SVEUČILIŠTE U ZAGREBU
FILOZOFSKI FAKULTET
ODSJEK ZA FILOZOFIJU

Jurica Marković

ETIČKI TEMELJI I MORALNI IZAZOVI *BLOCKCHAIN* TEHNOLOGIJE

Diplomski rad

Mentor: izv. prof. dr. sc. Hrvoje Jurić

Zagreb, rujan 2018.

Sadržaj

Etički temelji i moralni izazovi *blockchain* tehnologije

Sažetak: Diplomski rad nastoji utvrditi etičke temelje i moralne izazove *blockchain* tehnologije. U radu se daje definicija *blockchain* tehnologije, objašnjava njena inovativnost te pokazuje kako nužnošću iz nje dolazi do pojave *kriptovaluta*. Velika pažnja posvećuje se opisivanju spomenute tehnologije iz tehničkog aspekta koji je važan da se sadržajno razumije njen ne-tehnički dio u koji spada utvrđivanje etičkih temelja. Etika vrlina tijekom istraživanja pokazala se kao najkompatibilnija za razumijevanje i opisivanje tehničkog fundamenta *blockchaina*, a moralni izazovi protežu se kao lajtmotiv kroz cijeli rad. Razlog tome je i specifičnost *blockchaina* koji u velikoj bliskosti inkorporira svoj tehnički i ne-tehnički dio. Na taj način iskazuje veliki potencijal primjena u političko-ekonomsko-tehnološkoj sferi čije se sadržajno bogate i brojne implikacije imaju mogućnost istražiti i iz društveno-humanističke perspektive u znanosti.

Ključne riječi: *blockchain*, tehnologija, etika, moral, vrijednosti, kriptovalute

Ethical foundations and moral challenges of *blockchain* technology

Abstract: This graduate thesis has primary intention to identify the ethical foundations and moral challenges of blockchain technology. The paper gives definition of blockchain technology, explains its innovation and demonstrates how the emergence of cryptocurrency was a necessity of its fundamental – technical structure. Great attention is devoted to describing this technology from a technical aspect that was found important to utterly understand its non-technical part of which ethical foundations is a main part. During the research that preceded in making of this paper, The ethics of virtue proved to be the most compatible model for understanding and describing the technical fundamentals of blockchain and moral challenges which tend to be the leitmotif of the paper. The reason for being so is the specificity and uniqueness of the blockchain which lay in the close connection of its technical and non-technical part. Because of that, blockchain technology has a great potential of application in the political, economic and technological sphere and should have many rich-content and numerous implications. These implications could prove to be a source of a research from a socio-humanistic perspective in science as well.

Key words: blockchain, technology, ethics, morals, values, cryptocurrency

1. Uvod

1.1. Obrazloženje teme, motiva za pisanje, ciljeva te očekivanih rezultata

Osnovno obilježje čovjeka je da razvija i primjenjuje alate i materijale da bi proizveo nešto novo, što uključuje i da razmišlja o tehnici proizvodnje. Čovjek ima najprije mogućnost misliti o proizvodnji i načinu proizvodnje, a za razliku od životinje čini to na sistematičan i kreativan način koji odolijeva promjenama. Štoviše, čovjek je proizveo alate i strojeve koji su mu omogućili da mijenja okoliš.[1] Možemo reći da je čovjek biće tehnike i tehnologije. Tehnologija je razvoj i primjena alata, strojeva, materijala i postupaka za izradbu nekog proizvoda ili obavljanje neke aktivnosti.[2] Tehnika je ukupnost iskustveno ili znanstveno utemeljenih vještina, umijeća i postupaka, s potrebnim priborom, pomagalima i strojevima koji služe za zadovoljavanje ljudskih potreba u stvarnome životu.[3] I jedna i druga definicija daju nam do znanja da je čovjek kroz povijest stalno pronalazio način da svojom kreativnošću proizvede nešto novo. Suvremeni proizvodi dokaz su neprekidne inovativnosti. Nove tehnologije u današnjem svijetu[4] postale su svakodnevnica.

---

[1] »U osnovi, tehnike su metode stvaranja novih alata i proizvoda alata, a sposobnost za izgradnju takvih artefakata je određujuća osobina ljudskih vrsta. Ostale vrste stvaraju artefakte: pčele grade kompleksne košnice da bi spremile svoj med, ptice prave gnijezda, a dabrovi grade brane. No ta su svojstva rezultat obrazaca instinktivnog ponašanja i ne mogu se prilagoditi okolnostima koje se brzo mijenjaju. Čovječanstvo, za razliku od drugih vrsta, ne posjeduje visoko razvijene instinktivne reakcije, ali ima sposobnost sustavnog i kreativnog razmišljanja o tehnikama. Ljudi mogu inovirati i svjesno mijenjati okoliš na način koji ni jedna druga jedinka nije postigla. Majmun može ponekad upotrijebiti štap da bi stresao banane s drveta, ali čovjek može oblikovati štap u alat za rezanje i skinuti cijelu hrpu banana. Negdje u prijelazu između čovjeka i majmuna pojavljuje se hominid, prva čovjekolika vrsta. Zbog svoje naravi izrade alata čovjek je stoga tehnolog od početka, a povijest tehnologije zaokružuje cjelokpuni razvoj čovječanstva.« Vidi: Robert Angus Buchanan, »History of technology«, *Encyclopaedia Britannica*. Dostupno na: https://www.britannica.com/technology/history-of technology (pristupljeno 29. 8. 2018.); usporedi: »Tehnika je način otkrivanja. Tehnika bivstvuje u području, u kojemu se stječe otkrivanje i neskrivenost, αλήθεια, istina.« Vidi: Martin Heidegger, »Pitanje o tehnici«, u: *Kraj filozofije i zadaća mišljenja*, Naprijed, Zagreb 1996., str. 228.

[2] »Tehnologija«, *Hrvatska enciklopedija*. Dostupno na: http://www.enciklopedija.hr/Natuknica.aspx (pristupljeno 29. 8. 2018.). Usporedi: Ljiljana Šarić, Igor Čatić, »Raznoznačnost naziva tehnika i tehnologija«, *Mehanizacija šumarstva* 23 (1998) 3–4, str. 157–162.

[3] »Tehnika«, *Hrvatska enciklopedija*. Dostupno na: http://www.enciklopedija.hr/Natuknica.aspx (pristupljeno 29. 8. 2018.). Usporedi: Lj. Šarić, I. Čatić, »Raznoznačnost naziva tehnika i tehnologija«.

[4] »Kada sagledamo ljudsko putovanje s ove točke gledišta, značajka koja se doista ističe je sustavno sažimanje vremena u prelasku jedne faze na drugu. Prva faza je trajala 200 000 godina, a pozornica na kojoj se trenutno nalazimo trajat će oko 70 godina. To je velika razlika i ukazuje na to koliko se naša evolucija ubrzava. Poslovni svijet u kojem živimo danas je znatno drugačiji od okoliša prije 20 godina i gotovo je neprepoznatljiv korporativnom okruženju otprije 100 godina. Živimo u tzv. VNKD svijetu – volatilnom, nesigurnom, kompleksnom i dvosmislenom. Taj svijet zauvijek mijenja lice poslovanja.« Vidi: Alan Watkins, »The Evolution of Enlightened Leadership«, para. 2, u: *Coherence: The secret science of briliant leadership*, Complete Coherence Limited, London 2014. [Microsoft Edge, .epub format]. Kada sam napisao današnji svijet mislio sam na tzv. VNKD svijet.

U radu namjeravam obraditi i istražiti problematiku nove tehnologije, naziva *blockchain*.[5] Nastojat ću objasniti i pokazati da poprima sve veći značaj u svijetu. Cilj je diplomskog rada utvrditi etički temelj i moralne izazove *blockchain* tehnologije te se nadam da će na istraživanje potaknuti druge istraživače u domeni društveno-humanističkih znanosti u Hrvatskoj te stvoriti platformu za razvoj znanja.

Istraživanje je podijeljeno, ne računavši uvod i zaključak, na 3 cjeline. Na početku ću prve cjeline definirati i objasniti pojam *blockchain*. Krenut ću s radnom definicijom da bih disecirao pojmove i došao do njene aktualne i najpoznatije primjene u vidu *kriptovaluta*. Štoviše, pokazat ću da je do pojave *kriptovaluta* došlo nužnošću radi samih temelja na kojima je sazdana *blockchain* tehnologija. U ovoj su tehnologiji aristotelovski *physis* i *techne* izrazito bliski, čak i do te mjere da bi mogli reći da postoji djelomično preklapanje. Gotovo je nemoguće govoriti o ne-tehničkom aspektu *blockchaina* bez jasnog i jezgrovitog objašnjenja onog tehničkog. Drugu sam veliku cjelinu posvetio etičkom aspektu *blockchain* tehnologije i pokušao odrediti njen etički temelj. Najviše dodirnih točaka pronašao sam u etici vrlina kako je razvijana kod Platona i Aristotela te ću nastojali obrazložiti kroz tri potpoglavlja zašto je tome tako. Moralni se izazovi sami po sebi pojavljuju u obradi tehničkog aspekta. Svi pokušaji potpunog apstrahiranja posljedica koje sa sobom nosi *blockchain* tehnologija i implikacija onog etičkog, a nadasve moralnog, bili su uzaludni. Zašto je tome tako? Djelomičan odgovor leži u činjenici da je jedna od zasluga računalne etike informacijskog doba upravo nastojanje da eklatantno izvuče na površinu svu problematiku koja se kod rada s tehnologijom pojavljuje, bez daljnje zadrške. Međutim, nastojao sam izolirati problematiku u posebnu cjelinu. Treću cjelinu rada započet ću primjerima pozitivne uporabe *blockchain* tehnologije, a zatim prikazati njena tehnička i ne-tehnička ograničenja. Postoje mnogi scenariji kako bi se ta tehnologija mogla rabiti, ali ona još uvijek nije zaživjela do te mjere da bismo mogli podučavati o negativnim primjenama. Opisat ću koruptivne elemente *blockchaina* – prikazat ću jedan od mogućih scenarija prema kojem primjena *blockchaina* može poći u nepovoljnom smjeru te istaknuti još nekoliko primjera iz recentne literature. U

[5] U nastavku rada uz pojam *blockchain* rabit ćemo najčešće termin *tehnologija* te će se ova dva pojma najčešće pojavljivati u sintagmi. Iz danih definicija možemo uočiti da pojam tehnike predstavlja ukupnost iskustveno ili znanstveno utemeljenih metoda za zadovoljavanje čovjekovih potreba. Upravo radi *ukupnosti*, u ovom se radu tehnika shvaća kao opći pojam koji je nadređen pojmu tehnologije – primjeni spomenutog alata ili dijela znanja tehnike za rješavanje pojedinog problema ili obavljanje neke aktivnosti. Kada ćemo u radu govoriti o svojstvima *blockchain* tehnologije, pisat ćemo o njenim *tehničkim* i *ne-tehničkim* aspektima.

posljednjem dijelu ove cjeline, prije zaključka, dotaknut ću se pitanja morala i razjasniti status morala te moralnih izazova u domeni *blockchain* tehnologije. U zaključku ću nastojati sažeti napisano i ponuditi vlastito mišljenje na temelju provedenog istraživanja, a sve u obvezi koju nam jedan diplomski rad nalaže – da znanstvenoj zajednici priložimo unikatni produkt istraživanja kao krunu višegodišnjeg studiranja. S obzirom na to da se radi o recentnoj temi koja svoje mjesto tek traži u polju znanosti u Hrvatskoj, nadasve u društveno–humanističkom spektru, motiva za istraživanje i pisanje o ovoj temi nije nedostajalo.

1.2. Metodologija istraživanja: pristup, metoda, izvori, obrada

Tehnički, ili bolje reći tehno-znanstveni aspekt tiče se najviše izvedbenog dijela tehnologije. Istraživanje u tom smjeru bilo je duže i teže. Pojavljivalo se mnogo stručne terminologije koju je trebalo shvatiti i uklopiti u smislenu cjelinu. U pisanju o tehničkom aspektu držao sam se analitičke metode. Najprije sam ponudio radnu definiciju *blockchaina* koju sam raščlanjivao kroz preostala poglavlja i potpoglavlja, a za pisanje o ne-tehničkom dijelu, tj. određivanju etičkog temelja koristio sam se najviše sintetičkom metodom.

Izvori koje sam koristio prilikom izrade rada za tehnički dio su recentni, što je i razumljivo s obzirom na novost koju *blockchain* predstavlja. Naime, ni jedna jedinica literature nije starija od pet godina. Koristio sam se najviše stranim autorima, pretežito na engleskom jeziku. Osim knjiga u digitalnom formatu koristio sam dostupne izvore na internetskim portalima, opće (enciklopedijske) izvore te članke inozemnih stručnjaka. Proučavao sam projekte *kriptovaluta* uglavnom na internetskim stranicama, a izvore s društvenih mreža i *YouTube* kanala koristio sam kako bih proširio znanje o temi.[6] U ovom aspektu proučavanja, kod izrade rada najviše je poslužila knjiga Daniela Dreschera *Blockchain Basics*: *A Non-Technical Introduction in 25 Steps*. Radi se o jednostavnom opisivanju *blockchain* tehnologije iz ne-tehničke perspektive u dvadeset i pet koraka. Knjiga

[6] Budući da je *blockchain* fenomen recentna pojava, koristio sam se u istraživanju svim dostupnim izvorima. To sam učinio kako bih proširio znanje i postavio problematiku u valjan kontekst. Nakon skupljanja i obrade podataka te dodatnom provjerom, razlučio sam koji se izvori mogu koristiti u svrhu izrade znanstvenog rada. Proces filtracije bio je potreban i nužan jer još uvijek ne postoje eminentni i profilirani stručnjaci kada u ovom trenutku govorimo o *blockchainu*.

je poslužila i najviše doprinijela razumijevanju pojma *blockchaina* te sam po modelu koncentričnih krugova oko nje gradio znanje.

