hash se izračunava za prvi blok (eng. Genesis block) pomoću transakcija unutar tog bloka. Za svaki novi blok koji se generira, koriste se hashevi prethodnog bloka i transakcije toga bloka kao ulaz.“[12]

„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 izmijeniti samo jedno slovo, hash te informacije će izgledati u cijelosti drugačije.“ [13]

4.2 Što radi SHA-256?

SHA-256 član je SHA-2 kriptografskih hash funkcija koje je osmislio NSA. SHA označava Secure Hash Algorithm, broj 256 označava broj bitova Kriptografske hash funkcije ustvari su matematičke operacije koje se izvode nad digitalnim podacima. Usporedbom izračunatog "hash-a" (izlaz iz izvedbe algoritma) s poznatom i očekivanom hash vrijednošću, osoba može odrediti integritet podataka. Jednosmjerni hash može se generirati iz bilo kojeg dijela podataka, ali podaci se ne mogu generirati iz hash-a.

4.3 Primjer SHA-256 kriptiranja

Pogledajmo kako izgleda ulazni i odgovarajući izlazni sažetak hash funkcije. Budući da je SHA-256 poželjna hash funkcija mnogih blockchaina, prikazat ćemo kako to izgleda u praksi.

---

[12] Pejčić, Lovro, Analiza tehnologije Blockchain, Osijek 2018. str.12 (Dostupno na: https://zir.nsk.hr/islandora/object/etfos%3A1978/datastream/PDF/view) Datum pristupanja: 18.9.2020.

[13] Živković S. (2018) Blockchain tehnologija, Rijeka: Odjel za informatiku. Dostupno na: https://zir.nsk.hr/islandora/object/infri:289/preview (Datum pristupanja: 1.7.2020.)

Ovo je naš prvi primjer unosa:

Kriptografija je sastavni dio blockchaina

Kada se provede kroz SHA-256 hash funkciju, ova rečenica stvara sljedeći izlaz:

6a942976ca41fbda85676209061892bde79a27f8f0bfc0f9a03967f06d9db892

Možemo vidjeti da je izlaz kombinacija slova i brojeva od točno 64 znaka. Ali, osim toga, ne možete puno toga zaključiti gledajući ovaj sažetak. Ne postoje obrasci ili tragovi o tome kakav je bio unos.
Ukoliko se napravi čak i najmanja promjena na ulazu, kao u nastavku:

Kriptografija je sastavni dio Blockchaina

Primijetite da smo promijenili slovo "b" u riječi blockchain u "B" te smo na izlazu dobili potpuno drugačiji rezultat:

85487b0268ced3b5ec139be2e89f3b4cfe20803619f96a70536f070897b7833e

Možete vidjeti da je to radikalno drugačiji rezultat od prvog rezultata. Iako su ulazi gotovo identični, promjena jednog znaka stvorila je potpuno drugačiji izlaz.
Potrebno je naglasiti da se doslovno svaki ulaz može staviti u SHA-256 hash funkciju. Bez obzira na duljinu ulaza, izlaz će uvijek biti iste fiksne duljine i uvijek će se činiti potpuno slučajnim.[14]

[14] SHA-256 kalkulator koji sam koristio za „hashiranje“ dostupan je na https://xorbin.com/tools/sha256-hash-calculator (Datum pristupanja: 3.7.2020.)

5. Vrste konsenzusa

Konsenzus se može još nazvati i sporazumnom jednoglasnom odlukom. Odluka se donosi na temelju najveće moguće suglasnosti unutar skupine. U slučaju kriptovaluta, konsenzus se odnosi na način verifikacije transakcija te na taj način se raspoznaje ispravne od malicioznih transakcija. Najčešće korištena metoda je *Proof-of-Work* ili dokaz radom, a odnosi se na rudarenje. Novija metoda je *Proof-of-Stake* ili dokaz ulogom.

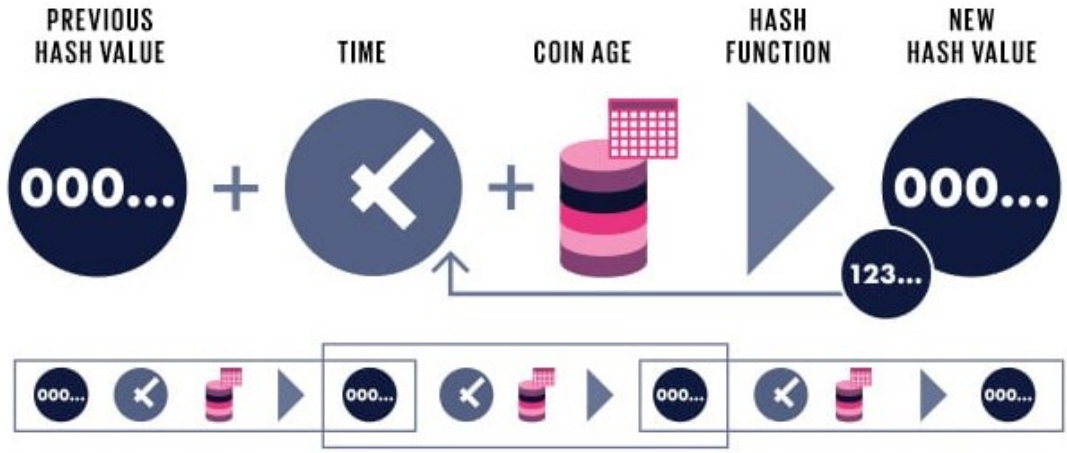
5.1 Proof-of-Work

Za kriptovalute, kao što su Bitcoin, Ethereum, Litecoin, Dogecoin, koristi se upravo metoda *proof of work*. Prednosti ove metode su da se u samu proizvodnju novog novca u cirkulaciji ulaže se vanjski faktor - struja i hardverska oprema. Bilo tko može rudariti kriptovalute temeljene na tom algoritmu konsenzusa te je ta metoda poželjna za situacije gdje ima puno neiskorištene električne energije s obzirom da cijena električne energije ulazi u konačnu kalkulaciju isplativosti. S druge strane postoje i nedostaci kao što je spora mreža kada je koristi velik broj korisnika. Rudarenje je isplativo samo uz korištenje profesionalne opreme i specijaliziranih grafičkih kartica čija cijena povećava vrijeme kada će se investicija u opremu isplatiti. Na kraju velika potrošnja energije je ekološki neprihvatljiva metoda. Poskupljenje struje može narušiti postojanje kriptovalute.

