# Primjena blockchain tehnologija u nefinancijske svrhe

**Cota, Ivan**

SVEUČILIŠTE U ZAGREBU

FILOZOFSKI FAKULTET

ODSJEK ZA INFORMACIJSKE I KOMUNIKACIJSKE ZNANOSTI

Ak. god. 2020./2021.

Ivan Cota

# Primjena blockchain tehnologija u nefinancijske svrhe

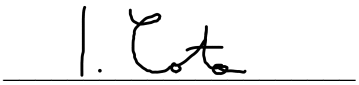
Završni rad

Mentor: dr. sc. Nikolaj Lazić, red. prof.

Zagreb, rujan 2021.

# Izjava o akademskoj čestitosti

Izjavljujem i svojim potpisom potvrđujem da je ovaj rad rezultat mog vlastitog rada koji se temelji na istraživanjima te objavljenoj i citiranoj literaturi. Izjavljujem da nijedan dio rada nije napisan na nedozvoljen način, odnosno da je prepisan iz necitiranog rada, te da nijedan dio rada ne krši bilo čija autorska prava. Također izjavljujem da nijedan dio rada nije korišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.



(potpis)

*Zahvaljujem se baki Nedi, didu Stanku i majci Aniti, za svesrdnu podršku u svim trenutcima studiranja.*

# Sadržaj

# 1. Uvod

U posljednjih desetak godina (točnije od 2008.) postupno u svakodnevni rječnik ulaze pojmovi poput *bitcoin, blockchain, kriptovalute, pametni ugovori, ethereum, digitalni tokeni, distribuirane knjige* itd. Rijetko tko danas nije čuo barem za *bitcoin*. Što ustvari znače svi ti pojmovi i odakle dolaze će se objasniti u uvodnom dijelu rada, a prije nego što se razmotri primjena tih tehnologija u nefinancijske svrhe, bit će navedene jednostavne definicije pojmova. Nakon objašnjenja osnovnih pojmova, u prvom dijelu rada će se iznijeti tehnološke pretpostavke ideje *blockchain*-a na jednostavan način, bez ulaženja u tehničke detalje. Pokazat će se na primjeru *bitcoina* kako funkcionira *blockchain* tehnologija i zašto je doživjela toliku popularnost da postoji realna opcija da bi mogla zamijeniti jedan od najstarijih izuma civilizacije - novac. U drugom dijelu rada će se iznijeti trenutne i buduće primjene tehnologije u nefinancijske svrhe, navesti prednosti i mane *blockchain*-a i sličnih sustava (IOTA) te njihove glavne pobornike u tehnološkom svijetu. U zaključku će se pokušati deducirati što nam je točno donijela ta nova tehnologija i koliko su realne šanse da bude revolucionarna i u kojem pogledu, kroz trenutne trendove i pokazatelje. Je li oko svega stvorena prenapuhana fama ili je zaista ideja iza *blockchain*-a nositelj korjenitih promjena u načinu funkcioniranja civilizacije, vjerojatno nećemo uspjeti odgovoriti, već nam to ostaje za vidjeti.

## 1.1 Osnovni pojmovi

U ovome poglavlju će biti navedene definicije i objašnjenja nekih tehnologija i pojmova koje su ključne za daljnje razumijevanje rada.

### 1.1.1 *Blockchain*

Osnovni pojam ovog rada - *blockchain* ima dvojno značenje u hrvatskoj i engleskoj literaturi. Može biti naziv za digitalnu bazu podataka ili se odnositi na samu tehnologiju koja tu bazu podataka koristi. Stoga, da ne bi došlo do zabune, u daljnjem tekstu će se pisati *„blockchain"* kada se odnosi na prvo značenje, tj. bazu podataka, a *„blockchain tehnologija"* kada se pojam odnosi na pozadinsku tehnologiju koja koristi istoimenu bazu. Iduće dvije definicije razjašnjavaju razliku:

*"**Blockchain** je digitalna baza podataka koja sadrži informacije (poput zapisa o financijskim transakcijama) koje se mogu istodobno koristiti i dijeliti unutar velike decentralizirane, javno dostupne mreže, također: tehnologija korištena pri stvaranju takve baze"*[1] (Merriam-Webster, 2021)

*„...je decentralizirani sustav elektroničke knjige koji stvara kriptografski siguran i nepromjenjiv zapis o svakoj transakciji vrijednostima, bilo da se radi o novcu, robi, imovini, radu ili glasovima."*[2] (World Economic Forum, 2018)

### 1.1.2 **Kriptovalute**

Prema definiciji Merriam-Webster online rječnika kriptovaluta je:

*„bilo koji oblik valute koji postoji samo digitalno, koji obično nema središnje tijelo koje ga izdaje ili regulira, već umjesto toga koristi decentralizirani sustav za bilježenje transakcija i upravljanje*

[1] Prijevod autora. Tekst u izvorniku glasi: „ a digital database containing information (such as records of financial transactions) that can be simultaneously used and shared within a large decentralized, publicly accessible network also **:** the technology used to create such a database"

[2] Tekst u izvorniku glasi: „It is a decentralized electronic ledger system that creates a cryptographically secure and immutable record of any transaction of value, whether it be money, goods, property, work or votes.

*izdavanjem novih jedinica, a koje se oslanja na kriptografiju za sprječavanje krivotvorenja i prijevara"*[3] (Merriam-Webster, 2021)

Uz tu definiciju, kriptovalute najjednostavnije možemo shvatiti kao digitalne „novčiće" koji se primaju i šalju između korisnika, s njima se plaća i čuvaju se u posebnom novčaniku (engl. *cryptocurrency wallet*). Vrijednost svake pojedine kriptovalute varira na dnevnoj bazi, kao što varira npr. cijena dionica, pa se kaže da su kriptovalute nestabilne.

### 1.1.3 **Bitcoin**

Bitcoin (valutni kod BTC) je prva i najpoznatija kriptovaluta koja je nastala 03.01.2009., kad je Satoshi Nakamoto (alias nepoznatog autora ili grupe autora) osmislio sustav, pokrenuo ga i „izrudario" prvi (nulti) blok, te mu dodijelio vrijednost od 50 bitcoina (Nakamoto, 2009). Uzevši u obzir da je *blockchain* ranije definiran kao digitalna baza podataka koja sadrži nepromjenjive informacije, sada se može reći da je bitcoin ustvari vrijednost dodijeljena binarnim skupovima podataka na *blockchain* bitcoin mreži. To je potpuno digitalna, virtualna valuta koja nema nikakav fizički oblik ni vrijednost i nitko ju ne nadzire, za razliku od klasičnih državnih valuta. Nastao je kao odgovor na problem „dvostrukog trošenja" (engl. *„double spending problem"*) o čemu će biti riječi kasnije u tekstu. Prvenstveno se koristi za ulaganja i naziva se „digitalnim zlatom", dok je razmjena vrijednosti bitcoinom kroz plaćanja još uvijek minorna naspram klasičnog novca.

### 1.1.4 **Pametni ugovori**

Pametni ugovori (engl. *„smart contracts"*), kako ih opisuje autor ideje Nick Szabo, su računalni protokoli koji izvršavaju uvjete postavljene u ugovoru, te navodi da se neke današnje tehnologije poput transakcija preko POS uređaja i kartičnog plaćanja mogu smatrati rudimentarnim pametnim ugovorima (Szabo, 1994). Ti računalni programi ili rezultati dobiveni transakcijskim protokolima, tj. pametni ugovori se mogu spremiti na *blockchain*

[3] Tekst u izvorniku glasi: „any form of currency that only exists digitally, that usually has no central issuing or regulating authority but instead uses a decentralized system to record transactions and manage the issuance of new units, and that relies on cryptography to prevent counterfeiting and fraudulent transactions

mrežu gdje upotrebom kriptografskih metoda koje će kasnije biti opisane, postaju potpuno sigurni od bilo kakvog daljnjeg manipuliranja ili krivotvorenja. Najjednostavnijim rječnikom, to su bilo kakvi ugovori između dviju ili više strana čija se autentičnost osigurava *blockchain* tehnologijom.

### 1.1.5 Internet stvari i IOTA

IOTA je distribuirana knjiga (engl. *„distributed ledger"*) koja se koristi za mikrotransakcije u okružju *„interneta stvari"*. Internet stvari je pojam koji se odnosi na globalnu mrežu svih uređaja koji se mogu povezati na Internet, primjerice računala, printeri, pametni telefoni, mrežna infrastruktura, pa sve do kućanskih uređaja poput televizije, hladnjaka ili klima uređaja. Kako je broj uređaja u takvom okruženju ogroman, a razmjena informacija između njih proporcionalno uvećana, sigurnu komunikaciju i potvrđivanje ranije spomenutih pametnih ugovora nije bilo realno riješiti *blockchain* tehnologijom. Kako navodi autor Sergej Popov, glavni problem zašto *blockchain* tehnologiju nije bilo moguće primijeniti na ekosustav interneta stvari je zbog toga što *blockchain* ima implementiran „*transaction fee*", odnosno naknadu za transakciju obavljenu na mreži (Popov, 2018). Stoga je razvijen sustav nazvan „The Tangle", koji ustvari ne počiva na *blockchain* tehnologiji, već na ideji usmjerenih acikličnih grafova (engl. „*Directed Acyclic Graphs*", skraćeno; DAG)[4]. Tehnologija usmjerenih acikličnih grafova (kasnije DAG) se smatra prirodnom nadogradnjom *blockchain*-a. *Blockchain*, Ethereum mrežu, DAG sustave i sve slične decentralizirane sustave zajednički nazivamo "tehnologije raspodijeljenih/distribuiranih knjiga" (engl. *Distributed Ledger Technologies; DLT*).