Za ne-tehnički dio rada poslužio sam se izvornom literaturom filozofa Immanuela Kanta i Johna Stuarta Milla te Platona i Aristotela. Kant i Mill, kao predstavnici dviju velikih etičkih struja, poslužili su mi pri smještanju *blockchain* fenomena u kontekst, dok sam proučavanjem klasičnih filozofa Platona i Aristotela uočio najveće podudaranje njihovog nauka o vrlini s problematikom *blockchaina*. Ostalu građu crpio sam iz općih pregleda etike i enciklopedijskih izvora. Detaljnije obrađivanje tehničkog dijela *blockchaina*, osim nužnosti povezivanja s ne-tehničkim bilo je potrebno za razumijevanje, a razlog tome je i nepostojanje relevantne literature na hrvatskom jeziku o *blockchainu* na koju bih se mogao osloniti.

2. Određenje *blockchain* tehnologije: tehnički aspekt

2.1. Što je *blockchain* tehnologija: definicija i objašnjenje

2.1.1. Radna definicija

Blockchain tehnologija[7] je decentralizirani sistem mreže ravnopravnih (eng. *peer-to-peer*)[8] računala koji omogućuje izravne transakcije podataka među čvorovima (eng. *nodes*)[9] unutar sustava, tako eliminirajući potrebu za posredništvom i trećom osobom (eng. *third party*).[10] Sustav pamti sve transakcije i pohranjuje ih u javnu knjigu salda (eng. *distributed ledger*).[11] Transakcije su pohranjene u blokovima[12] koji se slažu jedan na drugi u lančanom obliku (otuda i ime *block-chain*). Tehnologija ima namjeru u sustavu izgraditi i očuvati povjerenje i integritet (eng. *trust and integrity*)[13] da bi postigla sigurnost (eng. *security*). *Blockchain* tehnologija pokušava ostvariti taj cilj kroz dvije komponente: *hash* tehnologiju te kriptografsku tehnologiju.[14] *Blockchain* tehnologija ima veliku mogućnost primjene koja se u trenutku nastajanja ovog rada još razmatraju i definitivno proširuju a trenutno je najpoznatija primjena ove tehnologije kod *kriptovaluta* (eng. *cryptocurrency*).

Za razumijevanje definicije bit će potrebno pojasniti tehničke i funkcionalne aspekte proučavane tehnologije. Pokušao sam pronaći »zlatnu sredinu«, da ne ulazim previše u tehničko-funkcionalne detalje, a da opet postignem razumijevanje i osnovni pojam o tome što ta tehnologija predstavlja, po čemu je drugačija od svih prijašnjih tehnologija i koji je njen potencijal.[15]

---

[7] Pojam *blockchain* na hrvatski jezik mogao bi se prevesti kao *tehnologija povezanih blokova*.
[8] Vidi: Alex Tapscott, Don Tapscott, »A cautionary tale of blockchain regulation«, para. 6, u: *Blockchain Revolution*, Brilliance Audio, 2016. [Microsoft Edge, .epub format]
[9] Čvor predstavlja računalo čiji je krajnji korisnik čovjek. Vidi: isto, »Networked integrity«, para. 4.
[10] Isto, »Distributed power«, para. 6. [Microsoft Edge, .epub format]
[11] Isto, »How this worldwide ledger works«, para. 1–7. [Microsoft Edge, .epub format]
[12] Blok je organizirana jedinica podataka unutar strukture blockchaina. Za detaljnjije objašnjenje o tome što je blok vidi: Daniel Drescher, *Blockchain Basics: A Non-Technical Introduction in 25 Steps*, Apress, Frankfurt am Main 2017., str. 111–122.
[13] Usp.: isto, str. 29–32.
[14] Usp.: isto, str. 70–79, 93–101.
[15] Za objašnjenje u audiovizualnom formatu usporedi: Lorne Lantz, »TED Talks: The Blockchain Explained Simply«, *YouTube* (21. 12. 2016.). Dostupno na: https://www.youtube.com/watch?v=KP_hGPQVLpA&t=22s (pristupljeno 6. 9. 2018.).

Važno je odmah na početku istaknuti da se pojam *blockchain* može rabiti na četiri načina:

1. U smislu naziva za strukturu podataka (eng. *data structure*): u računalnoj znanosti i softverskom inženjerstvu, struktura podataka način je organiziranja podataka bez obzira na njihov konkretni informacijski sadržaj;
2. Kao naziv za algoritam: u softverskom inženjerstvu, pojam algoritam odnosi se na slijed uputa koje računalo mora ispuniti;
3. Kao naziv za skup tehnologija; Kada se koristi za upućivanje na skup tehnologija, *blockchain* se odnosi na kombinaciju ustroja podataka (eng. *blockchain-data-structure*), blokovski algoritam (*blockchain-algorithm*) kao i na kriptografske i sigurnosne tehnologije koje se u kombinaciji mogu koristiti za postizanje integriteta u potpunom decentraliziranom sustavu mreže ravnopravnih računala (eng. *purely distributed peer-to-peer system*) bez obzira na primjenu;
4. 4. Kao krovni termin (eng. *umbrella term*) za potpune decentralizirane sustave mreže ravnopravnih računala sa zajedničkim područjem primjene: pojam *blockchain* se također može koristiti kao krovni termin za potpuni decentralizirani *peer-to-peer* sustave poslovnih knjiga (eng. *purely distributed peer-to-peer systems of ledgers*) koje upotrebljavaju tehnološki paket *blockchaina*.[16]

U ovom radu objasnio sam što podrazumijeva točka 1) i točka 2), a držao sam se definicije 3) i pri opisivanju tehničkog aspekta spomenuo i točku 4) koja se najviše tiče primjene *blockchaina* u sferi *kriptovaluta*. Valja imati na umu činjenicu da je ova tehnologija nova pojava koja je tek u razvitku. Razvijanje tehničko-konceptualnog dijela *blockchaina* još uvijek traje. To u osnovi znači da ne postoji čvrsta definicija što *blockchain* tehnologija uopće jest te koje su sve konceptualne mogućnosti njene primjene i kakve to implikacije može proizvesti.

2.1.2. Decentralizirana mreža ravnopravnih računala

[16] Usporedi: D. Drescher, *Blockchain Basics*, str. 34–35.

Najprije nam valja utvrditi što uopće znači pojam decentraliziranog računalnog sustava. Postoji mnogo načina kako da se implementira softverski[17] sistem, međutim jedna od fundamentalnih odluka koja se treba donijeti u samoj implementaciji tiče se arhitekture (kako se komponente odnose jedna prema drugoj u sustavu). Dva glavna rješenja arhitektonike sistema su centralizirani i decentralizirani sistem. U centralnom su softverskom sistemu komponente povezane oko središnjice, centralne komponente, dok u decentraliziranom sustavu ne postoji centralna komponenta koja koordinira ili kontrolira ostale komponente u sustavu.[18] U praksi, radi se o spojenim računalima ili čvorovima (eng. *nodes*) bez središnjeg, glavnog računala naspram jednog, pojedinačnog računala (eng. *single computer*) koje obavlja sve operacije u sustavu. *Blockchain* tehnologija bazirana je na decentraliziranom sustavu, pa bi valjalo istaknuti koja su svojstva decentralizirane arhitekture.

Od pozitivnih svojstava decentraliziranog računalnog sustava, autor Daniel Drescher izdvaja sljedeće: veća računalna snaga (eng. *computing power*), smanjenje operativnih troškova tijekom vremena (eng. *cost reduction*) te veća pouzdanost i mogućnost za prirodni rast mreže (eng. *ability to grow naturally*).[19] Veća računalna snaga posljedica je umrežavanja više računala u decentralizirani sustav.[20] Sasvim nam se intuitivno nalaže da je više računala usmjerenih k nekom cilju jače od jednog, pojedinačnog računala. Zanimljivo, ovaj slučaj vrijedi i kada, s jedne strane, uspješno povežemo više računala manje računalne snage naspram, s druge strane, jednog izoliranog super-računala izrazito snažnih komponenti. Ukoliko se odlučimo u ulaganje u decentraliziranu računalnu mrežu, utoliko će na početku troškovi biti znatno veći nego za kupnju jednog računala. Međutim, cijena konstrukcije, održavanja i rada na super-računalu je i dalje mnogo veća, nego cijena konstrukcije, održavanja i rada u decentraliziranom sustavu. Drescher navodi da se zamjena super-računala (pojedinačnog računala) decentraliziranim sustavom može odviti bez posljedica na sam sistem.[21]

[17] »Programska podrška ili softver, skup programa i podataka potrebnih za rad računala. Pod tim se pojmom obično razumijevaju svi nefizički dijelovi računalnoga sustava, za razliku od sklopovlja, koje obuhvaća sve fizičke dijelove«. Vidi: »Softver«, *Hrvatska enciklopedija*. Dostupno na: http://www.enciklopedija.hr/natuknica.aspx (pristupljeno 30. 8. 2018.).
[18] D. Drescher, *Blockchain Basics*, str. 11.
[19] Isto, str. 12.
[20] Isto.
[21] Isto.

Nadalje, veća se pouzdanost temelji na činjenici da decentralizirani računalni sistem može nastaviti s radom unatoč tome što se neko računalo unutar njega pokvari i u potpunosti prestane funkcionirati.[22] Ako jedan element zakaže, drugi preuzimaju njegovu zadaću. Stoga pojedinačno računalo, odnosno centralna softverska arhitektura, ima pouzdanost manju nego decentralizirani sistem. Mogućnost za prirodni rast odnosi se na činjenicu da se računalna snaga cijelog sistema može podići priključivanjem novih računala u postojeću mrežu.[23] Pojedinačna računala pružaju identičnu količinu snage do momenta kada ih se zamijeni novim, snažnijim računalom. Budući da se konstantno povećava potražnja za računalnom snagom, pojedinačno smo računalo prinuđeni često dograđivati i mijenjati ako želimo držati »korak s vremenom«.

Istaknuo sam četiri prednosti decentralizirane arhitektonike. Za potpunu sliku valja istražiti koje su negativne strane decentraliziranog sistema ili njegova ograničenja. Ponovno ću se osloniti na autora Daniela Dreschera koji u svojoj knjizi navodi ukupno pet razloga *contra* decentraliziranih sistema, a oni su: manjak koordinacije (eng. *coordination overhead*), manjak komunikacije (eng. *communication overhead*), ovisnost o mreži (eng. *dependency on networks*), veća programska kompleksnost (eng. *higher program complexity*) i sigurnosni problemi (eng. *security issues*).[24]

Do manjka koordinacije dolazi zbog nepostojanja centralnog entiteta koji bi obavljao taj posao. Koordinacija se nužnošću mora odvijati među samim čvorovima decentraliziranog sistema. Drescher navodi da je koordinacija posla u decentraliziranom sistemu izazovna i zahtijeva mnogo truda koji se onda ne može utrošiti na rješavanje nekog specifičnog računalnog zadatka.[25] Koordinacija također zahtijeva komunikaciju da bi računala unutar decentralizirane mreže mogla komunicirati međusobno. To zahtijeva postojanje određenog komunikacijskog protokola koji podrazumijeva slanje, primanje i procesuiranje poruka. Upravo slanje, primanje i procesuiranje zahtijeva ulaganje dostatnog truda, tj. računalne snage, koja se potom ne može upotrijebiti za rješavanje nekog specifičnog računalnog zadatka. Nadalje, bilo kakva komunikacija zahtijeva određeni medij kroz koji će se odvijati.

[22] Isto.
[23] Isto.
[24] Isto, str. 13.
[25] Isto.

Računala u decentraliziranom sistemu komuniciraju preko mreže (eng. *network*). U praksi, najčešće se radi o internetskoj mreži te bez postojanja te mreže ne može postojati komunikacija među računalima. Bez mreže i komunikacije ne postoji ni povezanost računala te se na temelju navedenog može zaključiti da kod decentraliziranih sistema postoji ovisnost o mreži. Spomenuli smo da softver u decentraliziranom sustavu mora nužno rješavati i dodatne probleme koji se tiču koordinacije i komunikacije među računalima (kakvih nema, primjerice, kod centralne arhitekture). Radi toga je kompleksnost samog softvera podignuta na višu razinu (u tehničkom pogledu). Problemi sa sigurnošću, a kojih ćemo se i kasnije u radu više dotaknuti kada ćemo ulaziti dublje u temu, tiču se slanja podataka i informacija preko postojeće decentralizirane mreže drugim nepovjerljivim čvorovima. Postoji mogućnost da ti nepovjerljivi čvorovi iskorištavaju mrežu da bi prikupili i potom iskoristili podatke i informacije u svoju korist.

Prednosti i nedostatke naveo sam da bi čitatelj imao potpuniju sliku o tome što nam decentralizirani sustav nudi. Zasad valja reći da su kreatori *blockchain* tehnologije posegnuli za decentraliziranom arhitekturom. Spomenuo sam da uz pojam *blockchaina*, osim decentraliziranosti, dolazi i pojam mreže ravnopravnih računala (eng. *peer-to-peer system*). Valja nam rasvijetliti taj pojam iz kojega možemo primijetiti da se radi o više računala koja su mrežno spojena.