Ovu metodu je razvio tvorac Bitcoina, Satoshi Nakamoto koji je ovaj proces osmislio radi rješavanja složenih matematičkih problema pomoću računala kojega koriste rudari. Za rješavanje problema, rudari su nagrađeni kriptovalutama. Profit od rudarenja, računaju kada od dobivene vrijednosti oduzmu utrošak struje i opreme. Osim dobivenih kriptovaluta, rudar u svoj blockchain dodaje novi blok. Radi povećanja rudarenja, sve više se napušta ova metoda jer dolazi do iznimne potrošnje električne energije, što je ekološki neprihvatljivo, te se prelazi na metodu *proof-of-stake*.

5.2 Proof-of-Stake

Ova metoda se u mnogočemu razlikuje od prethodne metode. Blokovi se utvrđuju na temelju udjela novca na računu, odnosno ulogom, za razliku od metode Proof-of-Work, kada se izrada blokova temeljila na radu računala. Kriptovalute koje koriste ovu metodu su Cardano, Peercoin, QTUM, OmiseGo a i može se dodati Ethereum. Prednosti ove metode su brža obrada transakcija te veća skalabilnost[15], ekološki je prihvatljiva zbog male potrošnje električne energije i ne zahtijeva posebnu opremu.
U ovoj metodi tvorac blokova se određuje na temelju dva parametra. Prvi parametar je novac koji korisnik ima na računu a drugi na temelju vremena koliko korisnik ima taj novac na računu. Na sljedećoj slici prikazan je slijed određivanja tvorca blokova.



Slika 4. Prikaz određivanja tvorca blokova
Izvor: https://www.kriptovaluta.hr/tutorials/sto-je-konsenzus-i-koje-sve-vrste-postoje/, dostupno: 02.09.2020
Kod ove metode svaka transakcija ima proviziju, a kada tvorac blokova, odobri transakciju, provizija odlazi na njegov račun. Ova metoda je vrlo sigurna odnosno kada tvorac blokova pokuša potvrditi takozvanu lažnu transakciju, riskira sav svoj ulog.

[15] Skalabilnost – broj obrađenih transakcija u sekundi

5.3 Delegrirani Proof-of-Stake

Treća metoda je delegrirani Proof-of-Stake. Koristi se za kriptovalute kao što su BitShares, ICON, EOS, Tron, ARK i mnogi drugi. Ovu metodu definira brza obrada transakcija, podnosi veliko opterećenje mreže, svaka nepravilnost u mreži se detektira se u vrlo kratkom vremenu, svi korisnici mreže sudjeluju u odlučivanju tko će postati delegat. Sustav je djelomično centraliziran ali uz veliku prisutnost demokracije i također je ekološki prihvatljiv.

Dva su osnovna nedostatka kod ove metode. Prvi se odnosi na udruživanje delegata u grupacije radi manipulacije, a drugi nedostatak je u lakšem ostvarivanju 51% napada na mrežu. Tvorac ove metode je Daniel Larimer, blockchain inženjer koji je shvatio da Bitcoin troši veliku količinu električne energije i da nije ekološki prihvatljiv te da će u budućnosti doći do centralizacije Bitcoina. Kod ove metode, delegati su plaćeni na temelju provizije za svoj rad a izabrani su od strane zajednice. Pravo glasa kod odabira delegata imaju svi korisnici koji imaju udio u kriptovaluti, a vrijednost glasa se temelji na količini kriptovaluta odnosno ne računa se svaki glas isto.

5.4 Proof-of-Capacity

Sljedeća metoda je *Proof-of-Capacity* ili dokaz kapacitetetom. Ova metoda se odnosi na Burstcoin, SpaceMint. Karakterizira je:

- Korištenje tvrdog diska za rudarenje, što je višestruko energetski učinkovitije od specijaliziranih ASIC procesora
- ne zahtjeva dodatnu opremu,
- veća stopa decentralizacije u odnosu na PoW sustave,
- oprema se ne treba kontinuirano nadograđivati odnosno stariji tvrdi diskovi su također aktualni za ovaj princip rudarenja,

Ukoliko korisnik odustane od rudarenja, može obrisati podatke i dalje koristiti te tvrdi disk u druge svrhe.

S obzirom da je proof-of-capacity relativno nov algoritam konsenzusa sa malim udjelom korisnika, sigurnost sustava i dalje nije u potpunosti testirana te se može

lako razviti malware[16] koji bi koristio prostor na disku korisnika za rudarenje, bez znanja korisnika.

Metoda korist slobodan prostor na hard disku korisnika, zahtijeva od korisnika da odabere količinu slobodnog prostora za rudarenje.