IOTA i njena kriptovaluta nazvana „mIOTA", iako ne počivaju na *blockchain* tehnologiji, autori smatraju idućim korakom evolucije *blockchain*-a (Popov, 2018) te ih stoga moramo spomenuti zbog kasnijih referenci. Recimo još samo da naziv potječe od slova grčkog alfabeta jota koje označava beskonačno malu količinu nečega, što se savršeno uklopilo zbog sličnosti sa akronimom *IoT* za internet stvari i sa već spomenutim problemom transakcijske naknade

[4] Za teoretsko objašnjenje usmjerenih acikličnih grafova se predlaže: https://www.fer.unizg.hr/_download/repository/Osnovni_pojmovi-teorija_grafova.pdf

koja bi bila veća od vrijednosti prenesenih podataka, te je stoga upotreba *blockchain* tehnologije bila nelogična.

### 1.1.6 **Ethereum**

Ethereum je *blockchain* platforma sa svojom istoimenom kriptovalutom (Ethereum, Ether ili ETH) i svojim vlastitim programskim jezikom nazvanim Solidity, koji je stvoren isključivo za pisanje aplikacija, programa ili ranije spomenutih pametnih ugovora direktno na Ethereum *blockchain* mrežu. Kao svojevrsna nadogradnja Nakamotove ideje *blockchain*-a, Ethereum se ponekad naziva i „*blockchain 2.0*“. Osnivač Ethereuma, Vitalik Buterin kao glavne prednosti nad prijašnjom *blockchain* tehnologijom navodi koncept proizvoljne funkcije prijelaza stanja (Buterin, 2021), ugradnju Turing-potpunog programskog jezika, te izmijenjenog protokola tzv. „Merkle stabla“ (engl. *Merkle trees*), koji osim zapisa transakcije, ima mogućnost pohrane transakcije, stanja i računa kroz 4 različite verzije tih stabala (Gensler, 2018)

Ono što je autor ustvari htio postići je da njegova mreža ne bude samo podloga za razmjenu malih količina podataka *P2P*[5], već da se može slati i primati sve što se može pretočiti u Solidity kod, a kako je Solidity Turing-potpun programski jezik, mogućnosti su skoro neograničene. Na Ethereum se mogu postaviti digitalni tokeni[6], program, protokol, aplikacija, pa čak i sadržaj poput računalnih igara čija bi pravila onda korisnici mogli sami kreirati. Za razliku od IOTA-e i Tangle sustava, Ethereum je ipak prava *blockchain* tehnologija koja je zanimljivija zbog puno šire mogućnosti primjene u nefinancijske svrhe.

[5] *P2P* (engl. *peer-to-peer*) je koncept dijeljenja datoteka između dvaju računala (klijenta) direktno, bez potrebe za serverom. To se razlikuje od arhitekture klijent – poslužitelj (engl. *client – server*), u kojoj su neka računala posvećena služenju ostalima

[6] Digitalni token kao kriptovaluta

# 2. Tehnološki aspekti *blockchain*-a

S tehničke strane, *blockchain* spada u domenu računarske znanosti, a hrvatski naziv za *blockchain* je *tehnologija (povezanih) blokova*. Zbog praktičnosti originalnog izraza preuzetog iz engleskog jezika, u radu će se koristiti izraz *blockchain* (i neki drugi izrazi neprevodivih termina), poštujući hrvatsku računalnu terminologiju gdje god je to moguće.

## 2.1 Problem Bizantskih generala i dvostrukog trošenja

Problem Bizantskih generala su prvi puta predstavili Shostak, Lamport i Pease 1982. i ponudili rješenje za njega, nakon čega je kasnije puno puta revidiran sa raznim rješenjima, te je još uvijek zanimljiv u računarstvu. To je ustvari alegorija u kojoj generali predstavljaju čvorove u nekoj mreži računala, a problem nastaje kada ti decentralizirani čvorovi pokušaju postići konsenzus oko neke odluke. Zamislimo da se ispred neprijateljske utvrde nalazi nekoliko jedinica bizantske vojske na suprotnim stranama, udaljeni jedni od drugih, te da ne mogu komunicirati direktno, već samo putem glasnika. Dva su pozitivna ishoda u razrješenju situacije: svi generali (ili dovoljna većina) napadaju ili svi generali (ili dovoljna većina) se povlače. Jedan zapovjednik mora donijeti odluku hoće li napasti ili se povući i tu odluku komunicirati ostatku generala. Glavni problem je ustvari kako osigurati konsenzus, tj. kako biti siguran da su svi generali primili zapovjedi i da će ih izvršiti, te kako osigurati uspješnu strategiju iako su neki od generala možda izdajice i neće postupiti onako kako im je naređeno, te će možda drugim generalima namjerno prenijeti krivu poruku? Shostak i drugi pokazuju matematičkim (algoritamskim) modelom da je potrebno da omjer izdajica i onih koji izvršavaju zapovijed bude najmanje 1:2, tj. da iskreni generali budu u dvotrećinskoj većini, u protivnom strategija propada (Lamport, Shostak, & Pease, 1982). Ovaj problem je kasnije postao jedan od osnovnih koncepata na koji se obraća pozornost pri dizajniranju decentraliziranih komunikacijskih sustava, te novija rješenja predlažu kriptografske metode zaštite sadržaja poruke, pri čemu dvotrećinska većina iskrenih čvorova (generala) više nije nužna. Primjerice, moderni sustavi kontrole leta zrakoplova i svemirskih misija u zemljinu orbitu koriste komunikacijske sustave koji su otporni na problem bizantske greške (engl. *Byzantine fault tolerant*), najčešće koristeći se redundancijom u slanju poruka kako posljedice krivih instrukcija ne bi bile katastrofalne (Lamport, Shostak, & Pease, 1982).

Iako *blockchain* tehnologija u principu nudi rješenje za problem Bizantskih generala, u inicijalnom radu Satoshija Nakamota (Nakamoto, 2009) se odgovara na jedan drugi problem koji je više financijske prirode - problem dvostrukog trošenja. Problem dvostrukog trošenja se ne može dogoditi u novčanim transakcijama sa fizičkim valutama, jer ako je negdje potrošena jedna novčanica neke valute, ona više nije fizički kod vlasnika i ne raspolaže njome. Stoga je taj problem rezerviran samo za digitalne, odnosno virtualne valute (poput svih kriptovaluta i kartičnih transakcija). Digitalna vrijednost novca i digitalni zapis transakcije je ustvari skup binarnih podataka koji je pohranjen na nekoj mreži ili lokalnom računalu pa se stoga kao i svaki drugi digitalni sadržaj može proizvoljno umnažati, gdje je svaka kopija istovjetna originalu. Stoga ako se potroši neki iznos digitalnog novca, teoretski; taj isti iznos se može ponovno generirati i izbrisati podatak o transakciji, iz čega će kasnije biti nemoguće dokazati da iznos nije već potrošen. Iz tog razloga, ovaj problem se danas u najvećem broju slučajeva rješava centralnim autoritetom. Banke i kartične kuće predstavljaju taj centralni autoritet i preuzimaju odgovornost za kontrolu i nadgledaju sve transakcije i stanja računa korisnika. Satoshi Nakamoto je ideju *blockchain*-a i bitcoina predstavio kao rješenje za problem dvostrukog trošenja u decentraliziranim sustavima, oslanjajući se na neke prijašnje ideje koje ipak nisu doživjele takvu popularnost (DigiCash, B-Money, Bit Gold)[7].