Radi se, naime, o pojedinačnim čvorovima koji preko određene mreže (a koja im služi kao komunikacijski kanal) dijele podatke i informacije. Možemo također primijetiti da postoji jako velika sličnost s prethodno navedenim pojmom decentraliziranog sustava. To nije slučajnost jer pojam decentraliziranosti ide »ruku pod ruku« s pojmom mreže ravnopravnih računala. Dakle, kada govorimo o mreži ravnopravnih računala, ona je nužnom konstrukcijom povezana s decentraliziranim sustavom softverske arhitekture. Zato govorimo o decentraliziranoj mreži ravnopravnih računala (eng. *distributed peer-to-peer system*).

Budući da su čvorovi (eng. *nodes*) ravnopravni (eng. *peer* možemo doslovno prevesti kao hrv. *vršnjak*), nema potrebe da postoji neki nad-čvor koji bi provodio superviziju i koordinaciju. Posebnost decentralizirane mreže ravnopravnih računala jest dokidanje

posredništva (eng. *elimination of a third party*). U ukidanju posredništva leži veliki potencijal ovog sistema jer se podrazumijeva direktna interakcija među čvorovima.

Još jedan bitan moment kojeg ćemo kasnije u radu detaljnije obraditi jest taj da su sve informacije koje se nalaze u mreži ravnopravnih računala dostupne svim čvorovima.

2.1.3. Intrinzične vrijednosti *blockchaina*: integritet i povjerenje

Nakon objašnjenja pojma decentraliziranosti i mreže ravnopravnih računala potrebno je obrazložiti kako je *blockchain* tehnologija zapravo povezana s decentraliziranom mrežom ravnopravnih računala i u čemu je funkcionalnost te veze.

Odgovor leži u tome da *blockchain* tehnologija služi decentraliziranim mrežama ravnopravnih računala kao alat da postignu i održe *povjerenje* i *integritet*. Dvije spomenute vrijednosti izrazito su bitne jer inkorporiraju tehnički i ne-tehnički dio. O njima ne možemo razgovarati samo u tehničkom aspektu promatranja *blockchaina* i njihov smisao premašuje isključivo tehničku instancu. Povjerenje i integritet važni su nam kao vrijednosti u kontekstu *blockchain* tehnologije jer nastojanjem da ih izgradimo i zadržimo u sustavu postiže se sigurnost. Zašto nam je sigurnost važna također ćemo objasniti.

Pokušat ću definirati dvije spomenute vrijednosti: *integritet* je nefunkcionalni aspekt nekog sustava kojim se postiže sigurnost, kompletnost, konzistentnost, točnost i lišenost grešaka i korupcije. *Povjerenje* je vjerovanje u nekom odnosu u pouzdanost, istinitost ili vještine druge strane bez dokaza ili istraživanja. Povjerenje se daje unaprijed i može porasti ili se smanjiti s obzirom na interakciju.[26]

Kada sam pisao o decentraliziranoj mreži ravnopravnih računala, naveo sam da u slučaju postojanja mreže ravnopravnih računala čvorovi unutar nje, kao što sama riječ nalaže, jesu ravnopravni u vidu koordinacije i supervizije nad drugima. Ne postoji nadređenih i podređenih čvorova u takvom sustavu. Međutim, podaci i informacije u tom sustavu dijele se

[26] Za pojam povjerenja (eng. *trust*) usporedi: William Mougayar, Vitalik Buterin, »A New Trust Layer«, para. 1–10, u: *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*, John Wiley & Sons, Hoboken, New Jersey 2016. [Microsoft Edge, .epub format]

među svim čvorovima te se pojavljuje pitanje kako se unutar tog sustava može postići integritet i povjerenje bez nekog centralnog autoriteta koji će davati naredbu kako da se to izvrši. Problem se može još više zaoštriti postavi li se pitanje kako postići integritet i povjerenje u decentraliziranom sustavu ravnopravnih računala, gdje ne znamo točan broj čvorova, niti je poznato koliko se povjerenja može položiti u ostale čvorove. Dapače, pretpostavit ću najgori mogući scenarij i kazati da ne možemo uopće imati povjerenja i pouzdanosti u bilo koji čvor u sustavu. Ovaj problem javio se prije nastanka ovog rada. U literaturi se može pronaći pod nazivom – *problem bizantskih generala*.[27] Stvar postaje važna jer sam do razmatranja ovog problema došao počevši objašnjavati i proučavati *blockchain* tehnologiju. Štoviše, započeo sam prikazivati kako i zašto *blockchain* tehnologija nastoji napraviti sustav sigurnim za sve čvorove kroz vrijednosti integriteta i povjerenja. Da bi se dobio odgovor na tu problematiku valja proučiti sam tehnički postav *blockchain* tehnologije. Naime, ponuđen je odgovor u rješavanju problema bizantskih generala, a on leži u dvije tehnološke komponente *blockchaina*.

2.1.4. Prva tehnološka komponenta *blockchain* tehnologije: *hash* vrijednosti

Blockchain tehnologija sačinjena je od dvije važne tehnološke komponente. Jednu komponentu predstavljaju *hash* vrijednosti (eng. *hash values*), a drugu kriptografska tehnologija (eng. *cryptography*).

Hash vrijednosti proizvode se na temelju bitova i bajtova (eng. *bits and bytes*) koji čine neki podatak. Da bismo neki podatak transformirali u broj fiksiranih duljina[28] potrebne su nam tzv. *hash* funkcije (eng. *hash functions*). Te su funkcije mali računalni programi koji

[27] »Srodni računski izazov je tzv. *problem bizantskih generala*, a on se odnosi na situaciju u kojoj razne strane (generali) moraju imati određeni usklađeni mehanizam komunikacije na bojnom polju premda ne postoji međusobno povjerenje.« Vidi: Melanie Swan, *Blockchain*: *Blueprint for a New Economy*, O'Reilly Media, Inc., Sebastopol, California 2015., str. 2.

[28] »Fiksirana duljina [eng. *fixed length*] znači imati postavljenu duljinu koja nikada ne varira. U sustavima baze podataka polje može imati fiksiranu ili varijabilnu duljinu [eng. *variable length*]. Polje s varijabilnom duljinom je ono čija duljina može biti različita u svakom zapisu, ovisno o tome koji su podaci pohranjeni u polju. Izrazi fiksirane duljine i varijabilne duljine također se mogu odnositi i na cijeli zapis [eng. *record*]. Fiksirana duljina zapisa je ona u kojoj svako polje ima fiksnu duljinu. Zapis promjenjive duljine ima najmanje jedno polje s promjenjivom duljinom.« Vidi: Vangie Beal, »Fixed length«, *Webopedia*. Dostupno na: https://www.webopedia.com/TERM/F/fixed_length.html (pristupljeno 10. 9. 2018.). Usporedi: Eric W. Weisstein, »Hash Function«, *MathWorld*. Dostupno na: http://mathworld.wolfram.com/HashFunction.html (pristupljeno 10. 9. 2018.).

omogućuju transformaciju bilo kojeg podatka (bez obzira na veličinu ulaznih podataka; eng. *input*), u broj fiksiranih duljina. Ono što je nama za ovaj rad bitno jest specifična grupa *hash* funkcija koje se nazivaju kriptografskim *hash* funkcijama. One su posebne po tome što mogu proizvesti svojevrsni »digitalni otisak prsta« za bilo koji ulazni podatak.[29]

Ukratko ću opisati neke važnije značajke kriptografskih *hash* funkcija. Primjerice, odlika im je brzina. Omogućuju dobivanje *hash* vrijednosti za bilo koji podatak ili grupu podataka brzo. Ovo je poprilično bitna značajka ako uzmemo u obzir da se vrijeme ovdje tretira kao resurs, i to resurs koji se u ovom slučaju štedi. Nadalje, kriptografske *hash* funkcije determinističke su, što znači da sva nepoklapanja među *hash* vrijednostima koja se pojave u sustavu (primjerice da imamo dvije identične *hash* vrijednosti) nikako ne mogu biti izazvane *hash* funkcijama intrinzično. Ukoliko je došlo do poklapanja *hash* vrijednosti, utoliko je to moglo biti isključivo preko ulaznih podataka (eng. *input data*). Pojednostavljeno, greška se javlja u obrađivanim bitovima i bajtovima, a ne u *hash* funkciji. Nastavno na navedeno, valja navesti kako su kriptografske *hash* vrijednosti otporne na koliziju. Otpornost na koliziju označava da je jako teško, gotovo nemoguće, pronaći dva podatka koji bi dali identičnu *hash* vrijednost. *Hash* vrijednost sama po sebi predstavlja unikat kao što je i otisak prsta svake osobe i nemoguće je da postoje dva otiska prsta koji kolidiraju, preklapaju se. Osim navedenog, kriptografske *hash* funkcije su i pseudo-nasumične (eng. *pseudo-random*). Naime, nemoguće je predvidjeti *hash* vrijednosti na temelju ulaznih podataka.[30] Pojednostavljeno, ukoliko od jednog te istog ulaznog podataka pokušavamo više puta dobiti *hash* vrijednosti, utoliko će se ona uvijek izmijeniti i biti drugačija u svakom pokušaju. Još jedna posebnost kriptografskih *hash* funkcija jest da preko njih ne možemo pronaći originalne ulazne podatke koji su proizveli baš neku određenu *hash* vrijednost. To kriptografske *hash* funkcije čini jednosmjernim funkcijama.

Pobliže sam prikazao svojstva specifične grupe *hash* vrijednosti pod imenom kriptografske *hash* vrijednosti. Do pojma kriptografije stići ću ubrzo jer je to druga glavna

[29] »Dužina jednoga bita je uglavnom 32 simbola, a to predstavlja podatke koji su označeni. *Secure Hash Algorithm* (skrać. SHA) je kriptografska funkcija označavanja koja se koristi u *blockchainu*. SHA-256 je učestali algoritam koji generira kvazi-jedinstven *hash* fiksne 256-bitne (32-bitne) veličine. Pojednostavljeno, *hash* se može zamisliti kao digitalni otisak prsta koji služi tome da bi se podatak zaključao u mjestu unutar bloka.« Vidi: Tiana Laurence, *Blockchain for Dummies*, John Wiley & Sons, Inc., Hoboken, New Jersey 2017., str. 10.
[30] D. Drescher, *Blockchain Basics*, str. 73.

komponenta *blockchain* tehnologije. No prije toga, još ću se u nekoliko redaka zadržati na *hash* vrijednostima i spomenuti još neke pojmove.

Spomenuo sam da *hash* vrijednosti nastaju kao fiksirana duljina od podataka koje čine bitovi i bajtovi. *Hash* vrijednosti sastoje se od znamenki 0–9 ali i slova A–F u engleskom alfabetu. Kada stvaramo određenu *hash* vrijednost, primjenjujemo *hash* funkciju na određeni podatak. Taj proces naziva se *hashing*.[31] Osim pojma *hashing* spomenut ću i pojam *hash* referencija. *Hash* referencije, referiraju se na podatke koji su pohranjeni negdje drugdje, primjerice na tvrdom disku (eng. *hard disk*) ili u određenoj bazi podataka. *Hash* referencija omogućuje da se kriptografska *hash* vrijednost spoji s informacijom o tome gdje se točno nalazi određeni podatak u nekom sustavu (kada govorimo o *blockchainu* podrazumijeva se decentralizirani sustav mreže ravnopravnih računala). Ako je sam podatak u sustavu promijenjen, *hash* vrijednost tog podatka i informacija o točnoj lokaciji podatka u sustavu postaju nevažeći. Budući da se *hash* referencija odnosi (referira) na egzaktnu lokaciju nekog podatka u sustavu i njegovu *hash* vrijednost, onda i ona također postaje nevažeća.[32]

Hash referencija mogla bi se opisati i kao model zaštite unutar *blockchain* tehnologije koji nam služi da ponajprije zaštiti čvorove, odnosno krajnje korisnike od povlačenja podataka koji su bili izmijenjeni bilo namjerno, posredstvom djelovanja čovjeka, bilo slučajno nekom tehničkom greškom. *Hash* referencije koriste se u svim slučajevima kada želimo da podaci, jednom kada su stvoreni, u nekom sustavu ostanu nepromijenjeni. Dakle, *hash* referencije nam omogućavaju da pohranjujemo podatke koji su izuzetno osjetljivi i na najmanju promjenu, bilo lokacije, bilo *hash* vrijednosti.

2.1.5. Druga tehnološka komponenta *blockchain* tehnologije: kriptografija

[31] »*Hashing* je izumljen prije više od 30 godina. Dotična se stara inovacija koristi zato što stvara jednosmjernu funkciju koju se ne može dekriptirati. *Hashing* stvara matematički algoritam koji mapira podatak bilo koje veličine na niz bitova fiksne veličine.« Vidi: T. Laurence, *Blockchain for Dummies*, str. 10.

[32] »Stvorite kriptografsku *hash* vrijednost podataka koji bi trebali ostati nepromjenjivima. Kad trebate potvrditi jesu li se podatci mijenjali u kasnijem vremenu, jednostavno opet stvorite kriptografsku *hash* vrijednost podataka. Zatim usporedite novostvorenu *hash* vrijednost s *hash* vrijednošću koja je bila stvorena u prošlosti. Ako su oba *hash* podatka podudarni, onda se podatci nisu mijenjali nakon što se je stvorila prvotna *hash* vrijednost. U protivnom, podatci su se promijenili u međuvremenu.« Vidi: D. Drescher, *Blockchain Basics*, str. 82–83. Komparacija *hash* vrijednosti provodi se na temelju značajke da *hash* vrijednosti nisu podložne koliziji. Nemoguće je pronaći identične *hash* vrijednosti na temelju otpora prema koliziji. Sjetimo se, to bi bilo jednako pronalasku identičnog otiska prsta na svijetu. Postoji i drugi princip koji se tiče uočavanja promjene u podacima, a naveo sam ga u prethodnom citatu iz Drescherova djela.