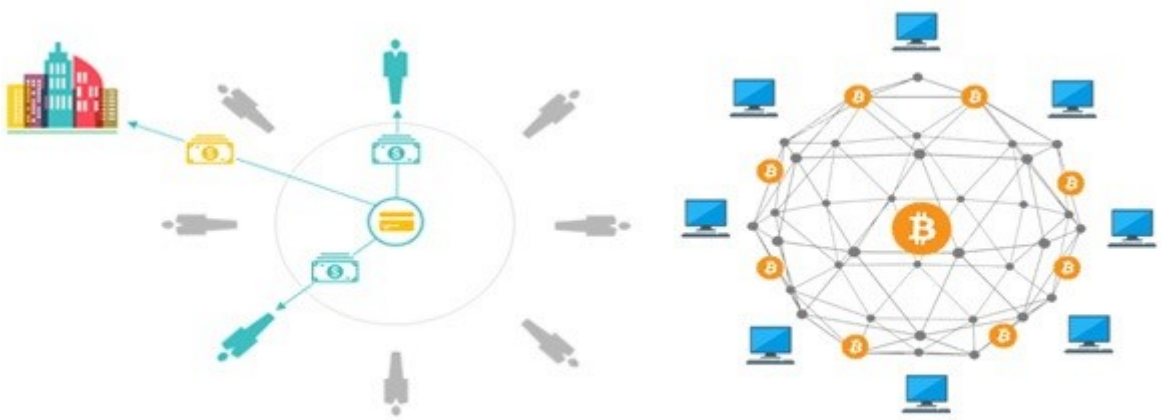
[16] Malware – zlonamjeran softver

6. Primjena blockchain tehnologije u svakodnevnom poslovanju

Svakodnevnim povećanjem broja korisnika na globalnoj razini, blockchain je na rubu da iz temelja promjeni bankarsko poslovanje, ali i poslovanje u drugim industrijama. S obzirom da se blockchain još uvijek uvelike izjednačava sa Bitcoinom odnosno kriptovalutama, treba znati da se ono samo „tehnologija“ koja omogućava da kriptovalute uopće funkcioniraju.

Iako se način poslovanja u financijskom sektoru koji prakticira blockchain tehnologija uvelike razlikuje od poslovanja koji prakticira trenutno bankarsko poslovanje. Iako su male šanse da će blockchain tehnologija u potpunosti zamijeniti trenutni bankarski sustav, barem nije izgledno da se to dogodi u bližoj budućnosti, banke bi imale velike koristi od implementacije iste.

Kod blockchain tehnologije naglasak je na neovisnosti i sigurnosti samog sustava te se transakcije upisuju trajno i bez mogućnosti naknadne izmjene.



Slika 5. Razlika između tradicionalnog bankarskog sustava i blockchain mreže

Izvor: http://www.7wdata.be/data-analysis/introduction-to-blockchain-and-what-it-means-for-big-dana Datum pristupanja: 15.9.2020

Na slici je vidljivo kako tradicionalni bankarski sektor zahtjeva treću stranu kao posrednika prilikom izvršavanja transakcije što u nekim slučajevima uzrokuje veće provizije (inozemno plaćanje, između različitih banaka i institucija). Dok s druge strane blockchain mreža (peer-to-peer) omogućuje direktno plaćanje između dva subjekta.

6.1 Primjena u financijskom sektoru

„Virtualne valute ili kripto valute (engl. Cryptocurrency) su digitalni ekvivalent novca. Glavna karakteristika virtualnih valuta je nepostojanje središnje institucije koja ih izdaje ili koja njima na neki način upravlja. Stabilnost samih virtualnih valuta se održava pomoću kompleksnih unutarnjih mehanizama sadržanim u samom protokolu. Za zamjenu iz virtualnih valuta u stvarni novac koriste se burze na kojima se tečaj formira ovisno o ponudi i potražnji za određenom virtualnom valutom. Glavni uzrok toga je visoka razina privatnosti korisnika mreže, zbog čega je se povezuje sa ilegalnim aktivnostima.“[17]

„Virtualne valute nisu novac niti novčani ekvivalent jer ne ispunjavaju osnovne funkcije novca. Virtualne valute nisu zakonsko sredstvo plaćanja u Republici Hrvatskoj, nisu strana valuta (deviza), u skladu sa zakonom nemaju ni svojstva elektroničkog novca, a trgovanje i plaćanje virtualnim valutama ne može se smatrati platnom uslugom. Stoga organizacije ili pojedince koji izdaju virtualne valute ili njima trguju nije licencirala Hrvatska narodna banka, niti ona nadzire njihovo poslovanje, kao ni bilo koja druga institucija u RH.“[18]

U trenutku pisanja ovog rada na tržištu se nalazi 6955 kriptovaluta sa ukupnom kapitalizacijom od 327,806,489,690 dolara prema web stranici www.coinmarketcap.com.

6.2 Pametni ugovori

„Pametni ugovori su stvoreni za sigurnu, transparentnu i lakšu razmjenu sredstava bez ikakve potrebe za posrednikom. Pametni ugovori predstavljaju programe koji su napisani da automatski kontroliraju prijenos sredstava između dvije ili više strana, nakon što budu zadovoljeni prethodno definirani uvjeti.

Upisani kod je glavna stvar i koncept svakog ugovora, to može biti bilo koji kod unutar blockchaina ako sadrži uvjet da može upravljati kriptovalutom, sredstvima ili imovinom. Značenje pametnog ugovora i karakteristike koda omogućuju automatsko izvršavanje predodređenog, osiguravajući nepovratnost i nepromjenjivosti.

[17] Primjene i mogućnosti blockchain tehnologije sa naglaskom na pametne ugovore, Matej Ćuže, završni rad (Pristupljeno 8.9.2020.)
[18] Dostupno na: https://www.hnb.hr/-/sto-su-virtualne-valute- (Pristupljeno: 8.9.2020)

Pametni ugovori omogućuju razmjenu novca, robe, nekretnina, vrijednosnih papira i druge imovine. Ugovori se pohranjuje i repliciraju u decentraliziranu struktura podataka u kojoj informacije se ne mogu krivotvoriti ili izbrisati. Istodobno, enkripcija podataka osigurava anonimnost partnera u ugovoru. Važna značajka pametnog ugovora je da oni mogu funkcionirati samo s valutom koja je unutar njegovog digitalnog ekosustava, kako povezati virtualne i stvarne sfere ugovora jedan je od glavnih problema pametnih ugovora. To je razlog postojanja "oracle" posebnih programa koji pomažu računalnim protokolima da pribavljaju potrebne informacije iz stvarnog svijeta.