## 2.2 Bitcoin: Peer-to-peer elektronički gotovinski sustav[8]

Kako je ranije spomenuto, glavna prepreka potpuno decentraliziranom sustavu transakcija i digitalnih valuta je bio problem dvostrukog trošenja, odnosno konsenzusa oko izvršenja transakcija. Satoshi Nakamoto kao rješenje predlaže *blockchain* sustav koji se bazira na kriptografskim metodama umjesto na povjerenju između čvorova i centralnom autoritetu:

*„What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party.“*

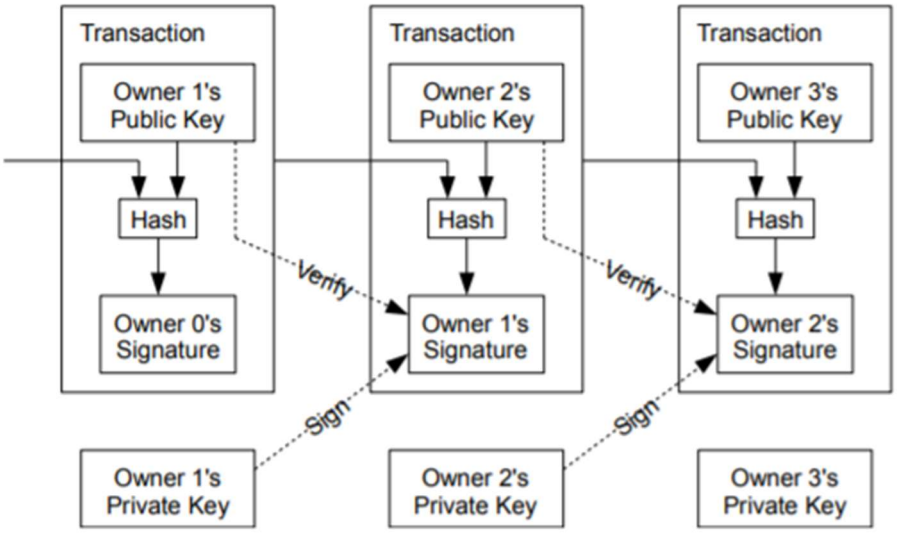
*„… we propose a solution to the double-spending problem using a peer-to-peer distributed*

[7] Preporuča se vidjeti objašnjenje na: https://academy.ivanontech.com/blog/byzantine-generals-problem-an-introduction

[8] Prijevod autora. Tekst u originalu glasi: *„Bitcoin: A Peer-to-Peer Electronic Cash System“*

*timestamp server to generate computational proof of the chronological order of transactions.“* (Nakamoto, 2009, str. 1)

Elektronički novac se definira kao lanac digitalnih potpisa. Svaki digitalni potpis se putem *„hash funkcije“*[9] pretvara u jedinstven podatak u binarnom zapisu, kojega koristi idući blok u mreži, te nakon što provjeri ispravnost zapisa svojim privatnim ključem, na njega dodaje javni ključ idućeg bloka i *hash*[10] na kraj zapisa. Taj zapis onda provjerava idući čvor u mreži svojim privatnim ključem i ponavlja postupak, što rezultira lancem blokova; otud naziv *blockchain*. Pošto još nije riješen problem dvostrukog trošenja jer idući blok u lancu ne može biti siguran da prethodni nije više puta napravio istu transakciju, Nakamoto uvodi nekoliko mehanizama koji otežavaju dvostruko trošenje do razine gotovo potpune sigurnosti. Prvi od njih je tzv. „*timestamping*“. To je ustvari mehanizam kojeg obavlja neki *blockchain* čvor (engl. *node*), koji svakom *hash*-u dodaje vrijeme nastanka i javno ga objavljuje, te time dokazuje da je neki *hash* nastao prije ili poslije nekog drugog. Ako netko želi modificirati, tj. lažirati *blockchain* transakcije, prvo treba izmijeniti podatke u *timestamp* dijelu *hash*-a, što je kao i u slučaju drugih mehanizama sigurnosti *blockchain*-a, iznimno računalno zahtjevan posao.




Slika 1. Dijagram ulančanog generiranja *blockchain* transakcija (*hash*-eva) (Nakamoto, 2009, str. 2)

[9] *Hash funkcija* je svaka funkcija koja se može koristiti za mapiranje podataka proizvoljne veličine u zapis fiksne veličine (https://en.wikipedia.org/wiki/Hash_function)

[10] *hash*-om skraćeno nazivamo podatak koji smo dobili primjenom hash funkcije

Slika 1., preuzeta iz originalnog rada ilustrira ovaj "lanac vlasništva" jer se novčići (bitcoini) prenose s vlasnika 1 na vlasnika 2, pa na vlasnika 3 itd. Transakcije se bilježe javno u blokovima, dok se privatni ključevi drže u tajnosti za svakog vlasnika. Drugi mehanizam osiguravanja podataka Nakamoto naziva „proof-of-work“. U suštini, proof-of-work (skraćeno PoW) je metoda dokazivanja istinitosti lanca podataka (blokova transakcija) prema kriteriju uložene računalne snage. Cilj PoW-a je uspješno dodati novi blok transakcija u *blockchain* i za to dobiti nagradu u obliku novih bitcoina. Da bi računalo dodalo novi blok transakcija, mora u taj blok zapisati broj koji se zove „*nonce“*. *Nonce* je broj na koji se zajedno s identifikatorom bloka primjeni SHA-256 algoritam i dobije se novi *hash* identifikator. Cilj rudarenja je naći broj *nonce* takav da primjena SHA-256 algoritma producira *hash* koji počinje s određenim brojem nula. Računalo nema nikakvu mogućnost doći do tog *hash*-a osim probati svaku kombinaciju broja *nonce* dok mu se ne posreći i nađe takav *nonce* koji odgovara zadanom kriteriju (broj nula na početku *hash*-a). U prosjeku potrebno je isprobati različiti *nonce* broj nekoliko milijardi puta prije nego se dobije *hash* koji zadovoljava uvjete. To se obavlja sad već iznimno popularnim „*rudarenjem“*- procesom koji koristi ogroman broj osobnih ili posebnih računala čiji se procesori koriste isključivo za mukotrpno izračunavanje i provjeru *hash* vrijednosti transakcija. Rudarenje je trenutno najveća kritika *blockchain* bitcoin mreže, zbog upotrebe ogromnih količina električne energije za svrhe koje nisu svima potpuno jasne i imaju neizvjesnu budućnost. U narednim poglavljima će se pokazati kako taj „proof-of-work“ sustav nije jedino, već jedno od nekoliko rješenja dokazivanja istinitosti lanca transakcija.

Bitcoin *blockchain* mreža funkcionira u nekoliko koraka (Nakamoto, 2009):

1. Nove transakcije (*hash*-evi) se odašilju svim čvorovima
2. Svaki čvor sprema te transakcije u blok
3. Svaki čvor zasebno radi proof-of-work metodom na tom bloku
4. Prvi čvor koji nađe vrijednosti koje odgovaraju proof-of-work zadatku (počinje li *hash* sa određenim brojem nula) odašilje taj blok svim čvorovima u mreži
5. Čvorovi prihvaćaju blok samo ako su sve transakcije u njemu ispravne, tj. ako nije došlo do dvostrukog trošenja
6. Čvorovi počinju raditi na idućem bloku u nizu, koristeći *hash* iz bloka kojeg su dobili u koraku 4 da bi stvorili idući *hash*, ponovno proof-of-work metodom

Ako se dogodi da se istovremeno odašilju dva bloka na mrežu kao ispravna, čvorovi uzimaju kronološki prvi blok kao istinit i počinju raditi na njemu. Ako se pokaže da su sve transakcije

na tom bloku ispravne i ako se nađe idući blok, lanac se nastavlja i to postaje istinita vrijednost, pa se time drugi blok koji je prihvaćen i sporije procesuiran odbacuje. Kako ga više niti jedan čvor ne računa, *hash*-evi iz tog bloka se ne mogu kasnije naći u lancu.

Jednostavno rečeno, sigurnost mreže i ispravnost zapisa o svim transakcijama se osigurava računalnom snagom. Kada bi netko htio izmijeniti podatak o nekoj prethodnoj transakciji, morao bi pronaći *hash* vrijednosti za sve buduće blokove na mreži, prije svih ostalih čvorova. To se može postići isključivo time da jedan korisnik drži više od 50% računalne moći mreže, što je više-manje nemoguće i toliko bi destabiliziralo sustav (time i bitcoin kao valutu) da se ne bi isplatilo (Nakamoto, 2009).

