BLOCKCHAIN TEHNOLOGIJA I NJEN UTJECAJ NA SVIJET

Širić, Mario

SVEUČILIŠTE U SPLITU
EKONOMSKI FAKULTET

INFORMATIČKI MENADŽMENT

ZAVRŠNI RAD

BLOCKCHAIN TEHNOLOGIJA I NJEN UTJECAJ NA SVIJET

Student:

Mario Širić, 1151533

Mentor:

prof.dr.sc. Željko Garača

Split, rujan, 2018.

SADRŽAJ

1. UVOD 1

2. KRIPTOGRAFSKA HASH FUNKCIJA 1

2.1. SHA-256 2

3. BLOCKCHAIN TEHNOLOGIJA 2

3.1. Povijest 3

3.2. Struktura blockchaina 3

3.3. Decentraliziranost i otvorenost blockchaina 4

3.4. Prednosti blockchain tehnologije 5

3.5. Nedostatci blockchain tehnologije 7

3.6. Vrste blockchaina 8

3.6.1. Javni blockchainovi 8

3.6.2. Privatni blockchainovi 8

3.6.3. Blockchainovi konzorcija 9

3.7. Kriptovalute 9

4. BITCOIN 10

4.1. Kako bitcoin funkcionira 11

4.1.1. Kriptografija 11

4.1.2. Rudarenje 12

4.1.3. Dvostruka potrošnja 13

4.1.4. Dokaz o radu 14

4.1.5. Dokaz o udjelu 15

4.1.6. Novčanik 15

5. ETHEREUM 17

5.1. Pametni ugovori 18
5.2. Ethereum Virtualni Stroj 19
5.3. Solidity 19
5.4. Ether 19
5.5. Dokaz o radu na Ethereum platformi 19
6. PRIMJENA BLOCKCHAIN TEHNOLOGIJE 20
6.1. Digitalni identitet 20
6.2. Financijske usluge i infrastruktura 21
6.3. E-trgovina i maloprodaja 21
6.4. Blockchain i Internet stvari 22
6.5. Upotreba u poduzećima 23
6.6. Medicinski zapisi 23
6.7. Obrazovni zapisi 24
6.8. Dijeljenje znanja 25
6.9. Sektor osiguranja 26
6.10. Označavanje prehrambenih proizvoda 26
6.11. Računovodstvo i revizija 27
6.12. E-glasanje 28
7. ZAKLJUČAK 28
8. SAŽETAK 29
9. SUMMARY 30
10. LITERATURA 31

1. UVOD

Važno je naglasiti da će se neki novi pojmovi spomenuti prije nego budu objašnjeni. Razlog tome je što se u početku ovog rada opširno opisuju razne tehnologije, a tek kasnije se povezuju svi spomenuti pojmovi u smislenu cjelinu gdje su, naravno, i detaljnije objašnjeni.

Naš globalni financijski sustav pomiče bilijune dolara dnevno i služi milijarde ljudi. Ali taj sustav je prepun problema, povećava trošak kroz naknade i kašnjenja, stvara trenje kroz suvišnu i napornu papirologiju i otvara mogućnosti za prijevaru i zločin. Financijski sustav je tako neefikasan zbog toga što je zastario, što je centraliziran i što ne dopušta svojim korisnicima brz i lagan pristup potrebnim informacijama. Spomenuti problemi, ali i mnogi drugi, se nalaze i u ostalim sustavima. Jednostavni procesi, kao što su odlazak kod liječnika, podizanje dokumentacije u javnim ustanovama, davanje svog glasa na izborima, itd., se bespotrebno kompliciraju dugim čekanjima u redu, nepotrebnom papirologijom, usporenom i neefikasnom birokracijom i ograničenom pristupu relevantnim dokumentima. Ako razmislimo, većina današnjih sustava je nedovoljno efikasna, netransparentna u svojim procesima, sklona greškama, nedovoljno zaštićena od napada, iziskuje iznimne napore te ogromnu količinu vremena. Iako spomenuti sustavi nisu doživjeli veće, i prijeko potrebne, promjene dugi niz godina, rješenje za ovakve inovacijske zapreke se napokon pojavilo. Zove se blockchain tehnologija.

2. KRIPTOGRAFSKA HASH FUNKCIJA

Za proučavanje blockchain tehnologije prvo moramo definirati što su kriptografske hash funkcije. Posebno je važno spomenuti funkciju SHA-256 jer se koristi prvi povezivanju i dodavanju novih blokova u blockchainu. Kriptografske hash funkcije važan su alat kriptografije i imaju temeljnu ulogu u učinkovitoj i sigurnoj obradi informacija.

Funkcija hash procesira proizvoljnu ulaznu poruku određene duljine u poruku fiksne duljine koja se naziva hash vrijednost. Kao sigurnosni zahtjev, hash vrijednost ne bi trebala poslužiti kao preslika dvije različite ulazne poruke i trebalo bi biti teško pronaći ulaznu poruku određene hash vrijednosti. Sigurne hash funkcije služe za integritet podataka, a ne za odbacivanje i autentičnost izvora zajedno sa shemama digitalnog potpisivanja. Ključne hash funkcije, koje se nazivaju i

kodovi za provjeru autentičnosti poruka (MAC-ovi), služe za integritet podataka i provjeru vjerodostojnosti podataka u postavci tajnog ključa.

2.1. SHA-256

SHA-256 je član SHA-2 kriptografskih hash funkcija koje je dizajnirala NSA.
SHA-256 se koristi u nekoliko različitih dijelova Bitcoin mreže:

- Rudarenje (eng. *mining*) koristi SHA-256 kao algoritam dokaza o radu (eng. *Proof of Work*).
- SHA-256 se koristi za stvaranje bitcoin adresa za poboljšanje sigurnosti i privatnosti.

SHA-256 kompresijska funkcija radi sa 512-bitnim blokovima poruke i 256-bitnim međurezultatima hash vrijednosti. SHA-256 je u biti 256-bitni kriptografski algoritam koji kriptira međurezultate hash vrijednosti koristeći blok poruke kao ključ.

3. BLOCKCHAIN TEHNOLOGIJA

Blockchain je decentralizirana, distribuirana i javna digitalna knjiga (eng. *ledger*) koja se koristi za bilježenje transakcija na mnogim računalima, tako da zapis ne može biti retroaktivno promijenjen bez izmjene svih sljedećih blokova i konsenzusa mreže. To omogućuje sudionicima da jeftino provjere i izvrše reviziju transakcija.

Blockchain baza podataka se upravlja autonomno koristeći peer-to-peer mrežu i distribuiranog poslužitelja vremenskog pečatiranja (eng. *timestamping*). Oni su ovlašteni masovnom suradnjom koja se pokreće kolektivnim vlastitim interesima. Rezultat je robustan tijek rada gdje je neizvjesnost sudionika u pogledu sigurnosti podataka marginalna. Korištenje blockchaina uklanja karakteristike beskonačnog dupliciranja digitalne imovine. To potvrđuje da je svaka jedinica vrijednosti prenesena samo jednom, rješavajući dugogodišnji problem dvostruke potrošnje (eng. *double spending*).

Blockchainovi su opisani kao protokol razmjene vrijednosti. Ova razmjena vrijednosti temeljena na blockchainu može biti brža, sigurnija i jeftinija nego kod tradicionalnih sustava. Blockchain

može dodijeliti naslovna prava jer, ako je pravilno postavljen za detalje ugovora o razmjeni, pruža zapis koji obvezuje ponudu i prihvaćanje.

3.1. Povijest

Blockchain je kreacija čovjeka ili kolektiva ljudi pod pseudonimom Satoshi Nakamoto. Nakamoto je objavio svoj izum 31. listopada, 2008. godine na jednoj kriptografskoj „mailing“ listi (metzdowd.com). Naziv znanstvenog rada je : “Bitcoin: A Peer-to-Peer Electronic Cash System“. Prva implementacija njegove ideje objavljena je u siječnju 2009. godine. Prvi program (eng. *client*) je kao otvoreni kod (eng. *open-source*) dostupan zajednici tog istog siječnja. Prvim “puštanjem” Bitcoin mreže 3. siječnja 2009. kreirani su i prvi bitcoini (kriptovaluta).

Nakamoto je softver razvijao i bio glavni programer sve do sredine 2010. godine. Zatim predaje projekt u ruke Gavina Andresena koji je jedan od glavnih suradnika. Isto tako je sve kreirane domene Nakamoto dao ključnim programerima koji su pomogli razvijati ovaj fascinantni softverski projekt. Do sredine 2010. godine sve izmjene na softveru je izvršavao Nakamoto.

Prvi inicijalni tečaj bitcoina dogovarali su individualci na forumima. Prva čuvena i zloglasna transakcija je 10 000 bitcoina za dvije pizze. Istih 10 000 bitcoina osam godina kasnije na današnji dan vrijedi cca. 250 000 000 kn. Danas se uglavnom trguje na bitcoin mjenjačnicama i burzama. Bitcoin kao način plaćanja uvode i velike kompanije kao što su: TigerDirect, Overstock.com, Expedia, Dell i Microsoft.

3.2. Struktura blockchaina

Blockchain, kao što mu ime i govori, se sastoji od lanca blokova koji sadrže serije valjanih transakcija koje su hashane i kodirane u Merkleovo stablo (kriptografska stablasta struktura u kojoj je svaki čvor koji nije list, obilježen hashem oznake njegove djece-čvorova). Svaki blok sadrži kriptografski hash prethodnog bloka u blockchainu, povezujući ih. Povezani blokovi tvore lanac. Ovaj iterativni proces potvrđuje cjelovitost prethodnog bloka, sve natrag do izvornog bloka koji se još naziva „genesis block“.