Prednosti pametnih ugovora:

- Brzina - prerada dokumenata ručno koristi puno vremena i odgađa završetak ciljeva. Pametni ugovori pretpostavljaju automatizirani proces i u većini slučajeva ne zahtijevaju ljudsku uključenost što štedi dragocjeno vrijeme.
- -Neovisnost - pametni ugovori isključuju mogućnost intervencije trećih strana, jamstvo za transakciju je sam program, čime ne postoji sumnja u integritet ugovora.
- Pouzdanost - podaci uneseni u Blockchain ne mogu se mijenjati ili izbrisati. Ako jedna strana u transakciji ne izvrši svoje obveze, druga će biti zaštićena uvjetima pametnog ugovora.
- Nema pogrešaka - automatizirani sustav za izvršavanje transakcija uklanja ljudski faktor i osigurava visoku točnost prilikom izvršavanja ugovora.
- Štednja - pametni ugovori pružaju značajnu uštedu zbog uklanjanja troškova posrednika i smanjenja operativnih troškova.

Nedostaci pametnih ugovora:

- Nedostatak regulacije - međunarodno pravno područje nema točno definirane koncepte blockchain-a, pametnih ugovora i kriptovaluta.
- Poteškoće implementacije - integracija pametnih ugovora s elementima iz stvarnoga svijeta traži puno vremena, novca i truda.
- Nemogućnost mijenjanja pametnog ugovora - Paradoksalno, jedna od glavnih prednosti pametnih ugovora, nemogućnost mijenjanja ugovora.

Pametni ugovori postoje u konceptu pravnih ugovora koji su sposobni poboljšati tradicionalne pravne ugovore, a sve je postignuto korištenjem pametnog koda. Kodovi koji se koriste u 5 ovakvom pametnom ugovoru još nisu zakonski prihvatljivi bez obzira što su u mogućnosti predvidjeti, pojednostaviti i učiniti stvari sigurnijima. Ovakav model

još se mora dobro istražiti jer postoji strah od raznih strana da je ovakav kod previše sofisticiran i da bi se njime moglo manipulirati. Za to nema konkretnih dokaza jer je sama tehnologija još u razvitku, proučavanju i analiziranju.“[19]

6.3.1 Moguće primjene pametnih ugovora

- Lanac opskrbe i praćenje proizvoda

Distributeri mogu koristiti pametne ugovore za prodaju i distribuciju svojih proizvoda po cijelom svijetu. Kôd koji stoji iza pametnog ugovora može pratiti mjesto vaših proizvoda, tako da ih možete pratiti dok mijenjaju ruke u cijelom opskrbnom lancu. Svaki aspekt opskrbnog lanca može se zamijeniti pametnim ugovorom, čineći cijeli sustav učinkovitijim. Od police u vašem skladištu do teretnog broda koji plovi u inozemstvu do izloga, pametni ugovori automatski objavljuju proizvode pravoj osobi nakon što se ispune svi uvjeti ugovora, stvarajući praktični pristup upravljanju lancem opskrbe i praćenju proizvoda.

- Police osiguranja i plaćanje

Polica osiguranja je sporazum između osiguravajućeg društva i potrošača. Ako ste pružatelj osiguranja, pomoću pametnih ugovora možete olakšati uvjete police. Svaki aspekt politike zabilježit će se u pametnom ugovoru. Osiguratelj će pregledati uvjete i pristati na ugovor. Sve dok ugovaratelj osiguranja i dalje ispunjava uvjete, poput plaćanja mjesečne premije, pametni ugovor će držati policu na snazi. Ako nešto krene po zlu i vlasnik police mora unovčiti svoju policu osiguranja, ugovor će automatski osloboditi uplatu osiguranja nakon što osiguratelj osigura potrebnu dokumentaciju koja opisuje štetu na njihovom domu ili automobilu. To ubrzava postupak plaćanja osiguranja, a cijeli sustav održava automatiziranim i učinkovitim. Vlasnici polica i osiguravajuća društva više ne moraju stvarati brdo papira svaki put kad netko treba prikupiti uplatu osiguranja.

[19] Pametni ugovori, Zoran Bartolović (2018) (Dostupno na: https://repozitorij.veleri.hr/islandora/object/veleri:1594/datastream/PDF/view) Datum pristupanja: 11.9.2020.)

- Trgovanje na burzi

Baš poput proizvoda koji mijenja vlasnika na opskrbnom lancu, pomoću pametnih ugovora možete pratiti kretanje dionice ili obveznice dok se ona premješta od jednog vlasnika do drugog. Dionice mogu učestalo mijenjati vlasnika, posebno ako su financijska tržišta u promjeni. No, pametnim ugovorima trgovci mogu brže kupovati i prodavati jer se svaka transakcija automatski provjerava i bilježi na blockchainu. To smanjuje cijenu po transakciji, stvarajući fluidnije tržište.

- Zaštita intelektualnog vlasništva

Ako ste umjetnik ili producent, možete zaštititi svoj rad i intelektualno vlasništvo pametnim ugovorima. Pojedinosti vašeg djela, uključujući sam sadržaj, bit će nedostupne ako netko ne ispuni zahtjeve pametnog ugovora. Ako napravite pjesmu i netko je želi upotrijebiti, morat će se pridržavati pravila pametnog ugovora plaćanjem tantijema, unošenjem podataka o projektu, uključujući kako planiraju koristiti pjesmu. Ako su ispunjeni uvjeti pametnog ugovora, pjesma će se izdati toj osobi. To umjetnicima i producentima pomaže prikupljati novac od svog rada bez skupih pravnih naknada.

6.3 Distribuirana pohrana podataka u oblaku

Pojam "oblak" koristi se za različite vrste platformi za distribuirano računarstvo - skup poslužitelja, mreže, softvera, sučelja itd. koji korisnici trebaju za izvršavanje određenog zadatka. "Računarstvo" se odnosi na isporuku ovog paketa kao usluge koju korisnici mogu koristiti kako žele.

Distribuirana pohrana u oblaku sastoji se od peer-to-peer decentraliziranog rješenja za pohranu u oblaku. Štiti vaše datoteke, kako na čvorovima, tako i u prijenosu, pomoću blockchain tehnologije i kriptografije za šifriranje datoteka.

U principu je predviđen distribuirani sustav za pohranu u oblaku gdje se svaki aspekt pohrane u oblaku, poput prijenosa, obrade ili pohrane podataka, unosi u blockchain. Nakon ovoga, što se dogodilo s podacima, kamo su otišli, tko je pristupio podacima i kako se tim podacima upravljalo može provjeriti svatko tko ima pristup blockchainu.