Nameće se pitanje; koju korist imaju čvorovi (računala) koji troše vlastite resurse od tog mukotrpnog provjeravanja vrijednosti, odnosno od osiguravanja mreže? Naknadu u obliku bitcoin kriptovalute. Svako računalo koje sudjeluje u procesu ima svoju javnu adresu, na koju mu se dodijeli određena količina bitcoina izračunata prema tome koliko je pridonio ukupnom radu na mreži. U početku, kada je tehnologija bila u povojima, čvor koji prvi nađe ispravan blok, dobiva određen iznos bitcoina na svoju adresu, kada se taj blok provjeri i potvrdi određen broj puta. Kako je snaga mreže rasla, svaki čvor je imao sve manji i manji udio, te se danas ti čvorovi (računala) udružuju u tzv. *„bazen“* (engl. *pool*). Kada jedno računalo iz bazena pronađe ispravan blok, javna adresa bazena dobije nagradu u obliku bitcoina, te ravnomjerno raspodjeljuje svim računalima u bazenu, prema količini uložene računalne moći (i vremena). Ta računalna moć primijenjena u određenom vremenu se također naziva *hash* (skraćeno *Hs*), i obično se izražava u MH/s, GH/s ili TH/s (mega, giga ili tera *hash*), ovisno o snazi računala ili računalnog bazena. Spomenimo još da je težina zadatka dinamična, tj. da se mijenja pri svakom novom izračunatom bloku u ovisnosti o trenutnoj snazi mreže, na način da se primjerice; u jednom bloku traži da prvih 30 znamenki *hash*-a budu 0, a na nekom drugom 28. Tim mehanizmom mijenjanja se održava otprilike konstantno vrijeme pronalaska jednog ispravnog bloka, koje danas odgovara oko 10 minuta. Satoshi Nakamoto je odmah u početku predvidio da ako se tehnologija bude primjenjivala u financijske svrhe, da bi moglo biti ogromnih problema ako se dopusti neograničeno generiranje blokova, a time i neograničeno generiranje bitcoina. To bi rezultiralo bezvrijednošću valute nakon nekog vremena. Primijenio je jednostavnu jednadžbu[11] koja se odnosi na nagrade koje mreža prima u obliku bitcoina za svaki

[11] Za više detalja i algoritmu koji kontrolira konačan maksimalan broj bitcoina na mreži pogledati poveznicu: https://en.bitcoin.it/wiki/Controlled_supply

pronađeni blok. Prema algoritmu u osnovnom kodu bitcoin *blockchain*-a, nagrada za rudare na mreži koji su pronašli blok se prepolavlja svakih 210.000 blokova ili otprilike svake 4 godine. Prva nagrada je iznosila 50 bitcoina za prvo razdoblje od 210.000 izrudarenih blokova. U vrijeme pisanja ovog rada trenutna nagrada za svaki blok iznosi 6.25 bitcoina, što znači da se nalazimo u četvrtoj eri mreže. Daljnjim prepolavljanjem nagrade, nakon 32 generacije (ere mreže) će vrijednost nagrade za svaki blok pasti ispod 0.00000001 ($10^{-8}$ bitcoina), te će se izrudariti svi mogući bitcoini, njih nešto više od 21 milijun. Kako se mreža približava toj brojci, vrijednost bitcoina izražena u standardnim valutama raste gotovo nevjerojatno posljednjih 12 godina.

# 3. Primjena u nefinancijske svrhe

Bitcoin i Ethereum pozadinske tehnologije, tj. njihove *blockchain*-e se ponekad uspoređuje sa generacijama računala. Ako je Bitcoin kalkulator, Ethereum je stolno računalo. Tolika je nadmoć tih novih karakteristika *blockchain*-a 2.0, koji predovodi tehnologiju distribuiranih knjiga u iduće poglavlje.

## 3.1 Ethereum i „dApps“ - *blockchain* 2.0

Kako je ranije navedeno (vidi 1.1.5. i 1.1.6), Ethereum i IOTA mreže nisu tehnologije istovjetne inicijalnom bitcoin *blockchain*-u, već se mogu smatrati nadogradnjom *blockchain* tehnologija. Ethereum se često naziva “*blockchain* 2.0” po uzoru na programersku notaciju verzija softvera.

*Blockchain* 2.0 se nadovezuje na ideju razmjene vrijednosti na principu ravnopravnosti i decentraliziranosti. U Nakamotovoj *blockchain* mreži (*„blockchain 1.0“*) vrijednost koja se prenosi na mrežu je u obliku kriptovaluta. S *Blockchain*-om 2.0, prenesena vrijednost je programibilna transakcija u obliku pametnih ugovora. Kombiniranjem pametnih ugovora s *blockchain* tehnologijom stvara se moćna mreža računala koja je decentralizirana i otporna na napade zlućudnih strana ili cenzuriranje od strane autoriteta. Ethereum kao i Bitcoin *blockchain* trenutno koristi proof-of-work metodu potvrde ispravnosti transakcija. Zbog sve veće popularnosti tehnologije i sve više aplikacija (programa) koji se izvode na mreži, broj transakcija raste proporcionalno te to trenutno rezultira zagušenjem i sporim izvođenjem transakcija. Stoga, Ethereum tim predvođen Vitalikom Buterinom predlaže prelazak sa proof-of work na *„proof-of-stake“* metodu provjere ispravnosti transakcija. Za razliku od proof-of-work principa, proof-of-stake (PoS) se dosta razlikuje u načinu na koji postiže globalni konsenzus. Umjesto da se rudari natječu za nagradu za svaki izrudareni blok, proof-of-stake zahtijeva od mrežnih validatora da osiguraju određenu količinu sredstava kao osiguranje od zlonamjernog ponašanja. Sa sigurnim pohranjivanjem ovih sredstava, validatori mreže mogu početi provjeravati transakcije. Odluče li lagati o valjanosti transakcije, drugi će validatori saznati, a mreža će lažnom validatoru oduzeti uložena sredstva (u obliku Ether tokena, tj. ETH). To stvara poticaj mrežnim validatorima da se suzdrže od plasiranja lažnih transakcija, te bi s dovoljno velikom mrežom, osigurali sigurnost mreže na gotovo istoj razini kao i proof-of-work metodom. Za razliku od PoW-a, nema rudarenja koje intenzivno troši resurse, te bi takav

princip mogao puno brže izvoditi transakcije i bio bi ekonomski isplativiji. Još jedna krucijalna prednost Ethereuma nad *blockchain*-om 1.0 su tzv. "*dApps"*. Decentralizirana aplikacija ili *„dApp"* je aplikacija ili program čiji se pozadinski kod (engl. *backend code*) izvodi na decentraliziranoj P2P mreži, poput *blockchain*-a. Korisničko sučelje (engl. *frontend, user interface*) takvih aplikacija može biti pisano u bilo kojem programskom jeziku koji ima mogućnost pozivanja pozadinske aplikacije na *blockchain*-u. Takve aplikacije sa stajališta korisnika vrlo nalikuju klasičnim web aplikacijama (poput Google aplikacija ili WhatsApp Weba). Developeri Ethereum organizacije iznose 4 glavne karakteristike dApps-a (ethereum.org):

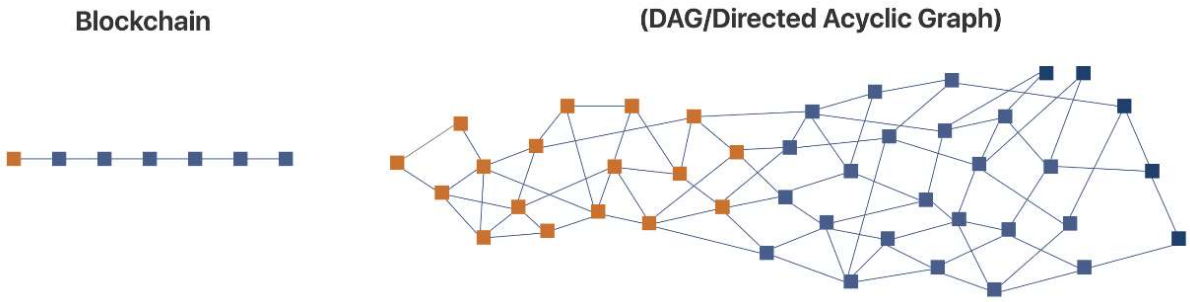
- Aplikacije su decentralizirane, što znači da ih nitko direktno ne posjeduje ili kontrolira, tj. da su nezavisne
- Izvode istu funkciju neovisno o okruženju, pa se kaže da su determinirane
- Turing-potpune su, odnosno nemaju restrikcija jer se može definirati bilo što
- Izolirane su, što znači da ako neki pametni ugovor ima određenu grešku, njegovo izvođenje neće utjecati na normalno funkcioniranje mreže, pošto se aplikacije izvode u virtualnom okruženju zvanom *„Ethereum Virtual Machine"*(EVM)[12]

Nepromjenjivost pametnih ugovora je najveća prednost decentraliziranih aplikacija, a ujedno i najveća mana. Ako se otkrije bug (greška) u ugovoru, ne može se izmijeniti već je potrebno ponovo programirati aplikaciju.