Ponekad se mogu stvoriti zasebni blokovi istodobno, stvarajući privremeni vilicu (eng. *fork*), odnosno diobu blockchaina u dvije nove grane. Osim sigurne hash-bazirane povijesti, svaki

blockchain ima određeni algoritam za bodovanje različitih verzija povijesti, tako da jedan s većom vrijednošću se može odabrati nad drugima. Blokovi koji nisu odabrani za uključivanje u lanac nazivaju se siročadi (eng. *orphans*). Korisnici koji podržavaju bazu podataka imaju različite verzije povijesti s vremena na vrijeme. Oni zadržavaju samo najvišu inačicu baze podataka koja im je poznata. Kad god peer dobije verziju s višom ocjenom (obično stara inačica s dodanim novim blokom), proširuju ili prebrišu vlastitu bazu podataka i ponovno prenose poboljšanje svojim peerovima. Nikada nije apsolutno jamstvo da će svaki pojedini zapis zauvijek ostati u najboljoj verziji povijesti.

Budući da se blokovi obično grade za dodavanje novih blokova na stare blokove i zato što postoji poticaj za rad samo na proširivanju novih blokova umjesto da se prebrišu stari blokovi, vjerojatnost da unos postane nadomješten pada eksponencijalno kako se dodatni blokovi nadovezuju jedni na druge. Na primjer, u blockchainu pomoću sustava dokaza o radu, lanac s najvećim dokazom o radu uvijek se smatra valjanom mrežom. Postoji niz metoda koje se mogu koristiti za dokazivanje utrošene dovoljne razine računanja (eng. *computing*). Unutar blockchaina računanje se vrši redundantno, a ne tradicionalno odvojeno i paralelno.

3.3. Decentraliziranost i otvorenost blockchaina

Decentralizirana priroda tehnologije blockchaina znači da se ne oslanja na središnju točku kontrole. Nedostatak jednog tijela čini sustav pravednijim i znatno sigurnijim. Način na koji se podaci bilježe na Blockchainu ističu najrevolucionarniju kvalitetu: vrijednost decentralizacije.

Umjesto da se oslanja na središnje tijelo da sigurno obavlja poslove s drugim korisnicima, Blockchain koristi inovativne konsenzusne protokole na mreži čvorova (eng. *nodes*), provjerava transakcije i bilježi podatke na način koji je nepotkupljiv. Budući da je blockchain knjiga podataka, izuzetno je važno da podaci koji se pohranjuju budu iskreni i točni.

Što je konsenzusni protokol?

Konsenzusni protokol skup je pravila koja opisuju komunikaciju i prijenos podataka između elektroničkih uređaja kao što su čvorovi. Konsenzus se postiže kada se dovoljni broj uređaja slaže oko onoga što je istina i što treba zabilježiti na blockchainu. Stoga su konsenzusni protokoli

vladajuća pravila koja omogućuju uređajima koji su raspršeni diljem svijeta da postignu dogovor, čime blockchain mreža može funkcionirati bez problema.

Budući da se sustav ne oslanja na središnje tijelo, naknade koje obično prikupljaju ove organizacije više nisu bitan faktor. Stoga se transakcije na blockchainu mogu smatrati jeftinijima, jer su jedini troškovi koji su nastali od strane uključenih strana nominalna naknada koja se koristi za nagrađivanje rudara (eng. *miners*) koji potvrđuju transakcije određene kriptovalute ili krivotvoritelja (eng. *forgers*) koji vode čvor na mreži.

Nadalje, informacije snimljene na blockchainu su sigurno istinite jer im je gotovo nemoguće manipulirati zbog toga što postoji više kopija koje zahtijevaju složeni konsenzus za uređivanje. Osim toga, u kombinaciji s ulogom koju imaju kriptografske hash funkcije u sustavu, manipulacija se dodatno otežava.

Podatci se još više osiguravaju činjenicom da nema oslanjanja na središnju točku skladištenja, smanjujući rizik gubitka ili uništavanja. Napad na jednu točku skladištenja ne bi rezultiralo gubitkom podataka budući da su sve informacije pohranjene na više uređaja širom svijeta. U tom smislu, bitcoin je najotpornija platforma koja je uspješno podnijela sve napade i pokušaje hakiranja.

3.4. Prednosti blockchain tehnologije

1. Raspodijeljenost

Blockchain omogućuje širokom rasponu računala da sudjeluje u mreži, dijeleći računalnu moć. Na primjer, Amazon kupuje i održava privatni skup računala za AWS (Amazon Web Services) kojem nitko ne može pridonijeti osim samog Amazona. Nasuprot tome, blockchain organizacija

Ethereum dopušta gotovo svakome da „posudi“ svoje računalo njihovoj mreži, jednostavno instaliranjem njihovog softvera. Raspodjela pomaže smanjiti rizik od neovlaštenih modificiranja, prijevara i „cyber“ kriminala. S više čvorova koji sudjeluju u blockchainu, sustavi su vrlo teško ugroženi putem tradicionalnih napada mreže brute force metodom.

2. Nepovjerljivost

Blockchain omogućava odvijanje digitalnih transakcija između stranaka koje si međusobno ne vjeruju. Zamislimo digitalni novac pohranjen u datoteci na računalu. Datoteka se može kopirati i zalijepiti beskonačan broj puta. Vrijednost ove digitalne valute bila bi blizu nule. U prošlosti, središnje institucije (banke) djelovale su kao voditelji glavnih knjiga, vodeći računa o iznosu koji svatko od nas posjeduje kao centralizirana glavna knjiga kako bi izbjegli problem dupliciranja, odnosno dvostruke potrošnje.

Distribuiranjem knjige na mnoge čvorove i sinkronizacijom ove knjige putem konsenzusa, blockchain omogućava stranama koje si ne vjeruju, da budu sigurne kako je transakcija stvarna, a ne bezvrijedna. Vremenom, povjerenje je postajalo snažnije putem zajedničkih procesa i nepromjenjivih evidencija transakcija. To olakšava masivni raspon potencijalnih digitalnih transakcija koje se nisu mogle dogoditi prije bez upravljanja od strane središnjeg tijela.

3. Nepromjenjivost

Kada je transakcija odobrena i podijeljena na distribuiranoj mreži, gotovo ju je nemoguće poništiti. Zapravo, tijekom vremena sve ju je teže i teže poništiti. U javnoj glavnoj knjizi, kao što je bitcoin, to znači da se blockchain može istražiti i otkriti broj bitcoinova na bilo kojem računu, ili trag gdje su raspoređena ta sredstva. U drugim scenarijima to se može koristiti za praćenje lanaca opskrbe ili provjeru tko je pristupao određenim datotekama na mreži.

4. Decentraliziranost

Iako je decentraliziranost već spomenuta, valja je ponoviti u kontekstu prednosti blockchain mreže. Blockchain također podržava smanjenje centraliziranih monopola ili "srednjih ljudi (eng. middle-men)" i uklanja troškove. Distribuiranjem, blockchain mreža može pronaći ekonomiju razmjera, bez centraliziranog ulaganja. To povećava konkurenciju na tržištu, snižavajući prepreke ulaska te stavlja pritisak na sve sudionike da postanu učinkovitiji. Uz to, dopuštajući peerovima da obavljaju poslove bez potrebe za povjerenjem, ometaju trenutačnu poslovnu praksu organizacija koje olakšavaju to isto povjerenje, kao što su banke. Izravne transakcije između peerova mogu dovesti do smanjenja koraka "srednjeg čovjeka", što dodatno povećava učinkovitost tržišta.

3.5. Nedostatci blockchain tehnologije

1. Rasipnost

Svaki čvor pokreće blockchain kako bi održao konsenzus preko blockchaina. To daje ekstremne razine tolerancije kvarova, osigurava odvijanje procesa bez zastoja, a podatke pohranjene na blockchainu zauvijek su nepromjenjive i otporne na cenzuru. Ali sve je to rasipno, jer svaki čvor ponavlja zadatak da dosegne konsenzus koji troši struju i vrijeme na putu.

To čini računanje daleko sporije i skuplje nego kad bi se sve odvijalo na jednom računalu. Postoje mnoge inicijative koje nastoje smanjiti ovaj trošak s naglaskom na alternativnim načinima održavanja konsenzusa, kao što je sustav dokaza o udjelu (eng. *Proof of Stake*).

2. Brzina i cijena održavanja mreže

Blockchain mreže zahtijevaju čvorove za pokretanje. No, budući da su mnoge mreže nove, nedostaje im čvorova kako bi olakšali široku upotrebu. Ovaj nedostatak resursa manifestira se kao:

- Veći troškovi - budući da čvorovi traže više nagrade za dovršavanje transakcija u scenariju ponude i potražnje
- Sporije transakcije - s obzirom da čvorovi potražuju transakcije s većim nagradama, stvara se promet s zaostalim transakcijama

S vremenom će uspješne javne blockchain mreže morati poticati čvorove, uz stvaranje povoljnih troškova za korisnike, s transakcijama dovršenim u relevantnom vremenskom okviru. Ta je ravnoteža ključna za ekonomiju svakog blockchaina.

3. Vilice

Mnoge valute i blockchainovi decentraliziraju svoje odluke. Na primjer, Bitcoin omogućava čvorovima, koji pokreću mrežu, da signaliziraju podršku za poboljšanja jezgre softvera. To omogućava blockchainu da izbjegne centralizirano odlučivanje, ali predstavlja i izazove kada su zajednice podijeljene oko najboljeg načina za poboljšanje samog softvera.

Kada čvorovi mijenjaju svoj softver, postoji mogućnost za vilicu u lancu. Čvorovi koji upravljaju novim softverom ne prihvaćaju iste transakcije kao čvorovi koji upravljaju starim. Time se stvara novi blockchain s istom poviješću kao i onaj na kojem se gradi.

Forkovi stvaraju značajnu neizvjesnost, budući da imaju potencijal da fragmentiraju moć blockchain mreže u mnoge varijante. Također je vjerojatno da će vilice biti neophodne, jer bez mogućnosti ažuriranja softvera, blockchain neće moći opstati u budućnosti.