Hash vrijednosti svojim tehničkim značajkama štite podatke u *blockchain* tehnologiji. Moglo bi se reći da druga tehnološka komponenta u *blockchainu* služi kao dodatni osigurač koji štiti podatke i krajnje korisnike u sustavu. Kada se piše o kriptografiji, sigurnost korisnika nastoji se postići kada korisnik šalje određene podatke u sustav i kada iz istog sustava podatke i prima. Ključno je da se zaštiti vlasništvo korisnika u oba momenta. Pritom nam valja imati na umu da *blockchain* tehnologija ovdje dolazi na pravi test jer je njen izazov zaštititi osobno vlasništvo svakog čvora (koji predstavlja tehnološku ekstenziju krajnjeg korisnika) te istovremeno omogućiti ulaz novim zainteresiranim korisnicima u decentraliziranu mrežu ravnopravnih računala. Iz te točke napetosti, dakle zaštite vlasništva svakog pojedinog korisnika u sustavu i omogućavanja ulaska novim, zainteresiranim čvorovima u koje možemo imati minimum povjerenja, pojavila se, u kontekstu *blockchaina*, kriptografija. Ona je komponenta koja omogućuje identifikaciju korisnika unutar *blockchaina* i zaštitu njihovog vlasništva.

Glavna ideja kriptografije jest ograničavanje ili potpuno onemogućavanje pristupa određenim podacima ili informacijama neovlaštenim ljudima. Zamislimo, primjerice, da postoje neki dokumenti koji su povjerljivi i ne želimo da svaka osoba u njih ima uvid. Stavit ćemo ih u sef kojeg ćemo potom zaključati te ćemo ključ staviti na povjerljivo mjesto. Ako želimo dokumente predstaviti nekoj osobi, onda ključem otvaramo sef te uzimamo dokumente iz njega i dajemo ih na uvid toj osobi. Pošto ih je osoba pregledala, dokumente ćemo vratiti u sef kojeg istim ključem zaključavamo.[33] U znanstvenom jeziku kriptografije, umjesto termina otključavanja i zaključavanja koristimo termin *enkripcija* i *dekripcija*. Pojednostavljeno, enkripcija predstavlja zatvaranje pristupa podacima, a dekripcija otvaranje pristupa podacima. U oba slučaja, potreban nam je ključ, odnosno šifra. U opisanom slučaju sa sefom, spomenuo sam da smo dokumente uzeli i vratili natrag istim ključem. Ako se u domeni kriptografije za enkripciju i dekripciju upotrebljava isti ključ, tada govorimo o simetričnoj kriptografiji. Dakle, svatko tko je bio u mogućnosti enkriptirati određeni podatak, mogao ga je dekriptirati jer se za ta dva procesa koristi isti ključ. Međutim, iskustvo je pokazalo kako nije poželjno imati isti ključ i za enkripciju i dekripciju. Razvijanjem dva različita ključa za ta dva procesa

[33] W. Mougayar, V. Buterin, »Software, Game Theory and Cryptography«, para. 1–6, *The Business Blockchain*. [Microsoft Edge, .epub format]

nastaje asimetrična kriptografija. U *blockchainu* se koristi upravo asimetrična kriptografija. U asimetričnoj kriptografiji nikada i ni u kojem slučaju ne mogu se dekriptirati već otprije enkriptirani podaci ključem koji je korišten kako bi taj isti tekst i nastao. Enkriptirani podaci zovu se i eng. *cypher text*. Dva ključa za koja smo utvrdili da postoje u domeni asimetrične kriptografije zovu se *privatni ključ* i *javni ključ*.[34] Privatni ključ može koristiti samo vlasnik, dok se javni ključ daje svima na potencijalno korištenje.[35] Slično primjeru sa sefom, upotrijebit ću primjer poštanskog sandučića[36] da bih olakšao razumijevanje problema. Naime, u poštanski sandučić svi mogu ubacivati poštu. Jednostavno je, podignemo poklopac i možemo unutra ubaciti poštu. No samo vlasnik sa svojim ključem može otključati ormarić i preuzeti svoju poštu. Sličan se princip koristi i u *blockchain* tehnologiji. Podatke vlasniku određenog čvora u sustavu može slati bilo tko iz sustava, no samo vlasnik ih može dekriptirati jedinstvenim ključem i dobiti u njih uvid. Takav javno–privatni pristup može uspješno identificirati korisnike, tj. primatelje i pošiljatelje određenih podataka u *blockchain* sustavu te između njih obaviti transakciju podataka. Da bi unutar decentraliziranog sustava ravnopravnih računala u kojem je uspostavljena *blockchain* tehnologija korisnik mogao primiti određene podatke, dovoljno je da upotrijebi privatni ključ i dekriptira podatke koje mu je prethodno pošiljatelj šaljući u sustav enkriptirao. No da bi pošiljatelj uopće mogao poslati enkriptirane podatke u sustav, potrebno je da ih ovjeri digitalnim potpisom. Na taj način *blockchain* tehnologija osigurava da samo istinski vlasnik može prenijeti svoje vlasništvo nekome drugome.

Da bi se upotpunilo razumijevanje kriptografije u kontekstu *blockchaina*, pokušat ću jezgrovito i sažeto objasniti kako funkcionira digitalni potpis. Kada želimo poslati svoje vlasništvo (odnosno podatke) nekom drugom čvoru, stavljamo digitalni potpis koji je unikatan. Digitalni potpis, radi lakšeg razumijevanja, možemo usporediti s osobnim potpisom u stvarnom, fizičkom svijetu. Kada stavljamo digitalni potpis, mi zapravo stavljamo

[34] »Jednom kad se novčanik pokrene, odnosno po prvi put uspostavi, automatski se generira adresa, javni te privatni ključ. *Bitcoin* je utemeljen na enkripciji javnog ključa, što znači da slobodno možete dijeliti javni ključ, no privatni ključ morate uvijek zadržati za sebe.« Vidi: M. Swan, *Blockchain*, str. 3. Ovdje nam je bilo važno pokazati kako u literaturi možemo naći primjere za javni i privatni ključ koji se konstruiraju po automatizmu a jako su važni za razumijevanje kriptografije. Pitanja *Bitcoina* i *kriptovaluta* dotaknut ćemo se kasnije.

[35] »Unatražni preračun u svrhu izvođenja privatnoga ključa iz javnoga je ili nemoguće ili izrazito skupo (potrebno je uložiti ogromnu računsku moć kroz duži vremenski period kako bi se provela transakcija).« Vidi: isto, str. 99.

[36] D. Drescher, *Blockchain Basics*, str. 99–100.

enkripciju privatnim ključem na određeni *cypher text* (koji dolazi od *hash* vrijednosti određenog podatka). Na taj se način preko točno tog privatnog ključa može doći do osobe koja je kreator digitalnog potpisa (osobu možemo proizvoljno nazvati Pero Perić). Budući da se u osnovi radi o *hash* vrijednosti (također unikatna), možemo jasno i precizno odrediti ne samo koji podatak je poslan nego i u kojem trenutku. Kada je naš Pero Perić stavio digitalni potpis na određene podatke koje je imao namjeru poslati drugom čvoru u sustavu, svi ostali čvorovi u mreži mogu verificirati te podatke. Naime, ostali čvorovi uočavaju određene podatke u sustavu načelom automatizma i izračunavaju njihovu *hash* vrijednost. Budući da je Pero Perić također priložio i javni ključ, svi čvorovi u sustavu javnim ključem dekriptiraju priloženi *cypher text* koji ide uz poslane podatke. Potom ponovno svi čvorovi uspoređuju svoje prvotne izračune *hash* vrijednosti poslanih podataka i dekriptiranog priloženog *cypher texta* i ukoliko dobivaju isti rezultat, utoliko se može ustanoviti da se radi o *unikatnom* digitalnom potpisu Pere Perića.[37] Na taj način recipijent na temelju verifikacije svih čvorova može potvrditi da se zaista radi o specifičnom čvoru krajnjeg korisnika Pere Perića koji je stvarni pošiljatelj poruke te se komparacijom *hash* vrijednosti podataka i *cypher texta*, ukoliko ustanovimo identičan rezultat, utoliko zaključuje da je to zaista ta poruka koju je Pero Perić želio poslati.

Premda se može činiti kompliciranim, želio sam s tehničkog aspekta jezgrovito prikazati kako funkcionira digitalni potpis kao kruna kriptografske tehnologije, a sve u svrhu zaštite krajnjih korisnika i njihovih podataka. Tim načinom mogu se spriječiti prevare: ukoliko se *hash* vrijednost podatka i *cypher texta* ne podudaraju, utoliko se lako može ustanoviti da je riječ o krivotvorenju.

2.1.6. Ustroj podataka u *blockchainu*

Ustanovio sam da *blockchain* svoju inovativnost temelji na dvije komponente: kriptografskoj tehnologiji i *hash* vrijednostima. Te sam dvije komponente nastojao opisati u najkraćim, ali opet najbitnijim crtama, pokušavajući približiti tehnološki doseg *blockchaina*.

[37] »Obzirom da se kriptografska *hash* vrijednost može smatrati digitalnim otiskom, otisci kao takvi su jedinstveni u svakoj transakciji. Bitno je obilježje kriptografije javnog i privatnog ključa da kriptirani tekst stvoren jednim ključem može biti dekriptiran jedino odgovarajućim ključem. Veza dvaju ključeva je jedinstvena. Stoga, uspješna dekripcija kriptiranoga teksta sa svojstvenim javnim ključem služi kao dokaz.« Vidi: isto, str. 106.

Spomenuo sam u definiciji *blockchaina* kako mu je glavna zadaća da u decentraliziranom modelu mreže ravnopravnih računala osigura vrijednosti povjerenja i integriteta i na taj način postigne sigurnost. Ukoliko se postigne sigurnost, utoliko je moguće provođenje najbitnije funkcije u *blockchainu* – prijenosa podataka.[38] Dakle, *hash* vrijednosti i kriptografska tehnologija nastoje pružiti sigurnost u sustavu kako bi se spomenuti prijenos podataka mogao odvijati. Budući da su svi podaci u sustavu u vlasništvu nekog čvora, a da su vlasnici tih čvorova ljudi,[39] realno možemo govoriti o prijenosu vlasništva u sustavu.[40] No da bi se razumio prijenos vlasništva, najprije trebamo imati osnovni pojam o ustroju podataka u *blockchainu* (eng. *blockchain-data-structure*). Podaci[41] u *blockchainu* ustrojeni su u obliku blokova koji su povezani lancem (otuda i ime eng. *block* + eng. *chain*; hrv. *blok* + hrv. *lanac*). Svaki blok sastoji se od dvije komponente – zaglavlja (eng. *header*) i Merkleova stabla (eng. *Merkle tree*).[42] U Merkleovu stablu nalaze se svi transakcijski podaci, a u zaglavlju se nalaze kriptografske *hash* vrijednosti za svaki pojedini blok. Još jedna inovativnost *blockchain* tehnologija nazire se u tome što pohranjuje i čuva cjelokupnu povijest o transakcijskim podacima. Sve transakcije koje su se ikad odvijale u sustavu nikada se ne brišu i uvijek, u svakom trenutku, dostupne su svim čvorovima na uvid. Osim toga, cjelokupnu povijest transakcijskih podataka gotovo je nemoguće promijeniti (eng. *immutability*).[43] Ovo svojstvo predstavlja dodatni sigurnosni prilog *blockchain* tehnologiji.[44] Načelo nepromjenjivosti podataka oslanja se na činjenicu da je bilo kakvo mijenjanje podataka unutar *blockchaina* zapravo ekstremno skupo. Teoretski postoji šansa da se podaci promijene, no velika

[38] Zašto je uopće potrebno da dođe do prijenosa podataka u *blockchainu* spomenut ćemo kasnije u radu.
[39] Misli se na krajnje korisnike u ovom slučaju.
[40] Vidi: W. Mougayar, V. Buterin, »Identity Ownerships & Representation«, u: *The Business Blockchain*. [Microsoft Edge, .epub format]. Vlasništvo i naš identitet na *blockchainu* koji označava tek nultu fazu korištenja nekih primjena te tehnologije, dva su nerazdvojna koncepta.
[41] »U suštini ne postoje namjerna i nenamjerna promjena u *blockchainu*. Ovi izrazi se zapravo odnose na motive ili osobu koja je uzrokovala promjenu. Međutim, ustroj podataka u *blockchainu* ne vrednuje ni motiv ni osobu koja je uzrokom nedosljednosti. *Blockchainu* su jedino važni dosljednost i ispravnost svih *hash* referenci. U slučaju da je jedna od njih nevaljana, onda je čitava struktura podataka nevaljana, unatoč tome tko je ili što uzrokovalo promjenu ili zašto je učinjena. Navedeno obilježje čini ustroj podataka u *blockchainu* vrlo vrijednim.« Vidi: D. Drescher, *Blockchain Basics*, str. 132–133.
[42] »Svaki blok je označen vezom prethodnih blokova, tako da su svi povezani blokovi zaštićeni od neovlaštenoga korištenja. To se naziva Merklovim stablom, koje je izumljeno 1979., te se otada uvelike koristi.« Vidi: David Gerard, »The blockchain«, para. 5., u: *Attack of the 50 Foot Blockchain*, Createspace Independent, 2017. [Microsoft Edge, .epub format]
[43] »Nepromjenjivi podatci (eng. *immutability*) znači da se podatci koji su jednom stvoreni ili napisani ne mogu više promijeniti. Zbog toga se takav tip podatka zove podatak samo za čitanje (eng. *read-only-data*).« Vidi: D. Drescher, *Blockchain Basics*, str. 137.
[44] Pogotovo ako znamo da je decentralizirana mreža ravnopravnih računala spremna uvijek prihvaćati nove čvorove i zbog toga *blockchainu* možemo pripisati i svojstvo transparentnosti.