Takav sustav pomaže u pružanju potpune sljedivosti, odgovornosti i transparentnosti za oblak i one entitete koji ili koriste ili upravljaju oblakom.

Korisnik ne treba posjedovati snažnu računalnu infrastrukturu. Umjesto toga, korisnik može koristiti sličnu infrastrukturu u vlasništvu treće strane i platiti samo za potrebnu količinu računalne snage.

Ovaj model plaćanja po upotrebi omogućuje prikladan pristup mreži na zahtjev i uštedu vremena u izgradnji ogromne računalne infrastrukture. To korisniku omogućuje koncentriranje napora na ključne poslovne aktivnosti. Korisnik putem interneta ima pristup informacija bilo kada s različitih uređaja - stolnih računala, prijenosnih računala, tableta i pametnih telefona.

6.3.1 Blockchain zasnovan na oblaku

U posljednjih nekoliko godina centralizirane vlasničke usluge koje se nude na Internetu zamjenjuju se decentraliziranim otvorenim - neučinkovite monolitne usluge zamijenjene peer-to-peer algoritamskim tržištima. Blockchain tehnologija prvo je decentralizirala novac s bitcoinima, a sada kreće prema decentralizaciji ostalih aspekata poslovnih procesa.

Blockchain tehnologija koristi se za nadzor svakog procesa i primjene u raznim industrijama u svrhu poboljšanja. Kao rezultat toga, pojavljuju se decentralizirane mreže za pohranu (DSN - decentralized storage networks) koje će izazvati divovske tradicionalne tvrtke za pohranu u oblaku poput DropBox-a, OneDrive-a i Amazona. Te su se tvrtke oslanjale na centralizirane usluge gdje se klijenti odriču suvereniteta svojih podataka i prelaze u milost i nemilost tvrtki. DSN agregira pohranu koju nudi više neovisnih davatelja usluga pohrane te se samokoordinira kako bi se klijentima omogućila pohrana i preuzimanje podataka. Usponom decentraliziranih usluga pohrane u oblaku koje pokreće blockchain, nestat će dani stresa zbog krađe podataka, hakiranja i kopiranja podataka klijenata i njihove prodaje trećoj strani.

6.3.2 Prednosti distribuirane pohrane podataka u oblaku

- Podaci zaštićeni od neovlaštenog pristupa

Na primjer, stručnjaci za izradu sigurnosnih kopija i pohranu dokazali su da se pohranjeni podaci nisu miješali kada je stvorena učinkovita i provjerljiva sigurnosna kopija. Distribuirana pohrana u oblaku temeljena na blockchain tehnologiji pohranjuje samo hash-eve svojih podatkovnih blokova. A šifrirani i distribuirani hash-evi dovoljni su za provjeru ovih blokova
podataka.

- Provjerljivost

Blockchain ne pohranjuje podatke samo u distribuiranom i šifriranom obliku, već također osigurava sekvencijalni lanac u kojem svaki blok sadrži kriptografski hash bloka. To povezuje blokove i na taj način stvara decentraliziranu knjigu transakcija.

- Nema posrednika

Za mnoge stručnjake u oblaku najveća promjena koju će blockchain vjerojatno donijeti je disintermedijacija[20]. To je zato što dobro dizajnirani i javno dostupni blockchain može zamijeniti mnoge funkcije na koje se trenutno oslanjamo kod posrednika.

6.4 Autentikacija digitalnog identiteta

Autentikacija je proces određivanja identiteta nekog subjekta, najčešće se odnosi na fizičku osobu. U pravilu korisnik odnosno subjekt koji traži autentikaciju, daje određene podatke po kojima druga strana (web poslužitelj, banka ili neka druga institucija) može utvrditi da je subjekt upravo taj kojim se predstavlja.

„Digitalni identitet predstavlja digitalnu formalnu reprezentaciju stvarne osobe, pod formalnim se misli na činjenicu da vlasnik-korisnik takvog identiteta nije ovlašten da taj identitet stvori ili mijenja, već to radi jedan od ovlaštenih državnih organa. Pod digitalnim identitetom se može smatrati e-osobna iskaznica, e-zdravstvena iskaznica, e-građani korisnički račun, e-vozačka dozvola, i tome slično, ukratko digitalni identitet

[20] Disintermedijacija - proces uklanjanje posrednika kao što su distributera ili brokera koji su ranije povezivali poduzeća s njihovim kupcima

koji neporecivo predstavlja fizičku osobu, kojom se ta osoba, pred zakonom, može identificirati.“[21]

„Gotovo šestina stanovništva na svijetu nema nikakav dokument kojim dokazuju svoj identitet. Neki jer su dokumente izgubili dok su bježali iz ratom pogođenih područja, drugi jer ih nikad nisu ni imali.

Nedostatak identifikacijskih dokumenata ograničava ih u ostvarivanju svojih prava - obrazovanja, zdravstvene zaštite, glasovanja, socijalne zaštite i slično. Kako bi na neki način riješili taj problem, Ujedinjeni narodi pokrenuli su ID2020, globalno javno privatno partnerstvo koje bi trebalo riješiti taj problem. Cilj je tog partnerstva stvoriti digitalni identitet koji bi omogućio ljudima bez dokumenata da ostvare svoja prava na siguran način.

Tvrtka Accenture, u suradnji s Microsoftom i Avanadeom razvila je prototip digitalnog identiteta utemeljen na blockchain tehnologiji - vrsti sustava baze podataka koji omogućava pristup istim podacima različitim sudionicima uz izuzetno visoku razinu povjerenja i sigurnosti.

Prototip koristi Microsoft Azure platformu u oblaku, a dizajniran je kako bi svakom pojedincu dao mogućnost da odlučuje o tome tko ima pravo pristupa njegovim podacima i pod kojim ih uvjetima smije dijeliti.