4. Nepromjenjivost pametnih ugovora

Jednom kada se pametni ugovor (eng. *smart contract*) doda u blockchain, on postaje nepromjenjiv. Ako postoje propusti u programskom kodu koji mogu biti iskorišteni od strane hakera, oni ostaju tamo zauvijek. To ne predstavlja problem kada se pametni ugovor ne upotrebljava, ali kako se pametni ugovori ponašaju kao računi, oni se mogu koristiti za pohranu velikih količina vrijednosti.

To može stvoriti scenarije gdje hakeri mogu iskoristiti nedostatke programskog koda kako bi poslali sadržaj pametnih ugovora na svoje račune. Budući da je blockchain nepromjenjiv, ove transakcije se vrlo teško mogu poništiti, što znači da se velike količine vrijednosti mogu zauvijek izgubiti.

3.6. Vrste blockchaina

3.6.1. Javni blockchainovi

Javni blockchain nema apsolutno nikakvih ograničenja pristupa. Svatko tko ima internetsku vezu može poslati transakcije u javni blockchain te postati ovjeritelj, odnosno sudjelovati u izvršenju konsenzusnog protokola. Obično takve mreže koriste neku vrstu algoritma kao što je sustav dokaza o udjelu (PoS) ili sustav dokaza o radu (PoW) te nude ekonomske poticaje onima koji ih osiguravaju.

Neki od najvećih i najpoznatijih javnih blockchainova su Bitcoin i Ethereum.

3.6.2. Privatni blockchainovi

Kod privatnog blockchaina, korisnici se ne mogu pridružiti osim ako ih ne pozovu mrežni administratori. Pristup sudionika i ovjeritelja je ograničen.

Ova vrsta blockchainova može se smatrati dobrom opcijom za tvrtke koje su zainteresirane za tehnologiju blockchaina, ali nisu zadovoljne razinom kontrole koju nude javne mreže. Tipično, one nastoje uključiti blockchain u svoje računovodstvene i evidencijske postupke bez žrtvovanja autonomije i rizika otkrivanja osjetljivih podataka javnosti.

3.6.3. Blockchainovi konzorcija

Često se konzorcijski blockchain smatra „polucentraliziranim“. I ovakav blockchain je ograničen, ali umjesto jedne organizacije koja ga kontrolira, broj tvrtki može pojedinačno rukovati čvorovima na takvoj mreži. Administratori blockchain konzorcija ograničavaju korisnička prava na svojevoljno čitanje i dopuštaju samo ograničenom skupu pouzdanih čvorova izvršavanje konsenzusnog protokola.

3.7. Kriptovalute

Kriptovaluta je digitalna imovina osmišljena kao sredstvo razmjene koja koristi snažnu kriptografiju radi osiguranja financijskih transakcija, kontrole stvaranja dodatnih jedinica i provjere prijenosa imovine. Kriptovalute koriste decentraliziranu kontrolu za razliku od centraliziranog sustava elektroničkog novca i središnjeg bankarstva. Decentralizirana kontrola svake kriptovalute funkcionira putem tehnologije distribuirane glavne knjige, tipično blockchaina, koja služi kao baza podataka javnih financijskih transakcija.

Bitcoin, prvi izdan kao softver otvorenog koda u 2009., općenito se smatra prvom decentraliziranom kriptovalutom. Od tada je stvoreno više od 4.000 altcoinova (alternativnih valuta), odnosno, varijanti bitcoina.

Decentraliziranu kriptovalutu kolektivno proizvodi čitav sustav po stopi koja je definirana kada se stvara sami sustav i koji je javno poznat. U centraliziranim bankarskim i gospodarskim sustavima, kao što su Sustav federalnih rezervi, određeni korporativni odbori i vlade, opskrba se kontrolira tiskanjem fiducijarnog novca. U slučaju decentralizirane kriptovalute, tvrtke ili vlade ne mogu proizvesti nove jedinice i do sada nisu pružale potporu drugim tvrtkama, bankama ili pravnim osobama koje su vlasnici imovine mjerene u kriptovalutama.

Od svibnja 2018. postoji više od 1.800 kriptovaluta. Unutar sustava kriptovaluta sigurnost, integritet i ravnoteža glavnih knjiga održava zajednica pojedinaca koji si ne moraju međusobno

vjerovati, a nazivaju se rudari (eng. *miners*): koristeći svoja računala kako bi pomogli potvrditi i vremenski odrediti odvijanje transakcija, dodajući ih u knjigu u skladu s određenom shemom vremenskih oznaka.

Većina kriptovaluta je dizajnirana tako da se postupno smanjuje broj jedinica, stavljajući ograničenje na ukupan broj te valute koji će ikada biti u optjecaju. U usporedbi s običnim valutama koje drže financijske institucije, kriptovalute mogu biti teže zaplijenjene od strane provoditelja zakona. Ova prepreka proizlazi iz iskorištavanja kriptografskih tehnologija.

4. BITCOIN

Bitcoin je decentralizirana kriptovaluta koju je stvorila nepoznata osoba ili grupa ljudi pod imenom Satoshi Nakamoto i koja je izdana kao open-source softver u 2009. godini. Ne oslanja se na središnjeg poslužitelja za obradu transakcija ili pohranu sredstava.

Od siječnja 2018, to je najčešće korištena alternativna valuta, sada s ukupnom tržišnom vrijednošću od oko 250 milijardi američkih dolara.

Bitcoin nema središnjeg izdavatelja; umjesto toga, peer-to-peer mreža regulira bitcoine, transakcije i izdavanje prema konsenzusu mrežnog softvera. Ove transakcije potvrđuju mrežni čvorovi pomoću kriptografije i bilježe ih u javnoj distribuiranoj knjizi, odnosno blockchainu.

Bitcoini se izdaju za različite čvorove koji provjeravaju transakcije putem računalne snage; utvrđeno je da će biti ograničeno i zakazano puštanje u iznosu od najviše 21 milijun bitcoin (BTC) jedinica, koje će biti u potpunosti izdane do 2140. godine.

Bitcoini se stvaraju kao nagrada za proces poznat kao rudarstvo. Mogu se razmjenjivati za druge valute, proizvode i usluge. Od veljače 2015. preko 100.000 trgovaca i prodavača prihvatilo je bitcoin kao sredstvo plaćanja. Istraživanja koje je provelo Sveučilište u Cambridgeu procjenjuju da je 2017. godine bilo 2,9 do 5,8 milijuna jedinstvenih korisnika koji koriste novčanik kriptovaluta, a većina ih koristi bitcoin.

Međunarodno, bitcoini se mogu razmjenjivati putem različitih web stranica i softvera zajedno s fizičkim novčanicama i kovanicama.

4.1. Kako bitcoin funkcionira

Već je spomenuto nekoliko pojmova u poglavlju blockchain tehnologije o kojima će i ovdje biti riječi kako bi se pokušalo što jasnije objasniti načine na koji bitcoin funkcionira.

4.1.1. Kriptografija

Postoji nekoliko kriptografskih tehnologija koje čine bit bitcoina.

Prva je kriptografija javnog ključa. Svaka jedinica povezana je s ECDSA (varijanta DSA – Digital Signature Algorithm, algoritma koja u svom radu koristi eliptične krivulje koje pružaju manju veličinu ključa s približno jednakim razinama sigurnosti i vremenom obrade te identičnom duljinom generiranog sažetka) javnim ključem svog trenutnog vlasnika. Kada se nekome šalju bitcoini, izradi se poruka (transakcija), veže se javni ključ novog vlasnika na taj iznos i potpiše ga se privatnim ključem. Kada se ova transakcija emitira na Bitcoin mreži, to daje svima na znanje da je novi vlasnik ovog iznosa vlasnik novog ključa. Spomenuti potpis pošiljatelja na poruci potvrđuje svima da je poruka autentična. Cjelokupnu povijest transakcija čuvaju svi, tako da svatko može provjeriti tko je sadašnji vlasnik bilo kojeg iznosa.

Ovaj potpuni zapis o transakcijama čuva se u blockchainu, što je niz zapisa zvanih blokova. Sva računala u mreži imaju kopiju blockchaina koja se ažurira tako da računala dodaju nove blokove u blockchain. Svaki blok sadrži grupu transakcija poslanih od prethodnog bloka. Kako bi se očuvao integritet blockchaina, svaki blok u lancu potvrđuje integritet prethodnog, sve do prvog, izvornog bloka. Unos zapisa je skup jer svaki blok mora zadovoljavati određene zahtjeve koji otežavaju stvaranje valjanog bloka. Na taj način, niti jedna strana ne može prebrisati prethodne zapise samo zaokruživanjem lanca.

Kako bi se otežalo generiranje bitcoina, koristi se troškovna funkcija hashcash. Hashcash je prva sigurna, efikasno provjerljiva funkcija troškova, odnosno funkcija dokaza o radu. Ljepota hashcash funkcije je da je neinteraktivna i nema tajnih ključeva kojim moraju upravljati središnji poslužitelji ili oslanjajući stranke; hashcash funkcija je kao rezultat potpuno raspodijeljena i beskonačno skalabilna. Hashcash funkcija koristi kriptografiju simetričnog ključa, to jest jednosmjernu funkciju hashcash - obično SHA1 ili SHA-256.

U Bitcoinu, integritet, nizanje blokova u lancu te hashcash troškovna funkcija sve koriste SHA256 kao temeljnu kriptografsku hash funkciju.

Kriptografska hash funkcija, u suštini, preuzima ulazne podatke koji mogu biti praktički bilo koje veličine i pretvara ih u relativno kompaktan niz koji je nemoguće preokrenuti ili predvidjeti na bilo koji način (u slučaju SHA-256 hash se sastoji od 32 byte-a). Čineći najmanju promjenu na ulaznim podacima mijenja se hash nepredvidivo tako da nitko ne može stvoriti drugi blok podataka koji daje točno isti hash. Stoga, dajući kompaktni hash, može se potvrditi da hash odgovara samo određenom inputu, a u Bitcoinu je ulazni podatak blockchaina znatno veći od SHA-256 hasha. Na taj način, Bitcoin blokovi ne moraju sadržavati serijske brojeve jer blokovi mogu biti identificirani pomoću njihovih hashova, što služi za identifikaciju kao i za provjeru integriteta.