financijska davanja u tu svrhu su zasad jedina zapreka koja će ljude natjerati da dvaput promisle žele li to zaista učiniti.[45] Osim mijenjanja postojeće strukture podataka u *blockchainu*, treba spomenuti da i dodavanje novih blokova zahtijeva ulaganje mnogo računalne snage, a slijedom toga i mnogo električne energije, što u konačnici znači i ulaganje financijskih resursa. Više o toj temi spomenut ćemo kod opisivanja *blockchain* algoritma.[46] Algoritam označava skup simbola i općeniti postupak za sustavno rješavanje pojedinačnih zadataka iz neke određene klase matematičkih problema.[47]

U opisivanju ustroja podataka u *blockchainu* preostalo mi je još spomenuti i način komunikacije među čvorovima. Zanimljivo, čvorovi komuniciraju putem »glasina« (eng. *gossip*).[48] Taj model prijenosa podataka s jednog čvora na drugi osigurava da podaci dođu brzo te da dođu do svakog čvora u sustavu.[49]

2.1.7. *Blockchain* algoritam

Opisivajući *blockchain-data-structure* saznali smo kako su podaci ustrojeni. Spomenuo sam načelo nepromjenjivosti povijesti podataka i način komunikacije među čvorovima u sustavu. Međutim, da bi se uopće došlo do te razine rasprave, najprije moramo osigurati da samo valjani podaci ulaze u *blockchain-data-structure*. Ako krenemo ustrojavati cijeli sustav na nevaljanim podacima, možemo postaviti pitanje ima li to uopće ikakvog

[45] »1. Pohranjivanje povijesti transakcijskih podataka na način da se najmanja manipulacija sadržaja ističe i tako postane primjetna; 2. Inzistiranje na manipulaciji transakcijske povijesti zahtijeva ponovno ispisivanje velikoga dijela dotične transakcije; 3. Dotjerivanje, odnosno ponovno ispisivanje povijesti podataka je računski skupo.« Vidi: isto, str. 137. Drescher navodi tri glavna razloga zašto je, iz tehničke perspektive, ekstremno skupo mijenjati ustroj podataka u *blockchainu*.

[46] Načelo nepromjenjivosti oslanja se na iznalaženja rješenja kod *hash* slagalica (eng. *hash puzzles*). Rješavanje *hash* slagalica obično zahtijeva ulaganje mnogo računalne snage. U svakom pojedinom *blockchain* sustavu postoji određenu razinu težine (eng. *difficulty level*) kod rješavanja *hash* slagalica.

[47] »Algoritam«, *Hrvatska enciklopedija*. Dostupno na: http://www.enciklopedija.hr/Natuknica.aspx?ID=1718 (pristupljeno 11. 9. 2018.).

[48] »Ideja je dopustiti računalima u peer-to-peer sustavu da dijele i razmjenjuju podatke na isti način kao što ljudi prenose vijesti. Ako čvorovi u peer-to-peer sustavu prosljeđuju podatke vršnjačkim čvorovima koji onda prosljeđuju te iste podatke svojim vršnjačkim čvorovima tada će svi čvorovi u sustavu primiti podatke. Detaljnije pojašnjeno, peer-to-peer sustav imitirat će način na koji skupine ljudi kao što su, primjerice, zaposlenici tvrtke, grupe prijatelja ili članovi sportskog kluba, međusobno komuniciraju.« Vidi: D. Drescher, *Blockchain Basics*, str. 146.

[49] »Drukčije vrste komunikacije jamče da se nova računala mogu pridružiti sustavu i prema tome doprinijeti rastu sustava. Nadalje, sustav se održava kao cjelina pomoću komunikacije s naglaskom na stvaranje novih i održavanje starih veza. Najvažnije je od svega to što sustav koristi način komunikacije nalik ogovoranju (eng. *gossip*) kako bi jamčio da na kraju svi članovi ravnopravnoga sustava prime sve transakcijske podatke i blokove, koji će se potom dodati u strukturu podataka u *blockchainu*.« Vidi: isto, str. 150.

smisla. Dakle, kada dizajniramo sustav *blockchain* tehnologije, bitno je da osiguramo da samo valjani transakcijski podaci ulaze u ustroj podataka. Što točno podrazumijeva valjane podatke i kako će se to postići? Da bismo osigurali da će samo valjane transakcije (eng. *valid transactions*) biti dodavane u *blockchain* sistem, svi čvorovi u decentraliziranoj mreži ravnopravnih računala ponašaju se kao nadglednici (eng. *supervisors*) ostalih čvorova u toj mreži. Svi čvorovi osim nadgledavanja nagrađuju i sve ostale čvorove (*nodes*) u sistemu za dodavanje valjanih i autoriziranih transakcija (eng. *valid and authorized transactions*) te za pronalaženje grešaka u radu drugih. Taj način rada potiče sve čvorove na to da podatke iz transakcija i same transakcije sprovode točno te da u nadgledavanju uočavaju i prokazuju greške ostalih čvorova.[50] Sustav nagrađivanja čvorova za dodavanje valjanih blokova je najbitnija značajka funkcioniranja *blockchain* sustava.[51]

Djelatnost *blockchain* sustava možemo nazvati i *blockchain* algoritam.[52] Kod dodavanja i nagrađivanja čvorova u *blockchain* sustavu odvijaju se složene matematičke operacije koje nećemo opisivati u ovom radu. Dovoljno je reći da ćemo sintagmu »*blockchain* algoritam« koristiti kao pojednostavljeni opis postupaka koji u konačnici dovode do izvršenja funkcije *blockchain* tehnologije.[53] Da bi čvorovi dodavali nove blokove u sistem postoji *natjecanje*. Natjecanje se može razdijeliti u dva dijela – natjecanje u brzini (koji će čvor biti najbrži u dodavanju novog bloka) te natjecanje u kvaliteti (koje se fokusira na ispitivanje valjanosti podataka novododanog bloka).[54]

[50] Isto, str. 155.
[51] »Nagrađivanje čvorova zbog uspješne dostave valjanih blokova je temeljni koncept *blockchain* algoritma.« Vidi: isto, str. 157.
[52] Usp.: Roger Wattenhofer, *The Science of the Blockchain*, Inverted forest publishing, 2016. Gotovo cijela knjiga prožeta je matematičkim operacijama koje dovode do rješenja nekog problema. U toj knjizi iz matematičko-logičke perspektive opisan je način rada *blockchaina*. Ako je čitatelj više zainteresiran za tu perspektivu može se posvetiti proučavanju algoritama koje Wattenhofer pomno opisuje u svojem djelu.
[53] Svrha *blockchaina* spomenuta je na samom početku rada u definiciji; da bismo objasnili u potpunosti kako *blockchain* funkcionira do ovog koraka nužno je bilo objasniti dvije tehnološke komponente od kojih se tehnologija sastoji te njen ustroj podataka.
[54] »Natjecanje u kvaliteti ima zanimljivi aspekt ravnopravne kontrole. Stjecanjem novoga bloka, svaki čvor shvaća da je već izgubio u pogledu brzine i da stoga mora ispunjavati ulogu suca u natjecanju po kvaliteti. Razumije se, dotični suci su najtemeljitiji i najstroži sudci koje se može zamisliti i to zato što su već izgubili u natjecanju u pogledu brzine stoga dalje nemaju više što izgubiti. U biti, svaki čvor zna da se može kad-tad vratiti u igru radi nagrade ako je u stanju dokazati da je dostavljeni blok nevaljan. U tom slučaju, natjecanje u brzini se ponovno uspostavlja, a čvorovi nanovo imaju priliku oblikovati svoj blok do kraja, čija je prethodna izgradnja inače bila prekinuta, te na kraju pobijediti u natjecanju. Rezultat je toga da će se kvaliteta natjecanja te pregleda dostavljenoga bloka obaviti na vrlo visokoj razini preciznosti.« Vidi: D. Drescher, *Blockchain Basics*, str. 158.

U bilo kojem trenutku natjecanja, svi čvorovi u sustavu nalaze se u jednoj od dviju mogućih faza. Oni: a) verificiraju novi blok koji je predan od strane drugih čvorova ili b) pokušavaju biti sljedeći čvor koji će napraviti novi blok koji će biti verificiran od strane ostalih čvorova u mreži.[55] Spomenuo sam da se svi podaci koji se nalaze unutar blokova pohranjuju u jedinstvenu povijest podataka u *blockchain* sustavu. Svi čvorovi mogu upisivati podatke u jedinstvenu povijest sustava. Problem je kako odrediti jedinstvenu povijest podataka u decentraliziranoj mreži ravnopravnih računala. Ne postoji centralni čvor koji će odrediti koja povijest podataka je točna, a u decentraliziranoj arhitekturi računala postoji mogućnost da svaki čvor stvori svoju povijest podataka. Pitanje koje se postavlja je pitanje *konsenzusa* i za *blockchain* sustav jako je važno jer ta tehnologija trenutno postiže komparativnu prednost garantirajući visoki stupanj sigurnosti. Nužno je, dakle, odrediti jedan lanac u kojeg svi čvorovi mogu upisivati povijest da bi se održala sigurnost. Međutim, osim sigurnosti, odredimo li jedan lanac oko kojeg se svi slažemo da je upravo taj i takav jedinstven, jasnije ćemo artikulirati koji podaci pripadaju kojem čvoru. Svaki čvor ukoliko predloži vlastitu povijest podataka, utoliko bi mogao pokušati maksimizirati poziciju. Utvrđivanjem jednog lanca u kojem svakome pripada onoliko koliko je zaista uložio značilo bi uvesti princip *distributivne pravednosti* – svakome po zaslugama. Ako se želi postići sigurnost sustava, onda je konsenzus oko jednog lanca u interesu svim čvorovima u sustavu. Povijest podataka vlada se principom nepromjenjivosti podataka (eng. *immutability*). Dodavanjem valjanih blokova u lanac blokova sve je manja mogućnost da neka osoba pokuša mijenjati povijest podataka.[56] Što je više vremena prošlo otkako smo konsenzusom odabrali jedan i jedinstveni lanac, u tome lancu bit će sve više blokova s valjanim podacima i postići će se konzistentnost (eng. *eventual consistency*).[57] Upravo radi konzistentnosti koja se

[55] Usporedi: »Developer Guide«, *Bitcoin*. Dostupno na: https://bitcoin.org/en/developer-guide (pristupljeno 26. 8. 2018.).

[56] Radi se o slučaju tzv. napada 51 posto (eng. *51 percent attack*) koji predstavlja jednu od najslabijih točaka *blockchain* tehnologije koja vrlo lako može postati koruptivni element i gdje upotreba tehnologije može poslužiti moralno upitnim namjerama određenih pojedinaca ili interesnih skupina. Više o napadu 51 posto spomenut ćemo u posljednjem poglavlju ovog rada.

[57] »Što se autoritativni povezani blok niže (u lancu) nalazi, to znači da se je puno prije u prošlosti povezao, tj. više je vremena prošlo otkako se je isti uključio u strukturu podataka u *blockchainu* [eng. *blockchain-data-structure*], odnosno, više se je truda uložilo u nadovezivanje blokova koji su bili na redu. Što je blok manje podložan utjecaju nasumičnih promjena blokova unutar najduže lančane poveznice, to je manja vjerojatnost da će biti isključen, tj. češće ga prihvaćaju čvorovi sustava te je bolje usidren u zajedničku povijest čvorova.« Vidi: D. Drescher, *Blockchain Basics*, str. 177.

povećava kako više vremena prolazi, tako sustav postaje otporniji na manipulativne promjene[58] i sve je teže nametnuti neki drugi lanac kao onaj pravi.[59]

2.1.8. Motivacija za korištenje *blockchaina:* sistem nagrađivanja

Opisao sam *blockchain-data-structure* i *blockchain* algoritam. Nakon što smo prošli kroz tehničke postavke funkcioniranja blockchain tehnologije, valja se zapitati – koja je motivacija neke osobe da kupi računalo i prespoji ga u mrežu decentraliziranih ravnopravnih računala? Spomenuli smo da je sustav baziran na dvije inovativne tehnološke komponente koje imaju namjeru osigurati integritet i povjerenje u sustavu ali ostaje pitanje – zašto bi to netko radio?

Kada sam spomenuo *hash* vrijednosti, namjerno sam izostavio detaljnije opisivanje jedne njihove moguće primjene da ne bih zbunio čitatelje. *Hash* vrijednosti mogu se koristiti i za izazivanje drugih računala u decentraliziranoj mreži ravnopravnih računala za rješavanje teških operacija (otprije spomenutih *hash* slagalica) koje zahtijevaju mnogo vremena, ulaganje računalne snage i posljedično, električne energije. Dolazimo do srži primjene *blockchain* tehnologije.[60] U rješavanju *hash* slagalica postoji razina težine (eng. *difficulty*

[58] Usporedi: Satoshi Nakamoto, »Bitcoin: A peer-to-peer electronic cash system«, *Bitcoin Project,* 2008. Dostupno na: https://bitcoin.org/bitcoin.pdf (pristupljeno 16. 8. 2018.). Odabir jedne povijesti transakcijskih podataka koja će odgovarati svima mogu nam uvelike olakšati dva kriterija. Naime, istražimo koji je najdulji lanac blokova u sistemu te koji je »najteži« lanac blokova u sistemu. Za najdulji lanac u sistemu potrebno je uložiti najviše računalne snage kako bi se obradilo transakcijske podatke. Više o tome može se saznati u radu nepoznate osobe pod imenom Satoshi Nakamoto. Međutim, ponekad taj kriterij ne važi, a možemo se osigurati tako da provjerimo onaj lanac koji je u svojim blokovima bilo najteže riješiti čvorovima, odnosno, u konstrukciju kojeg lanca su uložili najviše računalne snage za rješavanje *hash* slagalica (eng. *hash puzzles*). Ako u sistemu postoji dulji lanac za kojeg nismo sigurni da je pravi, možemo ih komparirati i prednost će dobiti potonji lanac. Navedeno vrijedi samo u sustavu gdje se razina težine (eng. *difficulty level*) rješavanja *hash* slagalica (eng. *hash puzzles*) određuje u toku.