Sofisticirana, decentralizirana ili distribuirana arhitektura baze podataka, temeljena na blockchain tehnologiji ujedno eliminira potrebu za centraliziranom pohranom i upravljanjem.

Accentureov prototip ne pohranjuje osobne informacije koje bi se mogle koristiti za identifikaciju, već koristi informacije koje su dostupne nakon što korisnik odobri pristup.

"Ljudi bez dokumentiranog identiteta pate jer su isključeni iz modernog društva", istaknuo je upravitelj Accentureovog globalnog blockchain poslovanja, David Treat. *"Naš prototip je osoban, privatan i prijenosan te omogućava pojedincima pristup i dijeljenje odgovarajućih informacija kada je to prikladno, bez potrebe za korištenjem papirnate dokumentacije*."

[21] Jan Petrović, Digitalni identitet, Zagreb 2018. str. 19

Kako bi njihov sustav funkcionirao i bez papirnatih dokumenata, Accenture se koristi Unique Identity Service Platformom koja u sebi sadrži biometrički sustav koji upravlja otiscima prstiju, slikama šarenice i drugim identifikacijskim podacima. Accentureova platforma sastavni je dio Biometric Identity Management System koji trenutno koristi UN-ov visoki povjerenik za izbjeglice i u koji je upisano više od 1,3 milijuna izbjeglica iz 29 zemalja.“[22]

6.5 Primjena u medicini

Kao jedna od reformi koja bi u velikoj većini svijeta bila dobrodošla jest – reforma zdravstva. Ne samo da su troškovi zapanjujuće visoki, već industrija i ljudstvo pati od nepravilne dijagnoze, lošeg iskustva i stalnih briga o sigurnosti pacijenta. Mnogo se toga može popraviti poboljšanom upotrebom podataka.

Medicalchain ima za cilj korištenje blockchain tehnologije za sigurno pohranjivanje medicinskih zapisa. Korištenje glavne knjige za zdravstvo bi značilo mnogo jer liječnicima, bolnicama, laboratorijima, ljekarnicima i zdravstvenim osiguravateljima omogućuje neposredniji pristup zdravstvenim evidencijama, što bi moglo pomoći u spašavanju života. Medicalchain unosi MedTokens i radi na komplementarnoj telemedicinskoj platformi MyClinic.com.

Iako je ideja još u razvojnoj fazi te se uzimaju probni pacijenti i doktori, mora se izgraditi vjerodostojnost na obje strane.

[22] Može li digitalni identitet zamijeniti klasične dokumente?, Martina Čizmić (2017), Dostupno na: https://zimo.dnevnik.hr/clanak/moze-li-digitalni-identitet-zamijeniti-klasicne-dokumente---481631.html Pristupljeno: 9.9.2020

7. Big Data i blockchain tehnologija

Izraz "Big data" nastao je sredinom 1990-ih i definiran je kao zbirka podataka toliko velikih, složenih i dinamičnih da premašuju procesorski kapacitet uobičajenih arhitektura baza podataka organizacija.

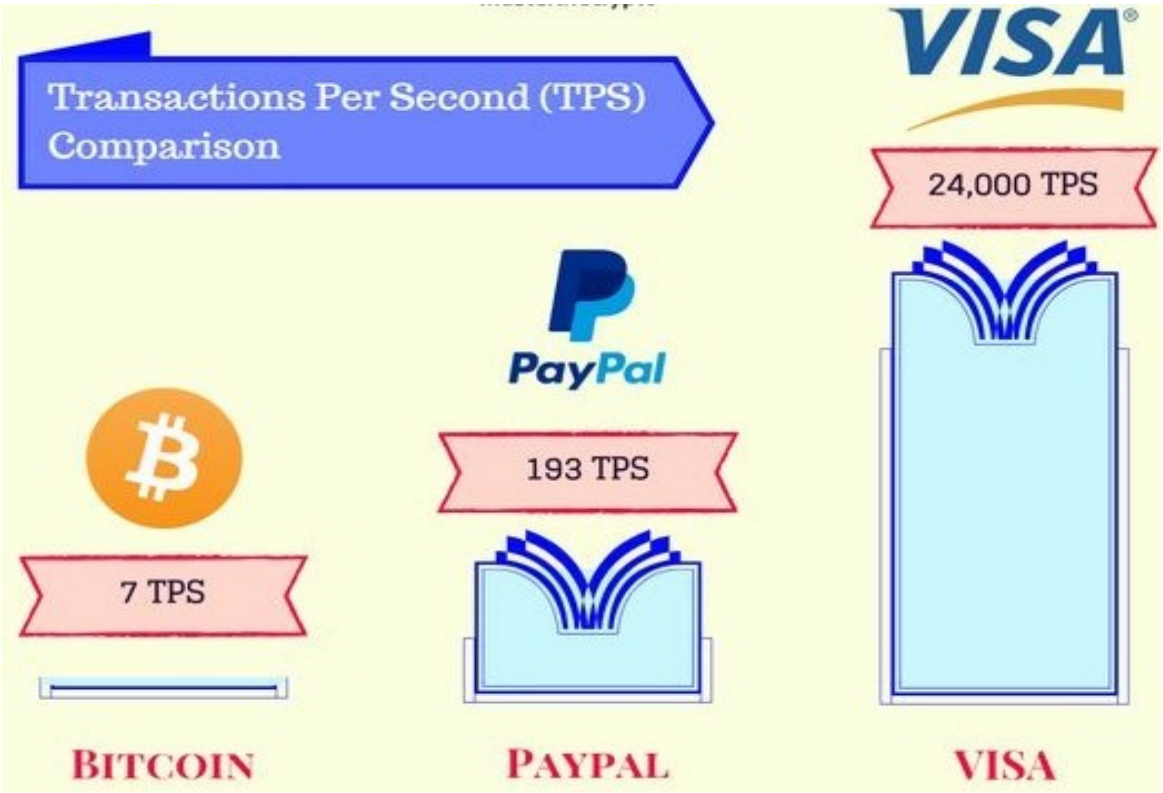
Organizacije se suočavaju s izazovom učinkovitog upravljanja velikim podacima, jer se jednostavno ne uklapa u ograničenja standardnih arhitektura baza podataka. Istodobno, veliki podaci crpe iz više izvora i transakcija i sadrže vrijedne obrasce i informacije. Samo prikupljanje podataka i informacija nije novo. Od 50-ih godina prošlog stoljeća, tvrtke koriste osnovnu analitiku kako bi otkrile skrivene obrasce i trendove, pokazale promjene tijekom vremena te potvrdile ili osporile teorije.
Kako poduzeća skupljaju veliku količinu podataka u svojim bazama podataka na velikim podatkovnim platformama, povećavale su se mogućnosti za iskopavanje inih podataka radi predviđanja. Kako ne mogu učinkovito upravljati podacima sa svojom trenutnom arhitekturom baze podataka, moraju potražiti alternativne načine za obradu. Dobro definirana strategija upravljanja podacima ključna je za uspješno korištenje velikih podataka u korporacijama. Podaci i analitika igraju sve važniju ulogu u poboljšanju konkurentske prednosti, a korporacije velike podatke i sposobnost njihove analize vide kao važan pokretač inovacija i značajan izvor stvaranja vrijednosti.
Blockchain mijenja način na koji svijet pristupa velikim podacima, a njegova tehnologija mogla bi se dobro kombinirati s velikim podacima. Blockchain se može koristiti za pohranu važnih podataka i osiguravanje da podaci ostanu u izvornom obliku dok se distribuiraju. Konačno, kako se pojavljuje sve više i više blockchain aplikacija za različita polja, tradicionalne industrije mogu iskoristiti blockchain za poboljšanje performansi.