Faktor težine (eng. *difficulty factor*) hashcash funkcije postiže se time da hash output ima niz vodećih nula. Tehnički, kako bi se omogućila preciznija kontrola od hashcashove metode vodećih 0 bitova, Bitcoin proširuje definiciju rješenja hashcashove funkcije tretiranjem hasha kao velikog „big-endian“ (metoda pohrane podataka od najznačajnijih bitova ka najneznačajnijim) broja i provjerom da je broj ispod određenog praga. Funkcija hashcash troškovne funkcije se ponavlja remeteći podatke u bloku jednokratnom vrijednošću sve dok se podaci u bloku ne hashaju da proizvedu broj ispod praga – što zahtijeva mnoštvo računalne moći. Ova niska hash vrijednost za blok služi kao lako provjerljiv dokaz o radu - svaki čvor na mreži može odmah potvrditi da blok zadovoljava tražene kriterije.

Ovim okvirom možemo postići bitne funkcije Bitcoin sustava. Imamo provjerljivo vlasništvo nad bitcoinima i distribuiranu bazu podataka svih transakcija, što sprječava dvostruku potrošnju.

4.1.2. Rudarenje

Spomenuli smo u prethodnom odjeljku da je dodavanje bloka u blockchainu teško jer zahtijeva vrijeme i računalnu moć. Poticaj za utrošeno vrijeme i struju je da osoba koja uspije proizvesti blok biva nagrađena. Ova nagrada je dvostruka. Prvo, proizvođač bloka dobiva određeni broj bitcoina, što je dogovoreno putem mreže. Trenutačno ovaj bonus iznosi 12.5 bitcoina, a ta vrijednost će se prepoloviti svakih 210.000 blokova. Drugo, svaka transakcijska naknada koja može biti prisutna u transakcijama uključenim u blok također dobiva proizvođač tog bloka.

To dovodi do aktivnosti poznate kao "bitcoin rudarenje" - koristeći procesorsku moć kako bi se pokušalo proizvesti valjani blok, a kao rezultat rudarenja neki bitcoini. Mrežna pravila su takva da se faktor težine prilagođava kako bi se proizvodnja blokova održala na oko 1 blok po 10 minuta. Dakle, što više rudara sudjeluje u rudarskoj aktivnosti, to postaje teže za svakog pojedinog rudara da stvori blok. Što je veći ukupni faktor težine to je za potencijalnog napadača teže prebrisati vrh blockchaina vlastitim blokovima (što bi mu omogućilo dvostruko trošenje).

Osim što je važno za održavanje baze podataka o transakcijama, rudarenje je i mehanizam kojim se bitcoini stvaraju i distribuiraju među ljudima u Bitcoin ekonomiji. Umjesto da se optjecajem bitcoina manipulira, oni se, umjesto toga, dodjeljuju onima koji pridonose mreži stvaranjem blokova u blockchainu.

4.1.3. Dvostruka potrošnja

Blockchain je zajednička knjiga koju dijele svi Bitcoin čvorovi, koja bilježi svaku transakciju koja se izvrši. Za razliku od konvencionalnih bankarskih sustava, nema središnjeg mjesta gdje se pohranjuje ova knjiga transakcija. To se postiže putem generiranja blokova, od kojih svaki tvrdi da je nastavak prethodnog bloka. Moguće je da se blockchain razdijeli, odnosno, moguće je da dva bloka oba ukazuju na isti roditeljski blok i sadrže neke, ali ne sve, iste transakcije. Kada se to dogodi, svako računalo u mreži mora samo odlučiti koja je grana "ispravna" te koja bi trebala biti prihvaćena i dalje proširena.

Pravilo je u ovom slučaju prihvatiti "najdužu" važeću granu. Iz ogranaka blokova koji su primljeni izabere se onaj čiji je ukupni "faktor težine" najviši. Ovo je redoslijed blokova za koje se pretpostavlja da su zahtijevali najviše računalne moći za generiranje. Za Bitcoin to će biti "pravi" red događaja, a to je ono što će se uzeti u obzir prilikom izračuna stanja koji se prikazuje korisniku.

Još je moguće da, budući da se novi blokovi neprestano stvaraju, kasnije neka druga grana postane najduža. Međutim, potreban je znatan napor za proširenje grane, a čvorovi rade na proširenju grane koju su primili i prihvatili (što je obično najduža grana). Dakle, što ova grana postane dulja u usporedbi s drugom najdužom granom, to će teže biti za drugu najdužu granu da sustigne i nadvlada prvu granu. Također, što više čvorova u mreži čuje za najdužu granu, manje je vjerojatno da će se druge grane proširiti sljedeći put kada se generira blok, budući da čvorovi prihvaćaju najduži lanac.

Stoga, što je više vremena transakcija dio najduljeg blockchaina, to je vjerojatnije da će ostati dio lanca zauvijek. To je ono što čini transakcije ireverzibilne i što sprječava ljude od dvostruke potrošnje. Ono što primatelj svake transakcije radi, nakon što mu se navodno prenese novac, je provjera koliko je dug blockchain postao nakon izvršenja navedene transakcije, jer što se više blokova doda na najdužu granu nakon transakcije, to je manje vjerojatno da ju neka druga grana nadvlada.

Kada blockchain postane dovoljno dug nakon transakcije, postaje gotovo nemoguće za drugu granu da nadvlada postojeću i tako ljudi mogu početi prihvaćati transakciju kao istinitu. Zato blokovi također služe i kao potvrde za transakciju. Čak i ako druga grana prevlada onu granu koja sadrži transakciju, većina blokova će se generirati od strane ljudi koji nemaju vezu s pošiljateljem transakcije, s obzirom da veliki broj ljudi radi na generiranju blokova. Budući da se transakcije prenose na sve čvorove u mreži, ti blokovi imaju jednaku vjerojatnost da će sadržavati transakciju kao i blokovi u prethodno prihvaćenoj grani.

Bitcoin se oslanja na činjenicu da niti jedan entitet ne može kontrolirati većinu računalne moći na mreži u određenom vremenu, jer kad bi mogao, proširio bi bilo koju granu stabla i to brže nego se ijedna druga grana može proširiti, čineći ju najdužom granom, i stoga trajno kontrolirao sve transakcije koje se pojavljuju u njoj.

4.1.4. Dokaz o radu

U sustavu dokaza o radu, rudari se natječu kako bi provjerili jesu li sve transakcije unutar bloka koji se trenutno gradi legitimne. Da bi to postigli, moraju riješiti kriptirane zagonetke koje potvrđuju integritet transakcije. Prvi rudar koji riješi ovu zagonetku dobiva blok nagradu, odnosno, određeni iznos valute koju provjerava. Nakon što se problem riješi, transakcije se vežu u blok koji se pohranjuje kao javna knjiga na blockchainu, a rudar najavljuje rješenje cijeloj mreži. Ostali rudari provjeravaju je li blok ispravan kako bi mogli nastaviti s rješavanjem iduće zagonetke i potencijalno osvojiti sljedeću blok nagradu. Na ovaj način, svi blokovi su provjereni i legitimizirani što omogućuje neometano odvijanje sustava i nemogućnost manipulacije istim.

Kao jedna analogija, na ovaj se sustav može gledati kao na međunarodno matematičko natjecanje u kojemu se prethodno neriješeni dokaz (blok) daje natjecateljima (rudarima). Tko prvi riješi ovaj

dokaz, prima nagradu (blok nagradu), a riješeni dokaz objavljuje se na internetu svima na uvid (blok je uspostavljen u blockchainu).

4.1.5. Dokaz o udjelu

Dokaz o udjelu u potpunosti se razlikuje od dokaza o radu. Umjesto stvaranja blokova računalnim radom, tvorac bloka se određuje njegovim udjelom u relevantnoj kriptovaluti.

U ovom sustavu, odabrani su krivotvoritelji, PoS ekvivalent rudara, za izgradnju blokova na temelju njihovog uloga u kriptovaluti i starosti tog udjela unutar blockchaina. Kao primjer, možemo zamisliti korisnika koji posjeduje 500.000 jedinica određene kriptovalute. Taj korisnik ima prednost nad nekim korisnikom koji posjeduje samo 400.000 jedinica te iste kriptovalute. Uz to, bitno je naglasiti i vremenski period u kojem je taj iznos na određenoj adresi. Pa tako korisnik koji drži iznos pohranjen na adresi godinu dana ima prednost nad korisnikom koji čuva iznos na svojoj adresi samo nekoliko mjeseci.

Dakle, ugledni korisnici sa pozamašnim iznosom određene kriptovalute koja je pohranjena na duže vrijeme na određenoj adresi ima značajne izglede da će biti odabran kao krivotvoritelj.

Zauzvrat, krivotvoritelj prima svu transakcijsku proviziju sadržanu u bloku kojeg se procesuira, što znači da u ovom sustavu nema blok nagrade, već samo spomenute transakcijske provizije.

4.1.6. Novčanik

Novčanik kriptovaluta pohranjuje javne i privatne ključeve koji se mogu koristiti za primitak ili potrošnju kriptovalute. Novčanik može sadržavati više parova javnih i privatnih ključeva. U slučaju bitcoina i kriptovaluta izvedenih iz njega, kriptovaluta je decentralizirano pohranjena i održavana u javno dostupnoj knjizi. Svaka jedinica ima privatni ključ pomoću kojeg je moguće upisati se u javnu knjigu te tako i trošiti spomenutu kriptovalutu.