[59] »Ovo je temelj sigurnosti *blockchaina* i ujedno čini osnovni razlog zašto zloćudni čvorovi ne mogu širiti novostvorene blokove koji bi inače ponovno ispisivali povijest (podataka ili transakcijskih podataka). Budući da se zahtjev mora ispuniti u trenutku i budući da njegovo zadovoljenje ovisi o sadržaju blokova, a prema tome i složenijih transakcija, stvaranje novih i valjanih blokova je teško (eng. *difficult*) i tijekom vremena iziskuje otprilike čitavu računsku moć vjerodostojnoga udijela ravnopravnih sudionika [eng. *the trustworthy portion of the mining peers*].« Vidi: Gavin Wood, »Ethereum: A secure decentralized generalized transaction ledger«, *Gavin Wood*, 2014., str. 7. Dostupno na: http://gavwood.com/paper.pdf (pristupljeno 15. 8. 2018.).

[60] »Sustavno ispitivanje svih mogućih kombinacija nema veze sa znanjem ili s misaonim zaključivanjem. Pristup otvaranju numeričkoga lokota osniva se na pukom trudu i upornosti. *Hash* slagalice su računske slagalice koje se mogu smatrati digitalnom istovrijednicom otvaranju numeričkoga lokota metodom pokušaja i pogreške.« Vidi: D. Drescher, *Blockchain Basics*, str. 89.

level) koja može biti veća ili manja te ovisno o tome zahtijevati više ili manje uložene računalne snage za njeno rješavanje. Skrenuo sam pozornost na to da u sustavu postoje i drugi čvorovi koji se međusobno natječu u rješavanju *hash* slagalica.

Upravo rješavanjem *hash* slagalica u domeni *blockchain* tehnologije dokazuje se da je uloženo potrebno vrijeme te računalna snaga i posljedično električna energija. To se naziva dokazom rada (eng. *proof of work*).[61] Verifikacijom rješenja koje su ponudili drugi čvorovi u sustavu potvrđuju se podaci koji se potom upisuju u zajednički lanac svih podataka. Međutim, ovaj proces i dalje nije održiv i teško da će se ova tehnologija proširiti ako ne postoji nagrađivanje čvorova koji sudjeluju u procesu.[62] Sustav nagrađivanja čvorova univerzalan je za sve primjene *blockchain* tehnologije kao glavni izvor motivacije za korisnike. Ono što se razlikuje je izbor konkretnog instrumenta isplate. Definicija i korištenje nekog instrumenta isplate koje se raspodjeljuje čvorovima u sustavu smatra se jednim od najvećih izazova u primjeni *blockchain* tehnologije.[63] Na ovoj točki istraživanja neizbježno se pojavljuju mnoga pitanja kako ćemo isplaćivati sredstva i tko će ih isplaćivati. Hoće li to biti neki centralni entitet? Ako hoće, nije li to protivno dosadašnjim rezultatima istraživanja pa i samom fundamentu *blockchain* tehnologije?[64]

Ako želimo *blockchain* tehnologiju koristiti isključivo za pohranu podataka, onda sa sustavom nagrađivanja ne nalazimo nikakav problem. Štoviše, on nam nije potreban. No *blockchain* tehnologija prepoznata je kao odlična podloga u novim projektima koji su imali za cilj stvoriti elektronički novac. U takve projekte savršeno se uklopilo sustavno nagrađivanje i rješavanje problema s instrumentom isplate čvorovima. Isplaćivanjem elektroničkog novca čvorovima ujedno ih se motivira da doprinose održavanju *blockchain* sustava koji se nalazi u pozadini kao tehnološko rješenje koje omogućuje sigurnost na temelju svojih komponenti.

[61] Vidi: S. Nakamoto, »Bitcoin: A peer-to-peer electronic cash system«, str. 3.
[62] »Sudjelovanje u glasovanju zahtijeva rad (eng. *costs work*) koji se nužno mora uložiti u rješavanje *hash* slagalica. Kako bi čvor primio nagradu, preuzima na sebe obavezu glasovanja ili predavanja novog bloka.« Vidi: D. Drescher, *Blockchain Basics*, str. 179.
[63] »Međutim, izbor konkretnoga instrumenta isplate kojim se kompenziraju održavatelji sustava nije identičan u svim primjenama *blockchain* tehnologije. Definicija i korištenje konkretnog instrumenta isplate kojim bi se kompenzirali svi ravnopravni članovi (eng. *peers*) za potvrđivanje (eng. *verification*) i dodavanje novih blokova u *blockchainu*, smatra se najvećim izazovom u etabliranju primjene *blockchain* tehnologije.« Vidi: isto, str. 184.
[64] Prije svega, decentralizirana mreža računala koja su ravnopravna.

2.1.9. Pojava *kriptovaluta*: dihotomija s *blockchain* tehnologijom?

Blockchain tehnologija može služiti kao baza na kojoj se rade (digitalni) projekti. Ukoliko je želimo koristiti kao tehnologiju na kojoj se temelji projekt izrade digitalnog novca, utoliko valja ustanoviti poželjna svojstva koja bi digitalni novac trebao imati.[65]

Prema svojstvima koje navodi Drescher, ističe se da je poželjno da se transakcija digitalnim novcem ne odvija preko centralnog entiteta. Ukoliko nije tako, utoliko ćemo biti u diskrepanciji s fundamentom *blockchaina* koji podrazumijeva decentralizaciju. Definitivno je poželjno da kompenzacija digitalnim novcem bude u digitalnom obliku. Fizički oblik instrumenta isplate kod digitalnog novca znatno bi otežavao isplatu, uostalom fizički novac (eng. *fiat currency*) je već domišljen kao fizički oblik instrumenta isplate. Kompenzacija u digitalnom obliku štedi mnoge resurse. Osim što je poželjno da digitalni novac bude dostupan u digitalnoj formi, treće je poželjno svojstvo prihvaćanje načina plaćanja u stvarnom svijetu. Od ostalih poželjnih svojstava koje navodi Drescher spomenut ću još i stabilnu ekonomsku vrijednost.

Ideja digitalnog novca nastala je još u prošlom stoljeću.[66] Navedene poželjne karakteristike pronašle su upravo prvom aktualnom primjenom[67] *blockchain* tehnologije dobar teren za svoje ostvarenje. Tako je nastala ideja decentralizirane mreže ravnopravnih računala koji se međusobno natječu u dostavi valjanog dokaza rada kako bi se konstruiralo i verificiralo nove blokove, pri čemu čvorovi zauzvrat dobivaju digitalni novac. Transakcijski podaci iz blokova upisuju se potom u zajedničku javnu knjigu salda.[68]

---

[65] Vidi: D. Drescher, *Blockchain Basics*, str. 186.

[66] Ekonomist Milton Friedman je 1999. godine dao intervju istaknuvši neke bitne značajke koje bi digitalna valuta trebala posjedovati. Usporedi: Charles Dearing, »Nobel Laureate Milton Friedman Predicted Bitcoin Era 17 Years Ago«, *Cointelegraph* (7. 7. 2017.). Dostupno na: https://cointelegraph.com/news/nobel-laureate-milton-friedman-predicted-bitcoin-era-17-years-ago (pristupljeno 28. 8. 2018.). Usp.: Daniel Cawrey, »How Economist Milton Friedman Predicted Bitcoin«, *CoinDesk* (5. 3. 2014.). Dostupno na: https://www.coindesk.com/economist-milton-friedman-predicted-bitcoin/ (pristupljeno 28. 8. 2018.). Usp.: Tim Collins, »The rise of Bitcoin was predicted by Nobel Prize winning economist Milton Friedman in an interview recorded 18 years ago, footage reveals«, *Associated Newspapers Ltd*. (20. 10. 2017.). Dostupno na: http://www.dailymail.co.uk/sciencetech/article-5000260/Bitcoin-predicted-Milton-Friedman-18-years-ago.html (pristupljeno 28. 8. 2018.).

[67] Vidi: W. Mougayar, V. Buterin, »Unpacking the Blockchain«, para. 5–32, u: *The Business Blockchain*. [Microsoft Edge, .epub format]

[68] Transakcijski se podaci upisuju u javnu knjigu salda (eng. *ledger*). Radi se o ekonomskom apektu *blockchaina* kojeg ćemo obraditi u narednom potpoglavlju.

»Govorim o *Bitcoinu*. Sustav *Bitcoina* ne uređuje (eng. *manages*) samo vlasništvo nad novim digitalnim novcem u potpunom decentraliziranom sustavu mreže ravnopravnih računala nego i nadoknađuje svoje članove (digitalnim) novcem čijem integritetu pridonose. Zbog činjenice da se *blockchain* snažno oslanja na kriptografiju, ova nova vrsta novca naziva se također i kriptografski novac ili skraćeno *kriptovaluta*. U pravilu, mogli biste reći da su *Bitcoin* i mnoge druge kriptografske valute poput pekarnica koje plaćaju svoje zaposlenike kruhom koje proizvode, a razlika je u tome što kruh koji proizvode zapravo predstavlja novu digitalnu valutu.«[69]

Možemo iščitati iz citata da je spomenuti digitalni novac dobio ime kriptografski novac ili kriptografska valuta (skraćeno: *kriptovaluta*). Rekli smo da je ovo bila jedna od prvih i najznačajnijih primjena *blockchain* tehnologije. Do toga je došlo jer se nastojalo riješiti problem sa sustavom nagrađivanja čvorova. Možemo reći da je pojava *kriptovaluta* u određenoj mjeri i proizvod nužnosti koji proizlazi iz samog *blockchaina*.

2.1.10. Ekonomski aspekt *blockchain* tehnologije i pojam vlasništva

O *blockchainu* se najviše piše iz ekonomskog aspekta jer je na taj način najlakše predstaviti tu tehnologiju, a primjena u vidu *kriptovaluta* ima upravo najveći utjecaj na ekonomiju.[70] Štoviše, postoje izvori koji sugeriraju da su se ideje *blockchaina* i *Bitcoina* kao prve kriptovalute javile paralelno,[71] a neki stručnjaci smatraju da su *blockchain* i kriptovalute, općenito govoreći, u velikoj dihotomiji.[72]

---

[69] Vidi: D. Drescher, *Blockchain Basics*, str. 186–187.

[70] »Dva su razloga zašto je upravljanje vlasništvom nad digitalnim dobrima najdiskutabilnija od svih primjena *blockchaina*. Prvo, taj je koncept najlakše razumjeti i objasniti. Drugo, korištenje te primjene ima najveći utjecaj na gospodarstvo (eng. *economy*).« Vidi: isto, str. 35–36.

[71] »No ima li *blockchain* tehnologija smisla bez kriptovaluta? Pitanje je to koje vrijedi postaviti, a *FreightWaves* je prošlog tjedna izvijestio s konferencije *blockchain* tehnologije organizirane od strane Digitalne komore za trgovinu u Washingtonu, D.C. gdje se raspravljalo baš o tom pitanju. Vrijedi postaviti [to] pitanje jer su se, uostalom, istodobno pojavile ideje o *blockchainu* i *Bitcoinu*.« Vidi: John Paul Hampstead, »*Blockchain* without cryptocurrencies«, *Freightwaves* (12. 3. 2018.). Dostupno na: https://www.freightwaves.com/news/blockchain/blockchain-without-cryptocurrencies (pristupljeno 23. 8. 2018.).