## 3.2 Usmjereni aciklični grafovi – IOTA i „The Tangle" sustav

*Blockchain* tehnologija koju koristi Bitcoin i ona koju koristi Ethereum (*blockchain* 1.0 i 2.0) za razliku od IOTA sustava koriste *blockchain* princip izvođenja transakcija te su time ograničene u svojoj upotrebi (*blockchain* 1.0 više nego Ethereum mreža). IOTA koristi sustav direktnih acikličnih grafova, čiji prikaz u usporedbi sa *blockchain*-om možemo vidjeti na slici:

[12] EVM je jednostavno rečeno program koji u virtualnom okruženju izvodi pametne ugovore. Za više informacija pogledati: https://ethereum.org/en/developers/docs/evm/




Slika 2. Pojednostavljena grafička reprezentacija *blockchain* i DAG tehnologije[13]

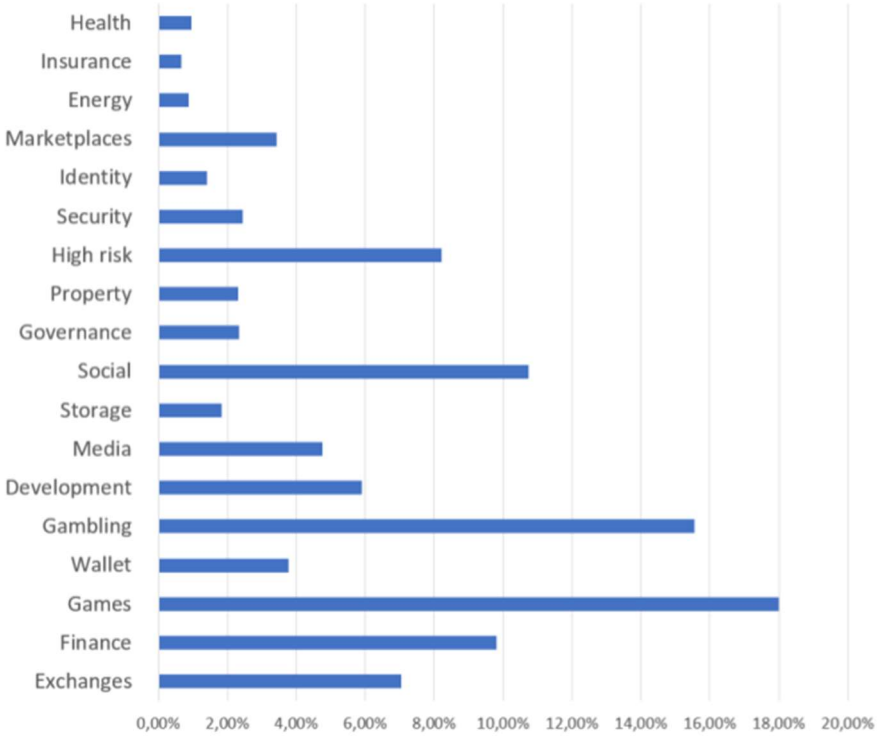
IOTA ne koristi rudarenje da bi potvrdila transakcije, kao što je to slučaj kod Bitcoin *blockchain*-a (zasad i kod Ethereuma). Rudarenje stvara dvije različite vrste učesnika u *blockchain*-u, one koji traže potvrdu transakcija i one koji te transakcije provjeravaju rudarenjem. Kod IOTA mreže, svaki čvor je ujedno i validator. Da bi neki čvor generirao novu transakciju, mora potvrditi dvije prethodne transakcije. Time se drastično smanjuje potreba za utroškom električne energije i omogućuje skalabilnost sustava. Tvorci sustava tvrde da se povećanjem opterećenja mreže brojem transakcija ustvari brže izvode te iste transakcije i mreža bolje funkcionira, što nikako nije slučaj kod *blockchain* tehnologija. Naoko paradoksalno; što god više transakcija dolazi na mrežu, to se više transakcija istovremeno izvršava (Schätz, 2018), te autori sustava tvrde da je mreža time sigurnija.

## 3.3 Potencijali tehnologije distribuiranih knjiga u području energetike

Energetski sektor, kao i ostale grane industrije doživljava promjene u 21. stoljeću. Još uvijek se većinom primjenjuju modeli centralizirane opskrbe energijom, poput plina, električne energije, nafte i naftnih derivata itd. Iako je teško pronaći primjenu *blockchain* tehnologija na sustav primjerice, opskrbe naftom neke kompanije ili države, kod električne energije to nije slučaj. Sektor opskrbe električnom energijom je predvodnik implementacije tehnologije distribuiranih knjiga u svim aspektima poslovanja. Ova implementacija tehnologija distribuiranih knjiga u energetici se ponajviše odnosi na sustave koji omogućuju komuniciranje pametnih ugovora i dApps-a, dok se *blockchain* 1.0 tehnologija primjenjuje većinom u transakcijskom smislu, recimo za plaćanja ili spremanje podataka o računima. A. Hrga i drugi

[13] Preuzeto sa: https://cbcamerica.org/Content/Images/dlt.png

iznose pregled korištenja dApps-a po industrijskim sektorima (Hrga, Capuder, & Podnar Žarko, 2020):




Slika 3. Primjena dApps-a u granama industrije izražena u postotcima (Hrga i drugi, 2020. str. 126156)

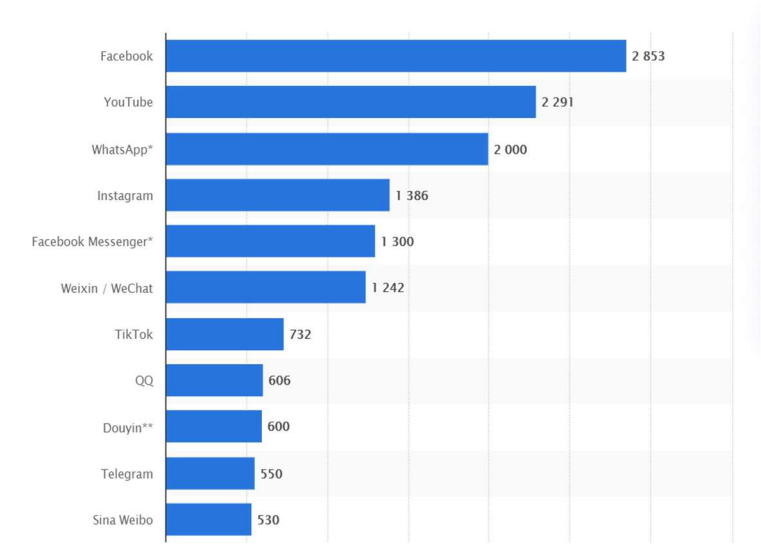
Iz grafa nam je vidljivo da se velika većina dApps-a koristi u industriji zabave, što nije neobično. Transakcije, mikrotransakcije i jednostavni programi su najpogodniji za izvođenje na DLT platformama, što savršeno odgovara industriji računalnih igara, online kladionicama, burzama, društvenim mrežama i platformama; u suštini svim područjima koje koriste mikrotransakcije. Prema izvoru na stranici *stateofthedapps.com* od 3625 decentraliziranih aplikacija (od čega 1810 aktivnih), trenutno aktivnih u području energetike je njih 1.1%, odnosno 20. Razlog ovako malog broja upotrebljavanih aplikacija leži u hirovitom interesu javnosti i ulagača, koji se ponajprije vode trendovima financijske vrijednosti tokena koja u posljednjem desetljeću drastično varira, pa se tako događaju periodi veće i manje aktivnosti koji ovise o cijeni kriptovaluta na tržištu. Također, neke od aplikacija jednostavno ne dožive primjenu, te se projekti nakon nekog vremena napuste.

Elektroenergetski sektor može postati vodeći u korištenju tehnologija raspodijeljenih knjiga, te autori navode nekoliko područja u kojima se potiče ili preporuča upotreba DLT-a (Hrga, Capuder, & Podnar Žarko, 2020, str. 126160)

- **Naplata električne energije** - mogu se koristiti javne DLT platforme, dok se za pohranu i dohvaćanje nepromjenjivih podataka o plaćanju predlaže privatni *blockchain*
- **Naplata usluge punjenja električnih vozila** – javne DLT platforme odgovaraju upotrebi u plaćanju na stanicama za punjenje električnih vozila. Za pohranu podataka o transakcijama se predlaže privatni *blockchain*
- **Registar imovine i/ili podataka –** javne *blockchain* tehnologije koje podržavaju pametne ugovore savršeno odgovaraju upotrebi u registrima imovine
- **Certificiranje za zelene izvore energije -** energetski certifikati se mogu oblikovati pomoću pametnih ugovora i javnog *blockchain*-a, te bi bili potpuno decentralizirani

## 3.4 *Blockchain* u društvenim mrežama

Tehnologije raspodijeljenih knjiga bi mogle postati standardno primjenjivane u društvenim mrežama. Facebook, Twitter, YouTube, Instagram, WhatsApp i druge mreže se sve češće nalaze na udaru kritika zbog kršenja ili mijenjanja uvjeta privatnosti korisnika. Facebook Inc. je nakon akvizicije WhatsApp-a i Instagrama postala dominantna tvrtka i preuzela kontrolu nad velikom većinom ukupnog svjetskog prometa podataka putem društvenih mreža.