4.1.6.1. Hardverski novčanik

Hardverski novčanici su namjenski uređaji koji služe kao dodatni sloj sigurnosti za opcije hladnog skladištenja (novčanik koji nije povezan s internetom i time smanjuje rizik od hakiranja) poput papirnatih novčanika. S papirnatim novčanikom, na primjer, sredstva su sigurna sve dok se ne

koristi računalo - ali ako je računalo koje se upotrjebljava za pristup valuti ugroženo, tada se povećava vjerojatnost da korisnički račun biva hakiran.

Nasuprot tome, hardverski novčanici imaju siguran čip u njima, što znači da kada se povežu s računalom kako bi se poslala kriptovaluta, nikada nije potrebno unijeti privatni ključ na računalo. Jednostavno se zaporka unese na hardver, što znači da je trgovanje na kompromitiranom računalu sigurnije. Ako se hardver pokvari ili izgubi, može se ponovno vratiti pristup kriptovaluti na novom uređaju iz teksta slučajno odabranih riječi koji se dobio s hardverskim novčanikom (npr. niz nasumice odabranih riječi koje se koriste za vraćanje novčanika i kriptovalute koja se nalazi na novčaniku).

Iako su hardverski novčanici najsigurniji način pohranjivanja kriptovaluta, vrijedi li platiti njihovu cijenu ovisi o iznosu kriptovalute koja se drži. Da bi se koristili hardverski novčanici, potrebno je imati softverski novčanik da bi se stupilo u interakciju s uređajem.

4.1.6.2. Softverski novčanik

Softverski novčanici temelje se na računalnom softveru. Softverski novčanici dostupni su u tri formata: na desktopu, u mobilnom izdanju i online:

Desktop novčanici su računalni programi koji pohranjuju kriptovalutu lokalno na stolnom računalu ili na prijenosnom računalu. Jedna od primarnih prednosti desktop novčanika je da ona nudi korisnicima potpunu kontrolu kriptovalute, bez potrebe za oslanjanjem na sučelje neke treće strane. Međutim, to znači da cijela sigurnost ovisi o korisniku. Ako je korisnik hakiran ili ako dođe do pada računala, sav novac se može izgubiti zauvijek. Strah od hakiranja jedan je od razloga zbog kojih neki ljudi radije koriste nekorištena ili rezervna računala koja nemaju pristup internetu kako bi pohranili svoje valute.

Mobilni novčanici djeluju putem aplikacije na mobilnom telefonu. Primarna prednost mobilnih novčanika je mogućnost brzog pristupa i jednostavnog korištenja svoje valute. Mobilni novčanici dolaze u dva formata: jedna vrsta aplikacija pohranjuje novac na mobilnom telefonu (i dolazi s istim prednostima i nedostatcima kao i desktop novčanici), dok drugi oblik mobilnog novčanika samo pruža pristup serverima za online pohranu (s istim prednostima i nedostatcima kao online novčanici).

Online novčanici su novčanici koji se nalaze na mreži i može im se pristupiti s bilo kojeg mjesta te s bilo kojeg uređaja, a može se povezati i sa stolnim i sa mobilnim novčanicima. Međutim, glavni nedostatak je što privatne ključeve pohranjuju vlasnici web stranice na kojem se nalazi novčanik što zahtijeva veliko povjerenje u njihovu odgovornost te samu sigurnost web stranice.

5. ETHEREUM

Ethereum je javna, distribuirana računalna platforma otvorenog koda temeljena na blockchainu te operativni sustav s funkcionalnošću pametnih ugovora.

Ether je kriptovaluta čiji je blockchain generirala Ethereum platforma. Ether se može prenijeti između računa i može biti korišten za kompenzaciju rudara koji sudjeluju u izračunavanju. Ethereum pruža decentralizirani Turingov kompletan virtualni stroj, Ethereum Virtual Machine (EVM), koji može izvršiti skripte koristeći međunarodnu mrežu javnih čvorova. "Gas", mehanizam internog određivanja cijena transakcija, koristi se za ublažavanje neželjene pošte i raspoređivanja resursa na mreži.

Ethereum je predložen krajem 2013. od strane Vitalika Buterina, istraživača i programera kriptovaluta. Razvoj je financiran putem online „crowdsale-a“ koji je održan od srpnja do kolovoza 2014. godine. Sustav je otvoren javnosti 30. srpnja 2015. godine s 11,9 milijuna jedinica „izrudarenih“ za sami „crowdsale“. To čini oko 13 posto ukupne ponude koja trenutno cirkulira.

Dakle, ukratko, Ethereum je otvorena platforma koja se temelji na blockchain tehnologiji koja omogućuje programerima izgradnju i implementaciju decentraliziranih aplikacija.

Decentralizirana aplikacija ili Dapp, u ovom kontekst, odnosi se na aplikaciju koja je izgrađena na blockchain tehnologiji. Decentralizirane aplikacije izvršavaju se na blockchainu i imaju koristi od svih njegovih svojstava poput nepromjenjivosti, otpornosti na manipulaciju i nemogućnosti prekida rada.

U suštini bilo koja usluga može se pretvoriti u decentraliziranu aplikaciju. Mogućnosti su beskrajne.

Pet glavnih elemenata omogućuje Ethereumu da funkcionira. Ti elementi su:

• Pametni ugovori

• Ethereum virtualni stroj

• Solidity

• Eter

• Dokaz o radu

5.1. Pametni ugovori

Pametan ugovor je, u suštini, kod koji upravlja razmjenom bilo čega od vrijednosti; od imovine i dionica do informacija i novca između stranaka. Pametni ugovori pokreću se na Ethereum blockchainu upravo onako kako su programirani i postaju autonomni agenti koji se izvršavaju kada su zadovoljeni prethodno navedeni uvjeti.

Ugovori u Ethereumu ne smiju se smatrati nečim što bi se trebalo "ispuniti" ili "poštivati"; oni su više nalik "autonomnim agentima" koji žive unutar Ethereum okružja za izvršenje (EVM), uvijek izvršavajući određeni dio koda kada se aktivira putem poruke ili transakcije i imaju izravnu kontrolu nad vlastitim saldom Ethera. U Bitcoinu, na primjer, korisnici mogu napraviti jednostavnu potražnju kao što je - poslati jedan bitcoin od Ivana do Marija. U Ethereumu, međutim, moguće je izraditi ugovor koji kaže da se pošalje jedan Ether Mariju ako je datum 25. listopada 2018., a Ivanov trenutni saldo je više od 20 Ethera.

Ono što čini pametne ugovore vrlo primamljivima je da se sami izvrše točno onako kako ih se dizajniralo nakon što su ispunjeni određeni uvjeti. Stvaranje pametnog ugovora s znatno složenijim uvjetima je također moguće. Pametni ugovor, na primjer, mogao bi olakšati automatsko prenošenje vlasništva nad nekretninom nakon što se ispune brojni kritični uvjeti. Sve ovo je moguće bez ikakvog ljudskog sudjelovanja.

5.2. Ethereum Virtualni Stroj

Pametni ugovori se pokreću pomoću Ethereum Virtualnog Stroja (eng. *Ethereum Virtual Machine*) i Ethera. EVM uključuje Turingov kompletni skriptni jezik, što znači da može riješiti bilo koji problem računanja. EVM pretvara Ethereum u programabilni blockchain, osiguravajući da se svi pametni ugovori izvršavaju na vrijeme i usklađujući ih s ostatkom mreže. Time EVM omogućuje razvoj potencijalno tisuća različitih aplikacija na platformi Ethereum.

5.3. Solidity

Ethereum ima svoj programabilni jezik pod nazivom "Solidity" koji je sličan JavaScriptu. Omogućuje programerima pisanje programa (pametnih ugovora) na Ethereumu i osmišljen je kako bi unaprijedio Ethereum Virtualni Stroj (EVM).

5.4. Ether

U Ethereum blockchainu, umjesto rudarenja za bitcoinima, rudari rade za Ether. Ether je nužan element za opstanak Ethereum mreže. To je kao „gorivo“ koje pruža poticaj programerima da naprave kvalitetne aplikacije te da mreža funkcionira bez poteškoća. Osim „goriva“ koje omogućuje pokretanje decentraliziranih aplikacija, Ether je također kriptovaluta kojom se može trgovati. U Ethereumu, Ether koriste programeri za plaćanje transakcijskih naknada za usluge i pohranu na mreži.

Svako računanje na platformi, kao rezultat transakcije, ima naknadu, a što je više potrebno pohraniti, više se plaća. To je zato što računanje i pohrana datoteka stavljaju opterećenje na mrežu. Dakle, naknade postoje kako bi obeshrabrile programere da pretjerano koriste mrežu. Bez naknada koje ohrabruju korisnike da poduzmu akciju, Ethereum mreža jednostavno ne bi mogla funkcionirati. Iz navedenog, može se zaključiti da je Ether poput „kripto-goriva“ koje pokreće Ethereum mrežu.

5.5. Dokaz o radu na Ethereum platformi

Iako je već bilo riječi o sustavu dokaza o radu, valja ukratko objasniti kako je implementiran na Ethereum platformi. Da bi decentralizirani sustav poput Ethereuma mogao funkcionirati bez

središnjeg posrednika, mora postojati način kako bi se mreža složila oko toga koji su transakcijski zapisi valjani.

Poput Bitcoinove mreže, Ethereum se oslanja na protokol dokaza o radu kako bi se postigao konsenzus o tome koji su transakcijski zapisi istiniti. Dokaz o radu obavlja se kako bi se olakšalo odvijanje transakcija na Ethereum blockchainu i odvratilo zloćudne aktere od slanja lažnih ili nelegitimnih transakcija. To zahtijeva od rudara da dokažu kako je određeni dio posla završen rješavajući složene matematičke zagonetke koje je teško odgonetnuti, ali lako provjeriti. Proces zahtijeva velike računalne napore (puno hardverske opreme i korištenja električne energije), budući da rudari koriste skupe računalne komponente kako bi opetovano i brzo nagađali odgovore na matematičke probleme sve dok netko ne pobijedi. Budući da ti matematički problemi zahtijevaju toliko posla da se uspješno riješe, prijevarne transakcije postaju nemoguće.