Blockchain se može interno koristiti kao baza podataka za aplikacije poput upravljanja fizičkom i digitalnom imovinom, bilježenja internih transakcija i provjere identiteta. Ovo može biti posebno korisno rješenje za tvrtke koje se bore uskladiti više internih baza podataka.

Blockchain je jedna od najbrže rastućih tehnologija koja pomaže osigurati i zaštititi podatke kriptografijom. Tehnologija se može koristiti na bilo kojem tržištu, sektoru ili aplikaciji koja treba sigurno razmjenjivati podatke u decentraliziranom formatu. Ugovori, transakcije i njihovi zapisi jedna su od definirajućih struktura u trenutnom poslovnom, pravnom i političkom sustavu. Oni upravljaju interakcijama među narodima, organizacijama, zajednicama i pojedincima. Ovi kritični alati - i birokracije stvorene za upravljanje njima - nisu išli ukorak s digitalnom transformacijom gospodarstva. Blockchain tehnologija ima potencijal riješiti ovaj problem.

8. Problemi koji prate uvođenje blockchain tehnologije

Kako svaka tehnologija koja dolazi na tržište, tako i blockchain, mora proći period sazrijevanja i prihvaćanja od potencijalnih korisnika. Kako se od sredine 2017. povećala potražnja za bitcoinom, problem skalabilnosti se višestruko povećao.



Slika 6. Usporedba skalabilnosti, Izvor: https://masterthecrypto.com/blockchain-scalability-bitcoin-scalability-problem-effects/ datum pristupanja: 10.9.2020

Iz slike je vidljiva problematika skalabilnosti i može se zaključiti kako je pred bitcoinom dug put kako bi bio kompetitivan pred tradicionalnom konkurencijom.

Zašto je blockchain spor? Da bi dobili odgovor na to pitanje moramo razumjeti kako on funkcionira.

Kako je prije navedeno, blockchain je podloga za mnoge kriptovalute ne samo bitcoin, ali s obzirom da je on prvi i najpoznatiji, uzet je za primjer.

Blockchain je doslovno lanac blokova međusobno povezanih, a svaki blok sadrži provjerene transakcije koje su nepromjenjive, sigurne i javne.

Blockchain ledger sporiji je u usporedbi s centraliziranim sustavima s obzirom da se obavljaju dodatni poslovi koji uključuju:

- Provjeru potpisa

Svaka pojedinačna transakcija unutar mreže zahtijeva digitalne potpise koji kriptografski potpisuje vlasnik privatnih ključeva (koji su tehnički vlasnici novca). To je obavezno u peer-to-peer mreži kako bi se dokazala autentičnost novca, a time i sama transakcija. Generiranje i provjera tih potpisa računalno je intenzivno i složeno. S druge strane, centralizirani sustav ne zahtijeva provjeru svakog pojedinog zahtjeva, jer središnji poslužitelj diktira pravila koja reguliraju pristup.

- Redundantna izračunavanja

Distribuirani sustav prirodno je suvišan zbog replikacije iste knjige na mnogim pristupnim točkama. Zbog prirode otvorenog koda Bitcoina, svatko može postati čvor i upravljati vlastitim poslužiteljem. Prednost ove arhitekture je što je mreža izuzetno sigurna (otporna na kvarove). Međutim, to znači da se transakcije moraju obrađivati pojedinačno i odvojeno za svaki čvor u mreži, što zahtijeva više posla i oduzima više vremena. Alternativno, odnos klijent-poslužitelj u centraliziranom sustavu zahtijeva obradu transakcije u samo jednoj instanci.

- Postizanje konsenzusa

Postizanje konsenzusa u decentraliziranom sustavu vitalni je uvjet za svaki blockchain. Bitcoin koristi mehanizam konsenzusa Proof-of-Work (POW) za postizanje konsenzusa, koji zahtijeva od rudara da rješavaju složene matematičke probleme koristeći ogromne količine računalnih i električnih resursa. Jednom kada se pokaže točnim, pobjednički rudar nagrađuje se u Bitcoinima (BTC) i mreža će pristati da se novi blok uključi u blockchain. To uključuje značajnu količinu komunikacije između čvorova u osiguravanju trenutnog stanja blockchaina. Mehanizam konsenzusa izravno utječe na prosječno vrijeme stvaranja bloka; za Bitcoin mrežu treba 10 minuta da se cijeli ovaj proces ostvari. U centraliziranoj bazi podataka šanse za sukobljene transakcije su minimalne i stoga zahtijeva mnogo manje vremena za obradu.