Slika 4. Prvih 10 društvenih mreža rangiranih prema broju korisnika (u milijunima)[14]

Na slici 4. možemo vidjeti da Facebook ima preko 2.8 milijardi registriranih korisnika, što odgovara brojci od 35.6% ukupne svjetske populacije, dakle više od trećine. Kako jedna jedina

[14] Preuzeto sa: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

kompanija ima kontrolu nad tom količinom podataka, Facebook se može karikaturno usporediti sa Orwellovim „Velikim Bratom“ iz romana 1984. Pitanje privatnosti podataka korisnika je sve aktualnije u posljednjim desetljećima, te se u svrhu zaštite istih može pronaći najbolja primjena *blockchain* tehnologija. Trenutno razmjene poruka na WhatsApp mreži se osiguravaju tzv. *„end-to-end (E2E)“* metodom, te se u tome polju predlažu primjene *blockchain* enkripcijskih metoda.[15]

Osim u osiguravanju podataka na mreži, *blockchain* tehnologije se primjenjuju i u svrhu zaštite autorskih prava na društvenim mrežama, detektiranje spama i zlonamjernih objava, te se čak razvijaju i decentralizirane društvene mreže. Primjeri takvih decentraliziranih društvenih mreža su *„Steemit“* i *„DTube“*. Steemit je decentralizirana društvena mreža napravljena na principu dApps-a koja se izvodi na Steem *blockchain* platformi (Steemit, Inc., 2017). Korisnici mogu objavljivati i kreirati sadržaj, označavati da im se nešto sviđa ili ne sviđa, kao što je to uobičajeno u korištenju društvenih mreža. Ono što je ne uobičajeno je da korisnici svojim aktivnostima na mreži za nagradu dobivaju tokene u obliku *„STEEM“* kriptovalute. Kako tržišna kapitalizacija svih dostupnih STEEM tokena iznosi oko 240 milijuna američkih dolara, može se zaključiti kako definitivno postoji interes za ovakvom novom vrstom društvenih mreža. Steemit na određen način predvodi društvene mreže u pogledu ravnopravnosti u odnosu korisnik-mreža. Dobrovoljnim dijeljenjem podataka sa Facebook-om korisnik zauzvrat ne dobiva ništa osim pristupa mreži, dok ovakva ideja kakvu nudi Steem kompenzira dijeljenje sadržaja isplatom u kriptovalutama.

Dtube (puni naziv: *„decentralised Tube“*) je alternativa YouTube-u, sagrađena također na Steemit platformi, uz razliku da se koriste drugačiji protokoli, primjereni dijeljenju video sadržaja. Ukratko, korisnici postavljaju i komentiraju video sadržaje, te su kao i kod Steem-a nagrađeni za svoju aktivnost. Najveća mana i najveća prednost Dtube-a je u tome što je kontrola decentralizirana, pa nema cenzure u klasičnom smislu. Također ne postoji ni mogućnost povlačenja ili zabrane video sadržaja kada se jednom postavi na mrežu (VA Digital 2020). Uglavnom više je negativnih aspekata korištenja DTube-a kao alternative YouTube-u. Aplikacija je još u beta verziji, Google i ostale tražilice je skoro uopće ne uključuju u rezultate pretrage, te nedostatak cenzure rezultira kojekakvim sadržajima koji se kasnije ne mogu mijenjati, niti se mogu izbrisati računi korisnika. Dvije su glavne prednosti; nema reklamnih sadržaja i DTube se smatra dobrim okružjem za sve kreatore koji su „propustili vlak“ za

[15] Primjer takvog istraživanja dostupan na poveznici: https://arxiv.org/pdf/2104.08494.pdf

YouTube. Mogućnost monetizacije sadržaja je također potpuno decentralizirana pa isplativost dijeljenja sadržaja često ostaje nejasna, te tek treba vidjeti hoće li ovakav pristup zaživjeti.

## 3.5 Certificiranje i izdavanje diploma na *blockchain*-u

Jedinstveni mehanizam pohrane i osiguravanja podataka na *blockchain*-u, uz mogućnost pohranjivanja i izvršavanja pametnih ugovora je našao primjenu i u području visokog obrazovanja. Tehnologije distribuiranih knjiga su stvorene za sigurno čuvanje i zapis podrijetla podataka, koje čine nepromjenjivim. Primjer dokumenta kojem takva tehnologija savršeno odgovara je diploma ili certifikat bilo koje vrste. Diplome visokoškolskih ustanova, certifikati završenog osposobljavanja, vozačke dozvole, stručni ispiti i razni drugi dokumenti koji nešto dokazuju bi se mogli spremiti na neku *blockchain* platformu. Time bi bili svima dostupni i sigurni od izmjena, a njihovo podrijetlo lako dokazivo.

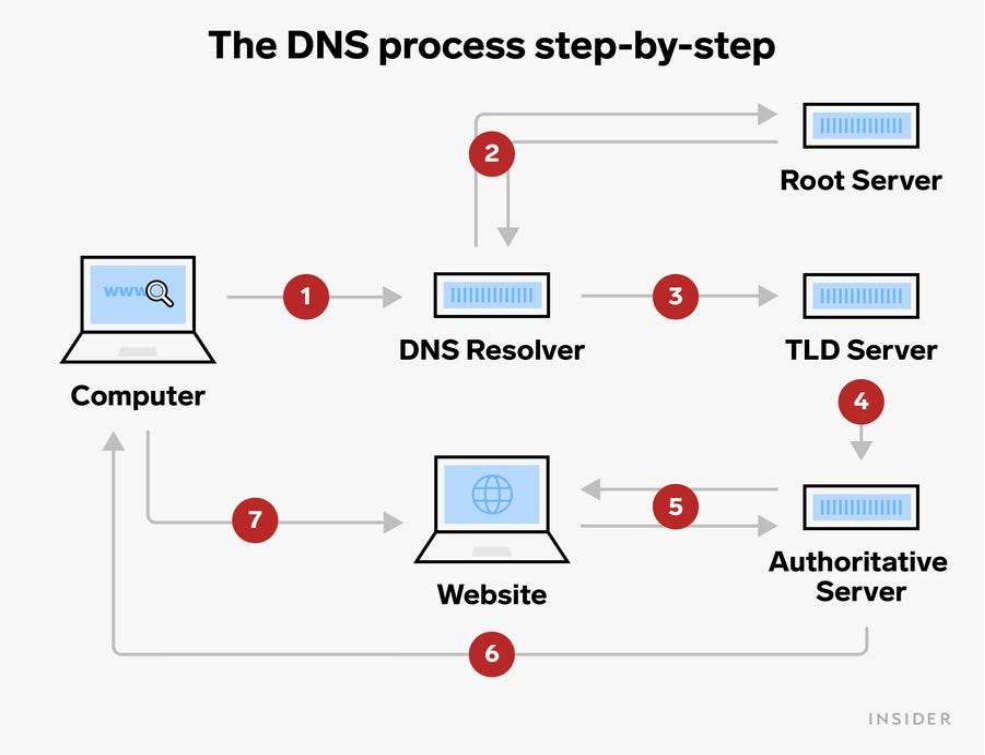
SmartDegrees je jedna od platformi koja koristi *blockchain* tehnologiju za pohranjivanje diploma i certifikata na Ethereum mrežu[16]. Diplomu ili certifikat iz institucije koja je odobrena od strane SmartDegrees-a korisnik postavlja putem aplikacije na platformu, uz koju bilježi neke osobne podatke koji kasnije služe dokazivanju vlasništva. SmartDegrees pohranjuje dokument i u aplikaciji o njemu radi zapis koji se može dijeliti i preko kojega se može po potrebi doći do izvorne, validirane kopije dokumenta. Aplikacija i ovakav sustav pohrane certifikata imaju izgleda da će zaživjeti u praksi zato što nude jednostavno, univerzalno rješenje za dokazivanje predispozicija osobe koja se recimo prijavljuje na neki oglas za posao. Društvena mreža LinkedIn, koja je namijenjena stvaranju profila korisnika za poslovne (profesionalne) svrhe se može povezati sa SmartDegrees platformom. Na taj način kompanija koja traži buduće zaposlenike može biti sigurna da je obrazovanje navedeno na profilu korisnika validirano. BCdiploma je još jedan primjer platforme koja nudi pohranjivanje digitalnih certifikata i diploma na *blockchain* mrežu.[17]

[16] Dostupno na: https://www.smartdegrees.es/en/home-en/

[17] Dostupno na: https://www.bcdiploma.com/en

## 3.6 *DNS* sustav baziran na *blockchain* tehnologiji

*Blockchain* tehnologija se može aplicirati i na *DNS*, tj. sustav domenskih imena (engl. *domain name system*). Da bi se razumjelo na koji način se *blockchain* tehnologija ovdje može primijeniti, prvo treba objasniti kako točno funkcionira *DNS* sustav. *DNS* je ustvari sustav dodjele naziva internetskim adresama, pošto računala ne razumiju u dovoljnoj mjeri ljudski jezik. „*IP*“ (engl. *Internet Protocol*) je protokol, odnosno skup pravila, koji uvjetuju format podatak koji se šalju puten interneta ili lokalne računalne mreže. Kod DNS sustava najvažnije su „IP adrese“. To su jedinstvene brojčane oznake računala koje je spojeno na Internet. IP adresa je u osnovi binarni broj, koji je u slučaju trenutno važeće verzije IP protokola, IPv4, binarni broj 32 bita dug.[18] DNS proces funkcionira ovako:




Slika 5. Prikaz funkcioniranja DNS procesa (Preuzeto s: https://www.businessinsider.com/what-is-a-dns-server)

1. Korisnik (računalo) preko web tražilice šalje upit za određeno web mjesto (web stranicu), primjerice „www.example.com“ . Pošto računalo ne razumije slovni upit, ono šalje zahtjev rekurzivnom imenskom poslužitelju (engl. *DNS Resolver*). Cilj imenskog poslužitelja je pronaći IP adresu povezanu sa upitom web stranice koja se traži.