Samo blokovi koji sadrže odgovor na složeni matematički problem bit će prihvaćeni i dodani Ethereum blockchainu. To se, u prosjeku, događa svakih 15 sekundi. Rudari koji uspješno riješe PoW zagonetku dobivaju određeni iznos Ethera kao nagradu. Budući da Ethereum nema središnjeg izdavatelja Ethera, to je također način na koji se stvaraju novi Etheri. Planirana je promjena iz sustava dokaza o radu u sustav dokaza o udjelu zvanom Casper u skoroj budućnosti.

6. PRIMJENA BLOCKCHAIN TEHNOLOGIJE

Blockchain je, kako je već pojašnjeno, izumljen i osmišljen kao platforma koja bi omogućila pojavu digitalnih valuta te kako bi omogućila brže, učinkovitije, sigurnije i transparentnije digitalne transakcije. To uključuje razmjenu kriptovaluta, novca pa čak i intelektualnih svojstava. Međutim, sada će biti riječi o alternativnim aplikacijama blockchaina u različitim poljima.

6.1. Digitalni identitet

Zahvaljujući sigurnom mehanizmu koji štiti nedopušteno izmjenjivanje, blockchain može igrati ključnu ulogu u osiguravanju digitalnih identiteta. Blockchain može zaštititi identitet pomoću enkripcije. Štoviše, blockchain se također može koristiti za izgradnju vrlo snažnog, sigurnog i neprobojnog sustava identiteta, koji može spriječiti neovlaštene aktivnosti.

Blockchain tehnologija ima potencijal zamijeniti sve postojeće fizičke identifikacije i premjestiti ih na digitalnu platformu. Niz identiteta kao što su putovnice, vozačke dozvole, osobne iskaznice pa čak i biračke glasovi mogu se digitalno odvijati upotrebom tehnologije blockchaina. Također je moguće da se svi identiteti skladište zajedno i osiguravaju blockchainom, što identitet pojedinca čini sigurnim i zaštićenim. Korištenjem blockchaina, neovlašteno izmjenjivanje različitih certifikata kao što su obrazovni, bračni, smrtni ili rodni listovi, ne može se izvršiti te se time sprječavaju neovlaštene i zlćudne namjere.

Radilo se o bankama, poduzećima, osiguranjima ili zdravstvenim ustanovama, upravljanje i kontrola pristupa identitetima je iznimno važna. A primjena tehnologije blockchaina u svim tim poljima može rezultirati besprijekornim nadzorom identiteta i autorizacijom istih.

6.2. Financijske usluge i infrastruktura

Blockchain tehnologija može pružiti platformu za bolje financijske usluge i pristupnike plaćanja. Digitalna kriptovaluta poput bitcoina, kao što je već poznato, pokreće tehnologija blockchaina. Korištenje takvih kriptovaluta može obnoviti postojeće platne sustave i druge financijske usluge. Na primjer, ako određena osoba šalje novac svojoj obitelji u drugoj zemlji, moguća sredstva prijenosa su banke, aplikacije za plaćanje (kao što su PayPal) ili druge posredničke organizacije kao što su MoneyGram ili Western Union. Ali njihovi troškovi za usluge su visoki, čak i za transakcije manjih iznosa (eng. *micropayments*).

Svi ovi posrednici mogu se eliminirati i novac se može izravno prenijeti od pošiljatelja do primatelja pomoću kriptovaluta, kao što je bitcoin, bez uključivanja bilo kakvog posrednika. Mlada poduzeća (eng. *startups*) kao što su Sentbe i Abra, započele su svoje usluge doznačivanja P2P transakcija koje su omogućene pomoću bitcoina i blockchain tehnologije. Praćenje transakcija i prava vlasništva također se mogu implementirati u financijskim sektorima pomoću blockchaina. Korištenje blockchain tehnologije u financijskom sektoru ne samo da će osigurati besplatan sustav plaćanja, već će također omogućiti siguran i zaštićen način za odvijanje mrežnih transakcija.

6.3. E-trgovina i maloprodaja

Ako se implementira na pravi način, blockchain tehnologija bi mogla masovno potpomoći e-trgovini i maloprodaji u smislu rasta, prodaje i marketinga. Trgovina na malo već je počela

svjedočiti rastu i dobitku od prodaje robe široke potrošnje i usluga korištenjem tehnologije blockchaina.

Internet djeluje kao velika platforma za promociju lokalnih tvrtki i drugih sadržaja na mreži, ali uvijek postoji rizik da se sadržaj koristi bez odgovarajućih dozvola na različitim mjestima. Svo ovo plagiranje sadržaja može se obuzdati pomoću tehnike vremenskog pečatiranja blockchaina i sačuvati originalnost bilo kojeg sadržaja.

Implementiranje blockchain tehnologije u maloprodajnoj industriji također će osigurati jasan i transparentan sustav upravljanja opskrbnim lancem, koji će korisnicima omogućiti uvid u porijeklo njihove hrane i ostale robe.

Web stranice e-trgovine i druge tvrtke kao što su OpenBazaar, Provenance, Everledger, Ascribe, i BlockVerify su neke od blockchainom potpomognutih poduzeća koja su uključena u maloprodajnu industriju. Na taj način, eliminiraju se posrednici i naplata provizija te se može postaviti izravni kanal za transakcije između kupca i prodavatelja. To neće samo povećati poslovanje malih dobavljača putem internetskog medija, već će i promicati gospodarstvo.

6.4. Blockchain i Internet stvari

Budući da je blockchain decentralizirani mehanizam, dopušta distribuciju digitalnih informacija među različitim čvorovima bez kopiranja. To može stvoriti novu vrstu interneta koja je sigurna i otporna na neovlašteno izmjenjivanje.

Koristeći blockchainov sigurni i distribuirani sustav šifriranih mreža, on može poslužiti kao platforma za Internet stvari (eng. *Internet of Things*) koji povezuje uređaje neprimjetno i pouzdano. Uporabom blockchain tehnologije, svim IoT uređajima može se upravljati po nižoj cijeni i manjom potrošnjom energije. Siguran model omogućuje jednostavnu ljudsku interakciju s uređajima bez potrebe za središnjim sustavom temeljenim na oblaku (eng. *cloud-based system*), koji je obično skuplji. Štoviše, budući da neće biti središnjeg nadzornog sustava kao što je oblak, vjerojatnost da cijeli sustav IoT bude oštećen ili zaustavljen je zanemariva.

To osigurava kontinuitet, jednostavnost operacija, robusnost, skalabilnost i sigurnost IoT pri vrlo malim troškovima. Moguć je razvoj još mnogih drugih obećavajućih i revolucionarnih razvojnih postignuća u IoT koja se mogu ostvariti pomoću tehnologije blockchaina.

6.5. Upotreba u poduzećima

Korištenje blockchain tehnologije u organizacijama može uvelike pridonijeti poslovanju. Sve organizacije i tvrtke trebaju se baviti upravljanjem imovinom, što uključuje aktivno i pažljivo praćenje svih fizičkih i nefizičkih sredstava unutar organizacije.

Točnost i vjerodostojnost podataka ključni su dijelovi upravljanja u svakoj industriji. Često tvrtke izdvajaju ogromne količine kapitala na ove procese i svejedno ne ostvare željene rezultate. Blockchain tehnologija može biti jednostavna, pouzdana, sigurna i jeftina alternativa za konfiguracijski menadžment. Sve neispravne izmjene podataka mogu se odmah pratiti, ostavljajući organizacijske podatke sigurnima od oštećenja.

Dok su neke od aplikacija blockchaina već u uporabi, većina njih se tek treba pojaviti. Blockchain je revolucionarna tehnologija koja još nije ostvarila svoj puni potencijal. Bez obzira na domenu, industriju ili aplikaciju, blockchain ima potencijal da transformira način na koji većina procesa funkcionira. Kada se vlade i pravne vlasti slože i ovlaste sustav otvorene knjige na globalnoj razini, blockchain će postati bitan medij za poboljšanje globalne ekonomije, poduzeća i sustava poštene trgovine.

6.6. Medicinski zapisi

Do sada su liječnici bili suočeni s brojnim preprekama kada je u pitanju digitalno pohranjivanje i razmjena podataka o pacijentima.

Rad iz 2013. objavljen u Online Journal of Public Health Informatics časopisu iznio je tri glavne prepreke učinkovitog upravljanja digitalnim zapisima:

- „Pristupačnost zapisima (znati gdje se medicinski zapisi nalaze i lako im pristupiti)
- Održavanje privatnosti (osigurati da samo one osobe koje je pacijent ovlastio mogu koristiti zapise)

- Osiguravanje funkcionalnosti zajedničkih informacija (osigurati dijeljenje zapisa između različitih platformi bez gubitka njihovog značenja te omogućiti demonstraciju njihove autentičnosti i vjerodostojnosti)“

S tehnologijom blockchaina, sve tri prepreke su svedene na prihvatljivu razinu ili potpuno eliminirane.

Prvo, decentraliziranoj blockchain bazi podataka mogu pristupiti ovlašteni pojedinci - bilo da su pružatelji zdravstvenih usluga, nositelji osiguranja ili pacijenti - bilo gdje, u bilo kojem trenutku i u formatu sa kojim mogu raditi sve stranke.

Dodatna prednost takvom sustavu bila bi tranzicija u kontroli. Tel Avivov dokaz o radu uveo je koncept koji će staviti moć dijeljenja medicinskih podataka u ruke pacijenata umjesto u ruke pružatelja zdravstvenih usluga.

Drugo, blockchain tehnologija omogućava sigurnosne mjere koje nisu dostupne drugim metodama digitalnog dijeljenja, što olakšava oslovljavanje briga privatnosti.

Konačno, blockchain tehnologija smanjuje broj posrednika koji obrađuju svaki ulaz i održava trajne, vremenske zapise svake transakcije, što smanjuje mogućnost pogreške, a istodobno pruža visoku razinu transparentnosti i povjerenja.