[72] »Što bi se moglo dogoditi ako bi se *blockchain* tehnologija ili DLT (skraćenica od eng. *distributed ledger*) usvojili bez kriptovalute? 1. San utemeljitelja *Bitcoina* bit će uništen; 2. Poduzeća i Vlade će izgraditi više pouzdanih informacijsko-tehnoloških (IT) sustava; 3. *Blockchain* će biti skrivena tehnologija nalik na *Big Data*, tako da građani, tj. potrošači neće shvatiti da (*blockchain*) bilo što revolucionizira; 4. Protokoli će postati alat IT svijeta, udaljen od većine ljudi.« Vidi: Nikolay Syusko, »Is there a chance for blockchain without

Iz rada Satoshija Nakamota može se uočiti da se ideja digitalnog novca nadogradila na ideju *blockchain* sustava. Dopustite dulji citat iz njegovog rada:

»Trgovina na internetu počela se gotovo isključivo oslanjati na financijske institucije koje služe kao povjerljive treće strane (eng. *third parties*) za obradu elektroničkih plaćanja. Premda taj sustav funkcionira dovoljno dobro za većinu transakcija još uvijek pati od inherentnih slabosti modela temeljenog na povjerenju. Potpuno nepovratne (eng. *non-reversible*) transakcije zapravo nisu moguće jer financijske institucije ne mogu izbjeći posredovanje u sporovima. Trošak posredovanja povećava transakcijske troškove čime ograničava minimalnu praktičnu veličinu transakcije i odbija mogućnost malih povremenih transakcija, a postoji i širi trošak u gubitku mogućnosti da se naplaćuju nepovratne uplate za nepovratne usluge. S mogućnošću povrata (sredstava), širi se potreba za povjerenjem. Trgovci moraju biti nepovjerljivi prema svojim kupcima, tj. gnjaviti ih radi više informacija nego što bi inače trebali. Određeni postotak prijevare se uzima kao neizbježan. Ti se troškovi i neizvjesnosti plaćanja mogu izbjeći koristeći fizičku valutu, ali ne postoji mehanizam za plaćanje putem komunikacijskog kanala bez pouzdane (treće) strane. Ono što je potrebno jest elektronički sustav plaćanja koji se temelji na kriptografskom dokazu umjesto povjerenja, što omogućuje objema stranama da posluju među sobom, izravno, bez potrebe za pouzdanom trećom stranom. Transakcije koje je računski nepraktično poništiti bi zaštitile prodavače od prijevara, a rutinski sigurnosni mehanizmi bi se lako mogli primijeniti kako bi zaštitili kupce. U ovom radu predlažemo rješenje problema s dvostrukim plaćanjem (eng. *double spending*) koristeći decentralizirani *peer-to-peer* server sa vremenskim žigom (eng. *peer-to-peer distributed timestamp server*) u svrhu generiranja računskoga dokaza kronološkog redoslijeda transakcija. Sustav je siguran dokle god iskreni čvorovi kolektivno kontroliraju više CPU-ovske (procesorske) snage od bilo koje suradničke grupe (potencijalno) napadačkih čvorova.«[73]

Iz ovog citata možemo zaključiti kako decentralizirana mreža ravnopravnih računala daje veću garanciju sigurnosti korisnicima, nego što je to mogla učiniti ijedna tehnologija

Cryptocurrencies«, *Hackernoon* (31. 7. 2018.). Dostupno na: https://hackernoon.com/is-there-a-chance-for-blockchain-without-cryptocurrencies (pristupljeno 23. 8. 2018.).

[73] Vidi: S. Nakamoto, »Bitcoin: A peer-to-peer electronic cash system«, str. 1.

prije. To dodatno zaoštrava argumentaciju u smjeru njene korisnosti. No što to čini ekonomski aspekt posebno privlačnim, a kriptovalute tako popularnom ekstenzijom *blockchaina*? Prije svega, *blockchain* tehnika je kod. Ona se može dizajnirati prema preferencijama:

»Prije no što počnete razvijati *blockchain* tehnologiju, morate se zapitati što želite učiniti s njom. Budući da želite dizajnirati softverski sustav koji upravlja vlasništvom, morate prije svega odlučiti kako opisati vlasništvo. Ispada da su transakcije dobar način kako opisati bilo koji prijenos vlasništva, a cjelovita povijest transakcija ključ je za identifikaciju trenutnih vlasnika.«[74]

Ključna riječ koju uočavamo jest – *transakcija*. Najprije trebamo dokučiti što bi predstavljali transakcijski podaci. Vlasništvo (ne samo strogo formalno nego i sadržajno) u ovoj tehničko-ekonomskoj domeni to nužno zahtijeva.[75] Transakcijski podaci opisuju transfere vlasništva. Možemo ih usporediti s bankovnim računima na kojima se mogu vidjeti datumi isplate ili uplate novca. Nasuprot transakcijskim podacima, postoje inventarski podaci koji opisuju trenutno stanje vlasništva. Razlika između te dvije vrste podataka u tome je što potonjim saznajemo trenutno posjedovno stanje korisnika, dok nam transakcijski podaci objašnjavaju i opravdavaju vlasništvo.[76]

Ako se vratimo na raniji citat iz rada Satoshija Nakamota, možemo vidjeti da se na kraju uvoda osvrnuo na sve komponente *blockchaina* koje smo dosad spomenuli. Stanovita ekstenzija tome, na temelju njegove preferencije, jest digitalni novac. Zato je i pokrenut

[74] Vidi: D. Drescher, *Blockchain Basics*, str. 59.
[75] »Koncept vlasništva i provođenje vlasničkih prava su temeljni elementi gotovo svakog ljudskoga društva (čak neke životinje imaju koncept vlasništva i borbu za prepoznavanje vlasništva). Velik dio aktivnosti banaka, osiguravajućih društava, skrbnika, odvjetnika, sudova, odvjetnika i konzulata tiče se upravljanjem vlasničkim pravima ili njihovom provedbom. Upravljanje vlasništvom tržište je čija se vrijednost procjenjuje na više milijardi dolara, a svaka tehnička inovacija koja bi mogla promijeniti način upravljanja vlasništvom izvršila bi ogromni utjecaj na njega. Ispada da *blockchain* uistinu može dramatično promijeniti način upravljanja vlasništvom.« Vidi: isto, str. 36.
[76] »Postoje dva konkurentna načina za opisivanje vlasništva – putem podataka o inventaru ili podataka o transakciji. Podaci o inventaru opisuju trenutno stanje vlasništva. Oni su slični izvatku stanja bankovnog računa koji samo prikazuje iznos novca koji je trenutno dostupan. Podaci o transakcijama opisuju prijenos vlasništva. Oni su slični izvatku stanja bankovnoga računa koji navodi svaku isplatu, polog i prijenos novca. Podaci o inventaru mogu se izvući iz zbroja svih transakcijskih podataka. Osim činjenice da i podaci o inventaru i podaci o transakcijama opisuju vlasništvo, njihova se temeljna filozofija drastično razlikuje. Podaci o inventarnim jedinicama samo navode ili iskazuju vlasništvo dok podaci o transakcijama objašnjavaju (porijeklo vlasništva) i time opravdavaju vlasništvo.« Vidi: isto, str. 64–65.

projekt *Bitcoin*, projekt prve *kriptovalute*. U sustavu *kriptovaluta* čvorovi uživaju sve benefite *blockchain* tehnologije dok konstantnim dostavljanjem dokaza rada (ili eng. *mining*) bivaju najčešće nagrađivani dobivanjem *kriptovalute* u čijem sustavu se nalaze. *Kriptovalute* postižu određenu vrijednost koja se može provjeriti na burzi.[77] Možemo ustanoviti da je vrijednost izuzetno volatilna, odnosno da jako oscilira iz dana u dan, čak iz sata u sat.[78] Kod većine kriptovaluta transakcijski podaci upisuju se u javnu knjigu salda koja je svima dostupna. Pojam javne knjige salda smo također spomenuli u proizvoljnoj definiciji na početku rada. Javna knjiga salda čuva transakcijske podatke po uzoru na *blockchain-dana-structure*, a također se po uzoru na *blockchain* algoritam koristi i konsenzus većine čvorova da bi se odabrao lanac koji vjerodostojno opisuje vlasništvo čvorova i provedene međusobne transakcije. Uzima se i kriptografski model da bi se pomoću pravila identifikacije, autorizacije i autentifikacije utvrdili stvarni vlasnici transakcijskih podataka u tom sustavu. Dakle, koriste se sve prednosti, a pojam vlasništva čini bitnu razliku radi čega možemo ustanoviti postojanje i važnost ekonomskog aspekta *blockchain* tehnologije.

2.2. Razlikovanje *blockchain* tehnologije od prethodnih tehnologija

U ovom ću poglavlju sažeti sve dosad napisano o *blockchain* tehnologiji i napraviti svojevrsni *summae summarum* koji ocrtava njenu inovativnost i komparativnu prednost pred drugim tehnologijama. Za to će mi poslužiti sedam principa na kojima leži idejno i arhitektonsko rješenje *blockchain* tehnologije:[79]

1) Umreženi integritet (eng. *Networked integrity*). Prvi princip su vrijednosti integriteta i povjerenja u sustavu kojeg *blockchain* nastoji postići. Tapscott će reći

[77] Vidi službenu stranicu burze. Dostupno na: https://coinmarketcap.com/ (pristupljeno 20. 8. 2018.).
[78] Tržišna kapitalizacija na dan 11. 9. 2018. iznosi 193,743,395,185 (riječima: sto devedeset tri milijarde, sedamsto četrdeset tri milijuna, tri stotine devedeset i pet tisuća, sto osamdeset i pet) američkih dolara, a volumen burze u 24 sata (sveukupna vrijednost svih transakcija) iznosi 11,002,141,063 (riječima: jedanaest milijardi, dva milijuna, sto četrdeset i jedna tisuća, šezdeset i tri) američkih dolara**.** Početkom ove godine, točnije 7. 1. 2018. Kapitalizacija tržišta iznosila je 813,871,000,000 (riječima: osamsto trinaest milijardi, osamsto sedamdeset i jedan milijun) američkih dolara, a volumen je iznosio 44,060,500,000 (riječima: četrdeset četiri milijarde, šezdeset milijuna, petsto tisuća) američkih dolara. Usporedi: https://coinmarketcap.com/charts/ (pristupljeno 11. 9. 2018.).
[79] Usporedi: Alex Tapscott, Don Tapscott, »The seven design principles of the blockchain economy«, u: *Blockchain Revolution*, Brilliance Audio, 2016. [Microsoft Edge, .epub format]

da su te vrijednosti upisane u kod *blockchaina*, ali to ne znači da su ljudi od njih amnestirani. Upravo suprotno, ako gledamo na tehnologiju kao produkt čovjekova rada i umnog dostignuća, koji ima za cilj olakšati i pojednostavniti određene poslove, tada shvaćamo da referentna točka tehnologije podrazumijeva čovjeka. Što to sve implicira, zašto su te vrijednosti generalno govoreći bitne, predstavit ćemo u nastavku rada kada ćemo sagledati, prije svega, ne-tehnički aspekt *blockchaina*.

2) Decentralizirana snaga (eng. *Distributed power*). Drugi princip je decentralizirana mreža. Nepostojanje centralnog entiteta daje svima mogućnost da doprinose sustavu i provode superviziju nad drugim čvorovima. Decentralizacija u savršenom obliku predstavlja ideju direktne demokracije.[80]

3) Vrijednost kao poticaj (eng. *Value as incentive*). Rad na inherentno upisanim vrijednostima u samoj tehologiji *blockchaina* motivirajuća je za sve čvorove i potiče ih da čim više doprinose sustavu jer postoji sustav nagrađivanja. On se najbolje manifestira kroz najpoznatiju primjenu *blockchaina*, a to su *kriptovalute*. Imamo mogućnost upisati vrijednost u određeni tehnološki projekt temeljen na *blockchainu* i određenom kompenzacijom motivirati krajnje korisnike da našem projektu doprinose kroz spajanje čvorova u decentraliziranu mrežu. Ovakav moment u tehnološkom svijetu prije nije bio poznat, a između ostaloga i sustav nagrađivanja daje *blockchainu* komparativnu prednost pred drugim tehnološkim rješenjima.

4) Sigurnost (eng. *Security*). Sigurnost je također inovativni moment kojeg nam nudi *blockchain*. Sigurnost se nastoji postići kroz doprinos svih čvorova vrijednostima koje su kreatori u njega upisali. Dvije komponente od kojih se sastoji sam *blockchain*, kriptografija i *hash* vrijednosti, upravo to i omogućuju.

[80] Carl Miller, »TEDx Talks: Digital Democracy«, *YouTube* (4. 5. 2016.). Dostupno na: https://www.youtube.com/watch?v=FNL22RvFwn0 (pristupljeno 11. 9. 2018.).

5) Privatnost (eng. *Privacy*). Privatnost u domeni *blockchaina*, premda predmet rasprave za neke pa i za samog Tapscotta, inovativna je utoliko što se pokušava postići u decentraliziranom sustavu s pretpostavljenim minimumom povjerenja prema svim ostalim čvorovima. U *blockchainu* postoji točka napetosti između privatnosti i transparentnosti. Naime, kako očuvati pravo na privatnost svakog čvora u decentraliziranoj mreži, a pritom je učiniti otvorenom za sve pitanje je koje sam već prethodno i postavio. Međutim, sama činjenica da se ona spominje i da se na nju obraća pažnja je već veliki korak koji bi mogao rezultirati ponudom tehničkih rješenja u budućnosti.

6) Očuvana prava (eng. *Rights preserved*). Koncept što čini razliku i jednu od glavnih značajki *blockchaina* je tzv. *pametni ugovor* (eng. *smart contract*). Pametni ugovor omogućuje prijenos vlasništva s jednog čvora na drugi, pri čemu sam sustav, odnosno ostali čvorovi, mogu verificirati poštuju li obje strane dogovoreno u ugovoru te u slučaju spora mogu biti posrednici.[81] Radi se o krajnjoj implikaciji ukidanja posredništva u domeni *blockchaina*. Ovakav način uređivanja vrijednosti povjerenja među krajnjim korisnicima može imati široke i značajne implikacije na poslovni svijet, ali ponajprije na pravne regulative. Paradigma bi se mogla preseliti na digitalne platforme, što podrazumijeva određene promjene i nudi benefite, ali neizostavno i nedostatke.

7) Inkluzija (eng. *Inclusion*). Možemo se zapitati koliko je zapravo inkluzivna *blockchain* tehnologija? Jared Norton navodi da ono što *blockchain* tehnologiju čini drugačijom jest da ona može biti inkluzivna za sve.[82] Kao razlog navodi da ne postoje pravila (barem zasad) prema kojima netko smije ući u svijet *blockchaina*, nikakve ulazne naknade (osim minimuma koji zahtijeva da posjedujete neku vrstu mobilnog uređaja s kojom se spajate na internet) i »prijateljsku okolinu« zahvaljujući načelu anonimnosti. Naime, ako pojedinoj fizičkoj osobi želim pružiti

[81] Usporedi: M. Swan, *Blockchain*, str. 16.
[82] Jared Norton, *Blockchain*: *Easiest Ultimate Guide To Understand Blockchain*, CreateSpace Independent Publishing Platform, 2016., str 19.

neku uslugu, mogu to učiniti uz minimalni rizik, odnosno veliku sigurnost prema ljudima kojima ne trebam znati ni njihovo ime i prezime.[83]

Svaki od navedenih principa podložan je raspravi iz više aspekata. Međutim, *blockchain* tehnologija nesumnjivo predstavlja inovativnost današnjice, inkorporirajući sve navedene principe. Kako će se oni koristiti, za koju namjenu, koje prednosti nude, gdje se kriju nedostaci te još mnoga pitanja dolaze zajedno s njima. Na njih ne možemo dati potpuni i apsolutni odgovor jer će razvitak i upravljanje ovom tehnologijom tek u budućnosti na njih ponuditi odgovore, ali nesumnjivo i otvoriti mnogo specifičnija i konkretnija pitanja.