[18] Za više informacija pogledati: https://www.kaspersky.com/resource-center/definitions/what-is-an-ip-address

2. Rekurzivni imenski poslužitelj prosljeđuje upit korijenskom imenskom serveru (engl. *Root Server*), na kojem je pohranjen popis svih vršnih domena. Vršna domena je zadnja dvoslovna ili troslovna oznaka u nazivu adrese, prva zdesna prije točke- u ovome primjeru „com“.
3. Kada imenski poslužitelj sazna vršnu domenu, šalje upit odgovarajućem serveru vršnih domena (engl. *Top-level domain server*)
4. Server vršnih domena tada prosljeđuje upit autoritativnom imenskom serveru (engl. *Authoritative nameserver*) koji treba vidjeti je li adresa valjana
5. Autoritativni imenski server šalje poruku na traženu adresu i čeka odgovor.
6. Kada je autoritativni imenski server dobio ispravan odgovor od adrese, šalje naziv adrese nazad računalu korisnika
7. Čim web preglednik korisnika dobije ovaj odgovor sa traženom adresom od autoritativnog imenskog servera, počinje učitavati mrežnu stranicu i dalje komunicira direktno s njom, tj. serverom na kojem se nalazi web mjesto.[19]

Cijeli ovaj proces izgleda komplicirano, ali u stvarnosti se izvodi u djeliću sekunde. Također, ako je neka stranica posjećena nedavno, njena adresa se sprema u privremenu memoriju preglednika (engl. *cache*), te se proces preskače pošto je tražena IP adresa poznata. Iz ovoga se može zaključiti da trenutni model funkcioniranja DNS sustava ima brojne mane i slabosti. Sustav je centraliziran i postoji od 1983. godine, a svime upravlja *Internetska organizacija za dodjeljivanje naziva i brojeva* (skraćeno; ICANN). Autor navodi tri glavna kriterija koja DNS sustav mora ispunjavati, bez kojih Internet i ostale tehnologije koje ga koriste ne mogu funkcionirati (Despres, 2020); dostupnost, integritet podataka i povjerljivost (osiguravanje privatnosti korisnika). Ranije opisani mehanizmi kojima se koristi *blockchain* tehnologija odlično osiguravaju potrebne uvjete integriteta, sigurnosti i nepromjenjivosti podataka pohranjenih na *blockchain*-u. Jednom kada je *blockchain* mreža pokrenuta, ne može se zaustaviti jednostavnim hakerskim napadima (poput DDoS-a[20]), što bi osiguralo konstantnu dostupnost sustava. Podatci pohranjeni na *blockchain*-u su nepromjenjivi i sigurni zbog PoW ili PoS metoda osiguravanja konsenzusa. Zahtjevi prema *blockchain*-u za dostupnost traženih podataka (adresa) se mogu slati HTTPS (engl. *HyperText Transfer Protocol – Secure*) protokolom, koji bi osigurao povjerljivost, tj. privatnost korisnika. Zbog ovih razloga je *blockchain* tehnologija odlično rješenje za probleme s kojima se DNS sustav suočava. Autor

[19] Preuzeto s https://www.businessinsider.com/what-is-a-dns-server
[20] Preporuča se objašnjenje na: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

ideju naziva *DNS on Blockchain* i ističe neke već dostupne projekte; ponajprije *Ethereum Name Service (ENS)*, tehnologiju koja nadopunjuje neke potrebe DNS-a i komplementarna je sa njime (Despres, 2020). Ipak, potreban je napredak u području skalabilnosti, sigurnosti i uporabljivosti sustava, iz čega se zaključuje da *blockchain* tehnologija možda još uvijek nije spremna za preuzimanje odgovornosti nad DNS sustavom.

## 3.7 *Blockchain* tehnologija u arhivistici

Moderni izazovi arhivistike su u suštini stari izazovi arhvistike. Kako očuvati integritet dokumenta, kako pohraniti dokaz o vlasništvu i vremenu nastanka dokumenta, te kako ga učiniti dostupnim na zahtjev u digitalnom dobu postaje sve veći problem, zbog nikad većeg porasta broja dokumenata koji se stvaraju svaki dan. Trenutne metode rješavanja ovog problema u digitalnoj arhivistici se oslanjaju na kopiranje sadržaja na digitalne medije poput CD-a i HDD-ova. Te dokumente onda čuvaju i o njima se tokom vremena „brinu“ arhivske institucije, periodično kopirajući sadržaj na dovoljan broj medija koji se pohranjuju na različitim mjestima kako bi se osigurala dostupnost u slučaju kvara na fizičkim uređajima pohrane. Digitalno očuvanje[21], u ovom slučaju arhivskog sadržaja (građe), je moderan problem s kojim se susreće arhivistika, te su propisane brojne smjernice i norme o metodama umnažanja, čuvanja, zaštite i pohrane podataka na digitalnim medijima, odabiru formata i migriranju sadržaja neovisno o platformi korištenja (poput *„eArchiving“*-a[22]).

Svaki digitalni arhivski zapis mora očuvati svoju autentičnost, pouzdanost, integritet i dostupnost. Digitalni potpisi i pečati obično osiguravaju autentičnost zapisa, a kvalitetna pohrana takvih digitalno potpisanih ili pečatiranih zapisa postaje kompliciranija, jer sadrži dodatnu razinu kompleksnosti (Stančić, 2018). Također, valjanost digitalnih pečata i potpisa ovisi o certifikatima koji se obično izdaju na nekoliko godina od strane centralnog autoriteta, a kad certifikat istekne, valjanost dokumenta se više ne može propisno dokazati, što nameće dodatne probleme. Kako arhivski zapis učiniti trajno neporecivim i pohraniti dokaz o vremenu nastanka i vlasništvu, je problem na koji se može odgovoriti primjenom *blockchain* tehnologije. Prema Stančiću (Stančić, 2018, str. 67), *blockchain* tehnologija se u arhivistici može primijeniti za:

[21] Za više informacija pogledati https://en.wikipedia.org/wiki/Digital_preservation
[22] Dostupno na https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eArchiving+Standards

- potvrđivanje integriteta zapisa
- dokazivanje da je zapis nastao u određenom trenutku (jer *blockchain* tehnologija koristi ranije opisani *timestamping*)
- potvrđivanje redoslijeda zapisa
- podršku stvaranja neporecivosti zapisa
- unapređenje mogućnosti validacije digitalno potpisanih dokumenata tijekom dugoročne pohrane

Razlozi zbog kojeg se otvaraju ove mogućnosti primjene *blockchain*-a u digitalnoj arhivistici najbolje opisuje autor:

*„U konceptu blockchain-a postoji nekoliko prednosti. Prije svega, samo hash-evi su pohranjeni (registrirani) u blockchain-u. Stvarni podaci, dokumenti ili zapisi koji se raspršuju, pohranjuju se u institucionalni sustav za upravljanje dokumentima ili zapisima. Drugo, svaki dodatni blok pojačava prethodne, budući da blokovi su međusobno povezani i svaki novi blok ovisi o vezama prethodnih blokova. Konačno, izmjena bilo kojeg bloka na lancu poništava sve naredne blokove.“*[23] (Stančić, 2018, str. 64)

Nepromjenjivost zapisa, decentraliziran pristup, *timestamping* i sigurnost mreže očuvana PoW ili PoS metodama, dovode do zaključka kako će *blockchain* tehnologija nesumnjivo naći svoju primjenu u arhivistici, pogotovo na mrežama koje će podržavati *dApps* i višeplatformski pristup sustavu. Kako se arhivistika uglavnom bavi službenim, javnim dokumentima i zapisima, ostaje pitanje zakonodavstva, tj. propisa i normi koje bi standardizirale ovakvu pohranu podataka, dokumenata i zapisa uz pomoć *blockchain* platformi.