6.7. Obrazovni zapisi

Zdravstvena industrija nije jedina koja bi se mogla revolucionirati tehnologijom blockchaina.

Tvrtka Sony Corporation, u suradnji s Sony Global Education, nedavno je podnijela patentnu prijavu za blockchain-bazirani repozitorij koji bi obuhvatio učeničke i studentske školske zapise, uključujući završene tečajeve, testne rezultate, diplome, studije i još mnogo toga, u obliku digitalnog prijepisa.

Sony je u priopćenju objavljenom 9. kolovoza 2017. godine izjavio: „Koristeći tehnologiju koja zajednički upotrebljava obrazovna postignuća i evidentira aktivnosti na otvoren i siguran način, ovaj pouzdani sustav centralizira upravljanje podatcima višestrukih obrazovnih institucija i omogućava bilježenje i referiranje obrazovnih podataka i digitalnih prijepisa.“

Takav sustav mogao bi omogućiti nastavnicima i studentima pristup relevantnim podacima, uz održavanje privatnosti. Mogao bi također pružiti budućim obrazovnim ustanovama i potencijalnim poslodavcima transparentno, pouzdano mjesto za stjecanje vjerodajnica podnositelja zahtjeva.

Uz pohranjivanje obrazovnih zapisa, Sony je predložio da obrazovne institucije mogu koristiti AI analizu podataka na takvoj platformi „kako bi pružile predložena poboljšanja u nastavnim programima i njihovom upravljanju."

6.8. Dijeljenje znanja

Everipedia, prva svjetska enciklopedija na blockchainu, nedavno je najavila planove za izgradnju nove, wiki mreže otvorenog koda koja decentralizira bazu znanja Wikipedije dopuštajući svakom uredniku da postane dionik u mreži.

Everipedia, za koju Larry Sanger, jedan od utemeljitelja Wikipedije, djeluje kao direktor informacija, oslanjat će se na EOS blockchain programu kako bi učinio korisničke doprinose odgovornijima, počevši od siječnja 2018. godine. Urednici će početi zarađivati „tokene" bazirane na njihovom "IQ-u" (bodovi zarađeni za korisne doprinose) koji će predstavljati virtualne dionice platforme.

Theodor Forselius, suosnivač i izvršni direktor Everipedije, rekao je: „Sposobnost pojedinca da bude dionik u enciklopediji koju uređuje i da dobiva stvarnu novčanu vrijednost zauzvrat, je ideja koja me uzbuđuje."

Korisnici će morati platiti određeni polog prije nego što daju doprinose. Ako se smatra da su njihove izmjene netočne, izgubit će token, a oni čije su izmjene ispravne, dobit će originalni polog i dodatne tokene kao nagradu.

Forselius je također naveo dvije dodatne prednosti za premještanje Everipedije na blockchain. Jedna je da podaci više neće biti pohranjeni na centraliziranom poslužitelju, što znači da će opstati, čak i ako središnja organizacija, Everipedia, prestane postojati. Druga je činjenica da će podatke biti nemoguće cenzurirati, što znači da vlade koje trenutno provode cenzuru na Wikipediji (kao što su Turska i Iran) neće moći spriječiti korisnike da pridonose platformi.

6.9. Sektor osiguranja

Blockchain tehnologija nalazi mnoge primjene u sektoru osiguranja, s obzirom da se taj sektor temelji na ugovorima i povjerenju između dviju stranki.

Primjena blockchaina u ovom smislu značilo bi da na distribuiranoj knjizi mogu biti pohranjeni i ugovor o osiguranju i osobni podaci potrošača, dok potrošač kontrolira tko ima pristup. Podaci ostaju pohranjeni na korisnikovom osobnom uređaju i time se može ukloniti potreba za brokerima i drugim posrednicima između osiguravatelja i potrošača.

Prisutnost pametnih ugovora već se osjeća u sektoru osiguranja. Osiguravajuća kompanija AXA pokrenula je web stranicu Fizzy, koja osigurava potrošače od letova koji su odgođeni za dva ili više sati. Fizzy bilježi kupnju na Ethereum blockchainu i povezuje dobiveni pametni ugovor s globalnim bazama podataka o zračnom prometu. Ako se zabilježi dostatno kašnjenje, naknada se automatski isplati.

Dodatan primjer korištenja pametnih ugovora u sektoru osiguranja je kompenzacija poljoprivrednika u slučaju suše ili druge nepogode koja nanosi štetu njihovim posjedima.

6.10. Označavanje prehrambenih proizvoda

Označavanje prehrambenih proizvoda organskim je popularna marketinška taktika. Pitanje je što zapravo znače te oznake. Tko određuje je li nešto organsko, kako to rade i je li to pouzdano?

Postoje tvrtke poput Where Food Comes From (WFCF) koje potvrđuju zahtjeve za označavanje proizvoda. WFCF se usredotočuje na provjeru izvora hrane za mliječne proizvode, meso i proteine. U osnovi, testiraju različite tvrdnje na tržištu. Provjeravaju tlo kako bi bili sigurni da se proizvodi mogu označiti organskim te provjeravaju uvjete u kojim žive životinje.

Ali blockchain tehnologija će napraviti korak dalje, tjerajući prehrambenu industriju da udovoljava i propisima i potražnji potrošača. Standardi dobavljača i reputacija bazirana na blockchain tehnologiji osigurat će integritet marketinških tvrdnji. Postojeći certifikati i izvješća o reviziji objekata bit će registrirani na blockchainu kako bi dokazali spomenute tvrdnje.

Nakon što svi sudionici u opskrbnom lancu pristanu na ovu metodu, nagradit će se i dodatno naglasiti dobro ponašanje moralnih kompanija, uklanjajući one kompanije koje daju lažne tvrdnje ili pogrešno navode podrijetlo svojih proizvoda putem decentraliziranih sustava praćenja.

Ako potrošači znaju da su oznake na prehrambenim proizvodima određene kompanije potkrijepljene nepromjenjivim blockchain sustavom, njihovo povjerenje u te proizvode će nesumnjivo porasti.

6.11. Računovodstvo i revizija

Računovodstvo se bavi evidentiranjem ekonomskih transakcija subjekta na način koji je sukladan računovodstvenim standardima. Ti se zapisi dijele s dionicima poput investitora, vlada, banaka, itd. Ovdje je nastao problem kako ti dionici mogu vjerovati knjigama tvrtke.

Došlo je do pojave javnog revizora čija je uloga bila (i još jest) služiti kao neovisni jamac financijskih informacija. Dionici su svoje povjerenje stavljali ne u menadžment tvrtke, koji je imao interes prikazati stanje tvrtke bolje nego što ono stvarno jest, već u revizore koje je uprava zadržala da bi jamčila za njih. Ovaj aranžman nažalost stvara problem agencije. Rade li revizori za menadžere koji su ih zaposlili i plaćaju ih ili za javnost koja se oslanja na njihov integritet kako bi donosila odluke?

Iako postoje pravila koja to reguliraju, računovodstveni skandali koji su se dogodili u posljednjih 15 godina dokazuju da slika nije tako dobra kao što se čini. Jedno od mogućih rješenja ovog problema je blockchain tehnologija. Budući da je promjena transakcija, odnosno cijelih blokova, u blockchainu gotovo nemoguća, korištenje blockchain tehnologije omogućuje jednostavno dokazivanje integriteta elektroničkih datoteka. Jedan je pristup generiranje hash niza postojećih dokaza poput faktura. Taj niz hashova predstavlja digitalni otisak (eng. *fingerprint*) datoteke. Nadalje, taj otisak je nepromjenjivo vremenski ispisan tako što se upisuje u blockchain putem transakcije. U bilo kojem kasnijem trenutku, moguće je dokazati integritet te datoteke ponovnim generiranjem otiska i usporedbom s postojećim otiskom pohranjenim u blockchainu.

U slučaju da su otisci prstiju identični, dokument je ostao nepromijenjen od prvog generiranja hasha u blockchainu. Tvrtke bi od ovakve implementacije blockchain tehnologije imale mnoge koristi: Standardizacija bi omogućila revizorima da automatski provjeravaju veliki dio najvažnijih

podataka financijskih izvještaja. Trošak i vrijeme potrebno za obavljanje revizije znatno bi se smanjilo te bi se oslobođeno vrijeme moglo utrošiti na provjeru vrlo složenih transakcija ili na mehanizme interne kontrole.

6.12. E-glasanje

Upotrebom blockchain tehnologije spriječilo bi se varanje sustava od strane bilo kojeg sudionika, od samih glasača do brojitelja glasova. Blockchain tehnologija bi se pobrinula da pojedina osoba ne može glasati nekoliko puta jer drži nepromjenjivi zapis njihovog glasa i identiteta. Isto tako nitko nikada ne bi mogao izbrisati glasove jer je, kao što je rečeno, blockchain nepromjenjiv. Oni koji su zaduženi za prebrojavanje glasova imali bi konačni zapis o broju glasova kojeg bi mogli u svakom trenutku kontrolirati regulatori ili revizori. Na blockchainu sve je nepromjenjivo i provjerljivo. Važna je, međutim, činjenica da se rezultati mogu šifrirati što bi potaknulo transparentnost, istodobno zadržavajući ključni osjećaj privatnosti.

Rezultati uneseni i pohranjeni na blockchainu nisu samo nepromjenjivi i transparentni, već su također odmah dostupni. To znači da provođenje izbora na blockchainu nije samo sigurnije nego i učinkovitije od tradicionalnog.

7. ZAKLJUČAK

Blockchain tehnologija je u samim začetcima. Njen potencijal je ogroman, ali pitanje je koliko će biti prihvaćena u budućnosti i hoće li napraviti ikakve značajne promjene u svijetu. Ono što sa sigurnošću možemo reći je da je pojava blockchain tehnologije napravila revoluciju u mnogim područjima svijeta, pogotovo u financijskom i poslovnom svijetu.