Ostali problemi s kojima se blockchain tehnologija susreće je nedostatak razvojnih programera, cyber napadi, regulacije unutar pojedine države, velika potrošnja električne energije kako bi se tehnologija održala. U konačnici jedan od većih problema je samo pridobivanje novih korisnika. S obzirom da je blockchain tehnologija u relativno ranoj fazi, očekuje se da bi većina navedenih problema trebala biti riješena s vremenom ili barem u nekoj mjeri umanjena.

9. Zaključak

Kako je pojam blockchain poznat kao nešto povezano s kriptovalutom Bitcoin, zapravo je blockchain tehnologija nešto puno više. Iako su kriptovalute cijelu tehnologiju učinile popularnom i potakli razna istraživanja na tu temu. Iako su kriptovalute tek djelomično prihvaćene, može se vidjeti da se ubrzanim korakom radi na implementaciji kako u bankarski sustav tako i druga područja gdje bi blockchain bio koristan.

Bez obzira na prednosti koje donosi blockchain tehnologija svojom implementacijom važno je istaknuti i nedostatke koji se trebaju riješiti kako bi se tehnologija počela masovno primjenjivati. Sam nedostatak razvojnih programera bi se trebao riješiti u sljedećih nekoliko godina, a rješavanje tog problema bi dalo dodatni vjetar u leđa za daljnju implementaciju i korištenje tehnologije.
Važno je naglasiti da blockchain tehnologija nije nadasve čarobno rješenje, ali svakako postoji potencijal da se znatno unaprijede mnogi procesi u društvu.

Blockchain tehnologija je revolucionarno rješenje. Učinit će život jednostavnijim i sigurnijim, mijenjajući način pohrane osobnih podataka i način obavljanja transakcija i usluga.

Sažetak

Blockchain tehnologija je oblik tehnologije koje svoje temelje bazira na sigurnosti. Pojavila se prvi puta 2008. godine, ali do značajnijeg zapažanja došlo je unazad nekoliko godina. Blockchain tehnologija tek čeka široka prihvaćenost, koja je nadasve blizu. Primjena se, zbog svojih karakteristika, najviše usmjerava prema računovodstvu i financijama te se sve više rješenja temeljena na blockchain tehnologiji implementiraju u poslovanje. Zbog specifičnosti i osjetljivosti podataka koje se generiraju te istovremeno moderna poslovanja teže ka neovisnosti, tu se blockchain tehnologija nametnula kao idealno rješenje.

Ključne riječi: blockchain, kriptovalute, decentralizirani sustav, pametni ugovori, konsenzus

Summary

Blockchain technology is a form of technology that bases its foundations on security. It appeared for the first time in 2008, but a significant observation was made several years ago. Blockchain technology is just waiting for mainstream acceptance, which is above all close. Due to its characteristics, the application is mostly focused on accounting and finance, and more and more solutions based on blockchain technology are being implemented in business. Due to the specificity and sensitivity of the data that is generated, and at the same time modern business strives for independence, blockchain technology has emerged as an ideal solution.

Keywords: blockchain, cryptocurrencies, decentralized system, smart contracts, consensus

Literatura

[1] https://www.iltanet.org/blogs/deborah-dobson/2018/02/13/the-4-types-of-blockchain-networks-explained?ssopc=1 datum pristupanja 24.6.2020

[2] Živković S. (2018) Blockchain tehnologija, Rijeka: Odjel za informatiku. Dostupno na: https://zir.nsk.hr/islandora/object/infri:289/preview (Datum pristupanja: 1.7.2020.)

[3] What is Cryptocurrencies Cryptography? (2017.) Dostupno na www.blockgeeks.com/guides/cryptocurrencies-cryptography (datum pristupanja: 26.6.2020)

[4] Može li digitalni identitet zamijeniti klasične dokumente?, Martina Čizmić (2017), Dostupno na: https://zimo.dnevnik.hr/clanak/moze-li-digitalni-identitet-zamijeniti-klasicne-dokumente---481631.html (datum pristupanja: 9.9.2020)

[5] Što su virtualne valute? Dostupno na: https://www.hnb.hr/-/sto-su-virtualne-valute- (datum pristupanja: 8.9.2020)

[6] Živković S. (2018) Blockchain tehnologija, Rijeka: Odjel za informatiku. Dostupno na: https://zir.nsk.hr/islandora/object/infri:289/preview (Datum pristupanja: 1.7.2020.)

[7] Pametni ugovori, Zoran Bartolović (2018) (Dostupno na: https://repozitorij.veleri.hr/islandora/object/veleri:1594/datastream/PDF/view) Datum pristupanja: 11.9.2020.)

[8] Mohsen Attaran, Angappa Gunasekaran, Applications of Blockchain Technology in Business, 2019

[9] Pejčić, Lovro, Analiza tehnologije Blockchain, Osijek 2018. str.12 (Dostupno na: https://zir.nsk.hr/islandora/object/etfos%3A1978/datastream/PDF/view) Datum pristupanja: 18.9.2020.

Popis slika

[1] Struktura blockchaina izvor: https://revistadigital.inesem.es/informatica-y-tics/blockchain/ (Datum pristupanja: 18.9.2020.)

[2] Transakcije grupirane u blok, vlastita izrada

[3] Povezivanje blokova radi formiranja blockchaina, vlastiti izvor

[4] Prikaz određivanja tvorca blokova
Izvor: https://www.kriptovaluta.hr/tutorials/sto-je-konsenzus-i-koje-sve-vrste-postoje/, (Datum pristupanja: 02.09.2020)

[5] Slika 4. Razlika između tradicionalnog bankarskog sustava i blockchain mreže
Izvor: http://www.7wdata.be/data-analysis/introduction-to-blockchain-and-what-it-means-for-big-dana (Datum pristupanja: 15.9.2020)

[6] Usporedba skalabilnosti, Izvor: https://masterthecrypto.com/blockchain-scalability-bitcoin-scalability-problem-effects/ (Datum pristupanja: 10.9.2020)