[23] Prijevod autora. Tekst u originalu glasi: *„There are several strengths in the blockchain concept. First of all, only hashes are stored (registered) in the blockchain. The actual data, documents or records being hashed are stored in the institutional document or records management systems. Secondly, each additional block reinforces the preceding ones, since the blocks are chained together and each new block is dependent on the links of the previous blocks. Finally, modifying any block on the chain invalidates all subsequent blocks.“*

# 4. Zaključak

Svaka tehnologija, pa tako i *blockchain*, ima svoj smjer i vrijeme sazrijevanja. Budući da je ideja stara tek desetak godina, novosti oko nje su još uvijek aktualne, a predviđanja budućeg smjera razvoja nesigurna. Dok se neki timovi developera i organizacije bave kontinuiranim postavljanjem novih tokena na burze i mjenjačnice kriptovaluta u želji za profitom, drugi se bave traženjem niša industrije u kojima bi *blockchain* savršeno odgovarao. Kao što je aplikacija *Kontakti* na pametnom telefonu zamijenila debele tiskane imenike brojeva, tako bi i *blockchain* tehnologija mogla zamijeniti neke postojeće tehnologije. Općenito, *blockchain* je savršeno pouzdan kad god treba pohraniti veliku količinu malih zapisa ili dokumenata, učiniti ih nepromjenjivima i sigurnima. Tako da je lako moguće da će se jednog dana fakultetske diplome izdavati putem Ethereuma ili neke druge mreže, a da će posjet stomatologu završavati dodavanjem podataka na *„DentChain“* (mogući naziv za budući stomatološki *blockchain*). Trenutna primjena tehnologije polako dopire do svih grana industrije i zabave, zahvaljujući evoluciji i nadogradnji sustava. S novim tehnologijama poput IOTA-e koje koriste neke metode koje se nastavljaju na Nakamotovu ideju, otvaraju se mogućnosti i to ponajprije za primjenu u nefinancijske svrhe. Zapravo, već u ovoj fazi razvoja DLT-a može se primjetiti da ta poveznica sa kriptovalutama koči razvoj i implementaciju u društvene domene. Zbog straha od financijskog rizika i lažne pretpostavke neodvojivosti *blockchain*-a i kriptovaluta, moglo bi se dogoditi da ideja padne u zaborav. Stotine dobrih ideja i implementacija DLT-a su propale jer nisu potakle dovoljan interes ulagača, ali ne ulagača u tehnologije, industrijalaca ili državnih fondova; već ulagača u kriptovalute koji u svemu gledaju isplativost. Više puta se tokom posljednjih godina govorilo kako je bitcoin balon i piramidalna prevara, a kriptovalute „zlato za budale“ i kako će sve to uskoro propasti. Mišljenje je autora da je propast kriptovaluta odlična stvar za tehnologiju distribuiranih knjiga, uz uvjet da nakon propasti ne prevlada iracionalan strah u obliku zakonskih zabrana upotrebe tehnologije. *Blockchain* nije bitcoin i što se prije to dvoje odvoji u svijesti onih koji o tome donose odluke, to bolje po svaku domenu u kojoj se *blockchain* može primijeniti.

# Literatura


Despres, S. (8. travanj 2020). *DNS on Blockchain: the next evolution of domain names?* Preuzeto 23. 9. 2021. iz https://blog.nameshield.com/blog/2020/04/08/dns-on-blockchain-the-next-evolution-of-domain-names/: https://blog.nameshield.com/blog/2020/04/08/dns-on-blockchain-the-next-evolution-of-domain-names/

ethereum.org. (n.d.). *Introduction to dapps | ethereum.org*. Preuzeto 23. 9. 2021. iz https://ethereum.org/: https://ethereum.org/en/developers/docs/dapps/

Gensler, G. (2018). 15.S12 Blockchain and Money. *Massachusetts Institute of Technology: MIT OpenCourseWare*. Creative Commons BY-NC-SA. Preuzeto 23. 9. 2021. iz https://ocw.mit.edu.

Hrga, A., Capuder, T., & Podnar Žarko, I. (21. srpanj 2020). Demystifying Distributed Ledger Technologies: Limits, Challenges, and Potentials in the Energy Sector. *IEEE Access, 8*, 126149-126163.

Lamport, L., Shostak, R., & Pease, M. (1982). The Byzantine Generals Problem. *Transactions on Programming Language and Systems, IV*(3), 382-401.

Merriam-Webster. (30. kolovoz 2021). *Blockchain | Definition of Blockchain by Merriam-Webster.* Preuzeto 23. 9. 2021. iz https://www.merriam-webster.com/dictionary/blockchain: https://www.merriam-webster.com/dictionary/blockchain

Merriam-Webster. (2021). *Cryptocurrency | Definition of Cryptocurrency by Merriam-Webster*. Preuzeto 23. 9. 2021. iz https://www.merriam-webster.com/dictionary/cryptocurrency: https://www.merriam-webster.com/dictionary/cryptocurrency

Nakamoto, S. (09. siječanj 2009). *Bitcoin: A Peer-to-Peer Electronic Cash System.* Preuzeto 23. 9. 2021. iz https//bitcoin.org/bitcoin.pdf: https//bitcoin.org/bitcoin.pdf

Popov, S. (30. travanj 2018). *The Tangle.* Preuzeto 23. 9. 2021. iz https://www.iota.org/foundation/research-papers: http://www.descryptions.com/Iota.pdf

Schätz, C. (05. kolovoz 2018). *How IOTA solves Blockchains scalability problem*. Preuzeto 23. 9. 2021. iz https://hackernoon.com/: https://hackernoon.com/how-iota-solves-blockchains-scalability-problem-12e5cae05531

Stančić, H. (2018). New Technologies applicable to Document and Records Management: Blockchain. *LLIGALL 48 Revista Catalana d'Arxivística*, 56-72. Preuzeto 23. 9. 2021. iz https://www.researchgate.net/publication/332849198_New_Technologies_applicable_to_Document_and_Records_Management_Blockchain

Steemit, Inc. (kolovoz 2017). *Steem: An incentivized, blockchain-based, public content platform.* Preuzeto 23. 9. 2021. iz https://steem.com/SteemWhitePaper.pdf: https://steem.com/SteemWhitePaper.pdf

Szabo, N. (1994). *Smart Contracts.* Preuzeto 23. 9. 2021. iz https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html: https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html

World Economic Forum. (2018). Building Block(chain)s for a Better Planet. *Fourth Industrial Revolution for the Earth Series* (str. 5,32). Geneva: World Economic Forum System Initiative.

# Popis oznaka i kratica

| | |
|---|---|
| BTC | Bitcoin |
| CD | Compact Disk |
| DAG | Directed Acyclic Graph |
| dApps | Decentralised Applications |
| DDoS | Distributed Denial of Service |
| DLT | Distributed ledger technology |
| DNS | Domain Name System |
| ENS | Ethereum Name System |
| ETH | Ethereum |
| EVM | Ethereum Virtual Machine |
| HDD | Hard Disk Drive |
| HTTPS | HyperText Transfer Protocol Secure |
| IoT | Internet of Things |
| IP | Internet Protocol |
| IPv4 | Internet Protocol (version 4) |
| mIOTA | megaIOTA |
| POS | Point Of Sale |
| PoS | Proof-of-Stake |
| PoW | Proof-of-Work |
| SHA-256 | Secure Hash Algorithm-256 |

# Primjena blockchain tehnologija u nefinancijske svrhe

## Sažetak

Prva primjena *blockchain* tehnologije je bila financijske prirode, kada je stvorena prva kriptovaluta - Bitcoin. Istraživanjem tehnologija distribuiranih knjiga (DLT) i njihovom nadogradnjom, osim novih kriptovaluta javljaju se i druge primjene *blockchain*a. Svugdje gdje se barata sa puno kratkih zapisa koje nalikuju transakcijama, *blockchain* se pokazuje kao izvrsno rješenje jer je siguran, robustan i podatke sprema na način da postaju nepromjenjivi. Kroz nekoliko primjera se daje naslutiti da će i u budućnosti *blockchain* i tehnologije koje su iz njega proizašle imati sve veću primjenu. Ethereum i pametni ugovori donose revolucionaran napredak i stvaraju *blockchain* 2.0. Stvaranjem posebnih programskih jezika kojima se programi pišu i izvode na *blockchain*-u, tvorći tako decentralizirane aplikacije, uvelike raste broj mogućih primjena tehnologije. Financijska primjena je već dovoljno dugo aktualna da se javljaju nerješivi problemi- iz čega se može zaključiti da je došlo vrijeme da DLT tehnologije prerastu ideju kriptovaluta i uđu u sve grane industrije u kojima su primjenjive.

**Ključne riječi:** *blockchain, kriptovalute, nefinancijska primjena, distribuirane knjige, Ethereum*

# Application of blockchain technologies for non-financial purposes

## Summary

The first application of blockchain technology was of a financial nature, when the first cryptocurrency – Bitcoin, was created. Apart from new cryptocurrencies, other applications of blockchain are emerging from the research of distributed ledger technologies (DLT) and their upgrades. Wherever it is required to manage a lot of short records that resemble transactions, blockchain proves to be a great solution because it is secure, robust, and stores data in a way that makes it immutable. Several examples suggest that the blockchain and the technologies that have emerged from it will continue to be used in the future. Ethereum and smart contracts bring revolutionary progress and create blockchain 2.0. By creating special programming languages in which programs are written and executed on the blockchain, thus creating decentralized applications, the number of possible applications of the technology is greatly increasing. Financial application has been around for a long time and unsolvable problems are starting to emerge- from which it can be concluded that the time has come for DLT technologies to outgrow the idea of cryptocurrencies and enter all branches of industry in which they are applicable.

**Key words:** *blockchain, cryptocurrencies, non-financial application, distributed ledgers, Ethereum*