Nakon dugog niza godina, napokon je dokazano da nema potrebe za posrednicima kod slanja i primanja transakcija te da nije potrebno vjerovati nikome da će se određena transakcija uspješno provesti. Sve ovo je moguće uz potpunu transparentnost, ali i, iako možda na prvi pogled kontradiktorno, uz očuvanje privatnosti. To znači da je lako provjeriti svaku transakciju i njenog pošiljatelja, odnosno primatelja, ali ne otkrivajući njihove stvarne identitete. Osim mogućnosti u financijskom sektoru, bitno je naglasiti i funkcije koje blockchain tehnologija nudi i u drugim sektorima pomoću, na primjer, pametnih ugovora. Ovdje se također uklanja potreba za posrednicima i vrlo se precizno sastavljaju i izvršavaju ugovori koji su sklopljeni.

Spomenute su i mogućnosti u pohrani dokumentacije, prijenosu vlasništva, glasanju i dijeljenju znanja. Osim navedenoga, podjednako su bitne i ostale primjene blockchain tehnologije o kojima je bilo riječi u prethodnim poglavljima i koje su vrlo lako ostvarive u skoroj budućnosti, a od kojih su neke već realizirane. Uz brojne mogućnosti blockchain tehnologije koje smo nabrojali, valja naglasiti da ista iziskuje mnogo resursa i da trenutno nije najisplativija opcija za realizaciju većine spomenutih tehnoloških unaprjeđenja. Radi se o potrošnji ogromnih količina računalne moći za provedbu i provjeru informacija.

Unatoč tome, blockchain tehnologija, kao i svaka druga tehnologija, će se razvijati i vrlo moguće smanjiti količinu resursa i energije potrebne za provođenje svojih funkcija. Ako se ovo pak ne dogodi, blockchain tehnologija je utkala put nekoj drugoj tehnologiji pokazavši mane sadašnjih sustava i metoda te dokazavši da ih je moguće savladati. Ne možemo znati što nas čeka u budućnosti i hoće li blockchain tehnologija kao takva opstati, no jasno je da je uspjela napraviti revoluciju u većini današnjih sustava te omogućila razvoj mnogih tehnologija koje su dosada bile nezamislive.

8. SAŽETAK

Blockchain tehnologija se može primijeniti ne samo za pružanje funkcionalnosti Bitcoin mreži i ostalim kriptovalutama, ali i za aplikaciju na druga pohranjiva sredstva: intelektualno vlasništvo, glazbu, osiguranje, fizičku robu i imovinu pa čak i korisničke podatke.

Ova tehnologija ima velike primjene i za industriju financijskih usluga. Za provedbu decentralizirane baze podataka ili javnog registra kao što je blockchain, kako bi se potvrdio identitet svih uključenih strana, više neće biti potrebno čekati da se transakcije odobre u razmaku od nekoliko dana. Provedba bi bila trenutna budući da će se i transakcija i nagodba dogoditi istodobno nakon što se glavna knjiga ažurira.

Jedna od najvećih upotreba blockchain tehnologije dolazi kod „menadžmenta identiteta“ (eng. *identity menagement*).

Radi se o ostavljanju digitalnih tragova s podatcima o osobama koji nisu u vlasništvu osoba o čijim se podatcima radi. Upravo blockchain tehnologija nudi mogućnost da se ti virtualni podatci vrate u pripadajući posjed i kako bi te iste osobe preuzele kontrolu nad njima.

Blockchain tehnologija, u osnovi, može promijeniti način na koji se razmjenjuje vrijednost i možda je upravo to razlog zašto se stvorio toliki entuzijazam i znatiželja da se sazna više.

Unatoč tome, blockchain tehnologija je još u početnim fazama i svijet svjedoči njenom razvijanju i ostvarenju punog potencijala.

Ključne riječi: blockchain tehnologija, kriptovalute, podatci

9. SUMMARY

Blockchain technology can be used not only to provide Bitcoin network's and other cryptocurrencies' functionality, but can also be applied to any asset: intellectual property, music, insurance, physical goods and property, and even user data.

This technology also has great implications for the financial services industry. On implementing a decentralized database or a public registry such as blockchain to verify the identities of all parties, no longer will we need to have our transactions stay "pending" for days. Settlement would be instantaneous since the transaction and settlement would happen simultaneously once the ledger is updated.

Perhaps the biggest use of blockchain technology is in „identity management".

Users leave digital traces with data about themselves, but they do not own said data. Blockchain technology offers the ability to bring this virtual data back to their rightful owners and to allow them to take control over it.

Blockchain technology can fundamentally change how we exchange value and, perhaps, this is the reason why such enthusiasm is present in the world with individuals longing to know more.

Nevertheless, blockchain technology is still in its nascent stages, and the world is just witnessing its development and full potential.

Keywords: blockchain technology, cryptocurrencies, data

10. LITERATURA

1. Admiral Markets (2017): Što je „Blockchain Fork“?, [Internet], raspoloživo na: https://admiralmarkets.com.hr/analytics/traders-blog/sto-je-blockchain-fork
2. Bitcoin Radionica (2017): Tko je izumitelj Bitcoina Satoshi Nakamoto?, [Internet], raspoloživo na: https://bitcoin-radionica.com/tko-izumitelj-bitcoina-satoshi-nakamoto/
3. Bitcoin Wiki (2010): Bitcoin, [Internet], raspoloživo na: https://en.bitcoin.it/wiki/Bitcoin
4. Bitcoin Wiki (2010): Difficulty, [Internet], raspoloživo na: https://en.bitcoin.it/wiki/Difficulty
5. Bitcoin Wiki (2011): How bitcoin works, [Internet], raspoloživo na: https://en.bitcoin.it/wiki/How_bitcoin_works
6. Bitcoin Wiki (2016): SHA-256, [Internet], raspoloživo na: https://en.bitcoin.it/wiki/SHA-256
7. Blockchain Expo (2018): How will blockchain impact the insurance sector?, [Internet], raspoloživo na: https://www.blockchain-expo.com/2018/02/blockchain/blockchain-insurance/
8. Blockchain Review (2018): Ethereum White Paper Made Simple, [Internet], raspoloživo na: https://blockchainreview.io/wp-content/uploads/2018/03/02.01._final_Ethereum-White-Paper-Made-Simple.pdf
9. Blockonomi (2018): Best Bitcoin Wallets 2018: Hardware vs Software vs Paper, [Internet], raspoloživo na: https://blockonomi.com/best-bitcoin-wallets/
10. BTC Croatia (2014): Merkleovo stablo, [Internet], raspoloživo na: http://btc-croatia.blogspot.com/2014/04/merkleovo-stablo.html
11. Centar Informacijske Sigurnosti (2007): Digitalni potpis, [Internet], raspoloživo na: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2007-02-182.pdf
12. CoinCentral (2018): Making Sense of Proof of Work vs Proof of Stake, [Internet], raspoloživo na: https://coincentral.com/making-sense-of-proof-of-work-vs-proof-of-stake/
13. Forbes (2018): 3 Innovative Ways Blockchain Will Build Trust In The Food Industry, [Internet], raspoloživo na: https://www.forbes.com/sites/samantharadocchia/2018/04/26/3-innovative-ways-blockchain-will-build-trust-in-the-food-industry/#285bfa832afc

14. Hacker Noon (2018): How Blockchain Will Make Electronic Voting More Secure, [Internet], raspoloživo na: https://hackernoon.com/how-blockchain-will-make-electronic-voting-more-secure-fba15d752bee
15. Harvard Business Review (2017): How Blockchain Is Changing Finance, [Internet], raspoloživo na: https://www.bedicon.org/wp-content/uploads/2018/01/finance_topic2_source2.pdf
16. Lisk (2018): What is Decentralization in Blockchain, [Internet], raspoloživo na: https://lisk.io/academy/blockchain-basics/benefits-of-blockchain/what-is-decentralization
17. Medium (2017): Blockchain Advantage and Disadvantages, [Internet], raspoloživo na: https://medium.com/nudjed/blockchain-advantage-and-disadvantages-e76dfde3bbc0
18. Object Computing (2017): 8 ways blockchain is changing the world, [Internet], raspoloživo na: https://objectcomputing.com/news/2017/12/20/8-ways-blockchain-changing-world
19. Quora (2017): How will blockchain impact accounting, auditing & finance?, [Internet], raspoloživo na: https://www.quora.com/How-will-blockchain-impact-accounting-auditing-finance
20. TechGenix (2018): Blockchain technology: Why it will change the world, [Internet], raspoloživo na: http://techgenix.com/blockchain-technology/
21. WhiteHat Security (2016): Blockchain Technology Explained – An Executive Summary, [Internet], raspoloživo na: https://www.whitehatsec.com/blog/blockchain-technology/
22. Wikipedia (2001): Hash function, [Internet], raspoloživo na: https://en.wikipedia.org/wiki/Hash_function
23. Wikipedia (2002): Endianness, [Internet], raspoloživo na: https://en.wikipedia.org/wiki/Endianness
24. Wikipedia (2004): Hashcash, [Internet], raspoloživo na: https://en.wikipedia.org/wiki/Hash_function
25. Wikipedia (2010): Satoshi Nakamoto, [Internet], raspoloživo na: https://en.wikipedia.org/wiki/Satoshi_Nakamoto
26. Wikipedia (2012): Cryptocurrency, [Internet], raspoloživo na: https://en.wikipedia.org/wiki/Cryptocurrency

27. Wikipedia (2014): Blockchain, [Internet], raspoloživo na: https://en.wikipedia.org/wiki/Blockchain
28. Wikipedia (2017): Cryptocurrency wallet, [Internet], raspoloživo na: https://en.wikipedia.org/wiki/Cryptocurrency_wallet
29. Wiley Online Library (1994): Cryptographic hash functions, [Internet], raspoloživo na: https://onlinelibrary.wiley.com/doi/abs/10.1002/ett.4460050406