2.3. Aktualna primjena *blockchain* tehnologije

Pišući o ekonomskom aspektu *blockchaina*, istaknuo sam da se najaktualnija uporaba danas promatra kroz *kriptovalute*. A kada se spomenu *kriptovalute*, neizostavno je spomenuti *Bitcoin*. Treba naglasiti kako je on najpopularnija i najpoznatija *kriptovaluta* s kojom priča o razvijanju *blockchaina* i ideje elektroničkog novca po prvi puta dobiva svoje realno lice i naličje:

»*Bitcoin* je prvenstveno dizajniran za slanje *Bitcoinove* kriptovalute. Međutim, kreatori su vrlo brzo shvatili da (*Bitcoin*) ima puno veći potencijal. Imajući to na umu, dizajnirali su *blockchain* sustav *Bitcoina* koji može ubilježiti više od samih podataka koji se odnose na kretanje *tokena* (približan prijevod jest hrv. vaučer). *Bitcoinov* sustav *blockchaina* najstariji jei jedan od najvećih na svijetu. Sastoji se od tisuća čvorova koji održavaju (eng. *running*) *Bitcoinov* protokol. Protokol stvara i osigurava *blockchain*.«[84]

Kada je ideja *blockchaina* dobila gotovo prirodnu ekstenziju u *kriptovalutama*, upravo je *Bitcoin* postao simbolom te evolucije i, može se reći, njegovom je pojavom započeo rad i na drugim projektima *kriptovaluta* te se sveukupna vrijednost tržišta *kriptovaluta* povećala.

[83] Isto, str. 20.
[84] T. Laurence, *Blockchain for Dummies*, str. 43.

Druga najpopularnija ili najpoznatija *kriptovaluta* u ovom trenutku, sudeći prema burzi,[85] je *Ethereum*:

»*Ethereum* je prvi put opisan 2013. god. u dokumentu koji je napisao Vitalik Buterin; on je bio vrlo aktivan u zajednici *Bitcoina* kao pisac i programer. Buterin je vidio da u *Bitcoinu* postoji znatno više potencijala od samog premještanja vrijednosti bez središnjeg autoriteta. Pridonio je naporima pri stvaranju obojenih novčića u *Bitcoinu* kako bi proširio korisnost *Bitcoina* izvan trgovine njegovog izvornoga *tokena*. Buterin je vjerovao da bi poduzeća, Vlade i svi drugi entiteti koji inače zahtijevaju središnji autoritet u vidu kontrole, također mogli biti izgrađeni na strukturi *blockchaina*.«[86]

Razlog tome nazire se i iz ovog citata. Priča o *kriptovalutama* dobila je svoj nastavak nakon *Bitcoina* u *Ethereumu.* On poboljšava tehničke performanse i nedostatke uočene u sustavu *Bitcoina* te veliku pažnju posvećuje inovativnosti i konceptu održivosti.[87] U trenutku kada nastaje ovaj rad, osim *Bitcoina* i *Ethereuma* postoji skoro dvije tisuće projekata *kriptovaluta*.[88] U ovom radu nećemo analizirati sve, ali ćemo ipak spomenuti još jedan projekt *kriptovalute* koja se čini zanimljivom. Naime, postoji *kriptovaluta* koja nudi anonimnost transakcijskih podataka, a naziva se *Dash*. To je druga *kriptovaluta* koja se razvila odmah nakon *Bitcoina*. Kreatori ovog projekta komparativnu prednost na tržištu pred drugim valutama nastoje postići anonimnošću, a tvrde da nastoje poboljšati rješenja za problem dvostrukog trošenja (eng. *double spending*),[89] koji je jedan od razloga radi kojeg anonimni

[85] Vidi službenu stranicu burze: https://coinmarketcap.com/ (pristupljeno: 27. 8. 2018.). Jasno je vidljivo da već neko vrijeme *Ethereum* kotira kao druga po redu *kriptovaluta* na burzi, odmah iza *Bitcoina*. Iako vrijednosno nisu ni približno jednaki, upravo zbog principa održivosti i potencijala u budućnosti *Ethereum* drži visoko, drugo mjesto.

[86] T. Laurence, *Blockchain for Dummies*, str. 52.

[87] »*Serenity* je posljednja planirana faza razvoja *Ethereuma*. Tamo će se *Ethereum* preseliti iz konsenzusa u modelu dokaza-o-radu [eng. *proof-of-work*], u kojem se rudari [eng. *miners*] natječu za stvaranje sljedećeg bloka, na model dokaza-o-udjelu [eng. *proof-of-stake*]. U modelu dokaza-o-udjelu čvorovi se odabiru pseudo-nasumično s tim da se mogućnost da se čvor odabere povećava na temelju udjela u mreži. Njihov udio mjeri se količinom *kriptovalute* u njihovu posjedu. Glavna prednost ove promjene bit će smanjenje troškova energije. To bi moglo privući pojedince da vode čvorove u mreži što bi povećalo decentralizaciju i sigurnost.« Vidi: isto, str. 53. Ovaj citat navodim kako bih pokazao zašto *Ethereum* tako dobro kotira na burzi *kriptovaluta*. U široj slici valja imati na umu kako se *blockchain* tehnologija kroz prizmu *kriptovaluta* neprestano poboljšava u tehničkoj izvedbi, a s pojavom više projekata stvara se i raznolikost tržišta i stvara se sve više modela uporaba.

[88] Vidi: »All Cryptocurrencies«, *CoinMarketCap*. Dostupno na: https://coinmarketcap.com/all/views/all/ (pristupljeno 11. 9. 2018.).

[89] »*Dash* je *kriptovaluta* koja nastoji biti maksimalno prilagođena korisnicima [eng. *user-friendly*] i najpodesnija raznim plaćanja na svijetu. *Dash* mreža ima trenutačnu potvrdu transakcije, zaštitu od dvostrukog plaćanja (eng. *double spending*), anonimnost koje pruža plaćanje gotovinom, samoupravni i samofinancirajući model kojega

Nakamoto i pristupa razvijanju ideje *Bitcoina*.[90] Osim *kriptovaluta*, postoji i nekoliko projekata izvan te domene koji uzimaju *blockchain* kao fundamentalnu tehnologiju na kojoj grade svoje poslovanje. Navest ću neke od njih.[91]

R3 je tvrtka koja je na temelju *blockchain* tehnologije razvila platformu *Corda*.[92] Platforma služi kako bi smanjila troškove poslovnih transakcija između poslovnih subjekata koristeći pametne ugovore (eng. *smart contracts*). Na njihovoj internetskoj stranici navedeno je da svoj projekt usmjeruju specifično za poslovanje (»*Corda* je uspostavljena specifično za poslovni svijet.«).[93] Projekt *OpenBazzar* ne predstavlja tvrtku ni organizaciju. To je *open source* projekt koji predstavlja virtualnu tržnicu. Budući da *blockchain* tehnologija eliminira posrednike na ovaj način, na temelju *blockchain* tehnologije na internetu možete direktno prodavati i kupovati robu. Možete koristiti i *Bitcoin* te više od 50 *kriptovaluta* kao sredstvo plaćanja, a jedna od posebnosti je i da ne morate plaćati naknadu da biste kupovali ili prodavali putem te platforme.[94] *Bitfury* grupa razvija softverska i hardverska rješenja s *blockchainom* kao bazom. Na svojoj internetskoj stranici navode da su najveća tvrtka na svijetu koja u potpunosti operira u *blockchainu*, a svoje poslovanje usmjeruju prema poslovnim subjektima, Vladama država te drugim zainteresiranim organizacijama. Činjenica da ova tvrtka ima urede u 11 zemalja diljem svijeta[95] govori nam koliko se koncept *blockchaina* već proširio.

---

pokreću motivirani puni čvorovi [eng. *full nodes*] i jasni putokaz [eng. *roadmap*] za mjerenje do 400 MB blokova korištenjem jedinstveno razvijenog hardvera otvorenog koda [eng. *open source hardware*] (...) ove ali i mnoge druge ključne značajke izdvajaju *Dash* u ekonomskom aspektu *blockchaina* [eng. *blockchain economy*].« Vidi: Vidi: »What is Dash?« *Dash Core Group*. Dostupno na: https://docs.dash.org/en/latest/introduction/about.html (pristupljeno 23. 8. 2018.).

[90] S. Nakamoto, »Bitcoin: A peer-to-peer electronic cash system«, str. 1.

[91] Usporedi: T. Laurence, *Blockchain for Dummies*, str. 193.

[92] »*R3*-ova tri stupa (djelovanja) su sljedeća: kvalitetan financijski *blockchain* [eng. *financial-grade blockchain*]: *R3* je razvio tehnologiju osnovnog sloja [eng. *base layer technology*] koja podržava potrebe globalne financijske institucije; istraživanje i razvoj: *R3* je stvorio bilateralni istraživački centar koji ispituje i stvara industrijske standarde za komercijalni stupanj tehnologije povezanih blokova; razvoj proizvoda: *R3* usko surađuje s institucijama radi stvaranja proizvoda koji rješavaju probleme duž lanca vrijednosti.« Vidi: T. Laurence, *Blockchain for Dummies*, str. 193.

[93] Vidi: »The Corda Platform, Blockchain for every business in every industry«, *R3*. Dostupno na: https://www.r3.com/corda-platform/ (pristupljeno 23. 8. 2018.).

[94] Vidi: »The Story of Openbazaar«, *Openbazzar*. Dostupno na: https://www.openbazaar.org/ (pristupljeno 23. 8. 2018.).

[95] Vidi: »About Bitfury«, *Bitfury Group Limited*. Dostupno na: https://bitfury.com/about (pristupljeno 23. 8. 2018.).

3. Određivanje etičkih temelja *blockchain* tehnologije

Nakon obrade tehničkog aspekta, prelazim na istraživanje ne-tehničkog u *blockchain* tehnologiji. Ne-tehničko najprije označava etičko. Da bismo uspješno trasirali istraživački put do određenja etičkih temelja, krenuo sam s pregledom etičkih pravaca i identificiranja etika korisnih za razumijevanje *blockchaina*.

3.1. Pregled etičkih pravaca

Za potrebe ovog rada, u etici kao filozofskoj disciplini proučavanja morala, razdvojit ću meta-etiku, normativnu etiku te primijenjenu etiku.[96] Premda ne postoji čvrsta i općeprihvaćena razdioba, ovdje ću je uvjetno konstruirati da bih detektirao gdje se nalazi etički temelj *blockchain* tehnologije.

Metaetika, najkraće rečeno, proučava narav i metodologiju moralnih odluka.[97] U metaetici raspravljamo o tome što uopće znači »dobro« i što znači »činiti dobro«, postoje li uopće moralne istine te možemo li opravdati i racionalno braniti svoja uvjerenja o tome što je »dobro«, a što je »zlo«.[98] Normativna etika, kao što i sam naziv nalaže, teži uspostavljanju normi koje vrijede općenito. Kod normativne etike postavlja se pitanje »kako trebamo živjeti?«. Unutar normativne etike možemo razlikovati konsenkvencijalističku etiku te deontološku etiku.[99] Primijenjena etika nastoji donijeti opravdane zaključke za stvarne scenarije koji se najčešće odvijaju u određenom vremenskom roku kada je potrebno donijeti odluku, a pritom se često događa da nam u trenutku kada je odluku potrebno donijeti nisu podastrte sve pouzdane informacije. Primijenjena etika proučava konkretne slučajeve u kojima postoji moralna dvojba, poput laži ili pobačaja.[100]

---

[96] Podjela koju sam predložio u vidu šire etičke rasprave o oblicima etičke analize svakako je problematična i upitna, ali u svrhu ovog rada pragmatična.
[97] Harry J. Gensler, *Ethics. A Contemporary Introduction*, Routledge, New York 2011., str. 3.
[98] Geoff Sayre-McCord, »Metaethics«, *The Stanford Encyclopedia of Philosophy*, 2014. Dostupno na: https://plato.stanford.edu/archives/sum2014/entries/metaethics (pristupljeno 16. 8. 2018.).
[99] H. J. Gensler, *Ethics*, str. 110.
[100] Isto, str. 3.

S ovom razdiobom u vidu, prisjetimo se najvažnije značajke *blockchain* tehnologije: ona ima namjeru izgraditi i zadržati integritet i povjerenje u decentraliziranoj mreži ravnopravnih računala (u kojoj ne možemo procijeniti razinu povjerenja u ostale čvorove) putem kriptografske tehnologije i *hash* tehnologije. U tom i takvom sustavu transakcijski podaci koje razmjenjuju svi čvorovi dostupni su u javnoj knjizi salda i vidljivi su u svakom trenutku. Iz ove skraćene definicije obratimo pažnju na dvije vrijednosti koje proučavana tehnologija nastoji izgraditi i zadržati. Iako se, s tehničke strane, to osigurava tehnološkim komponentama, i dalje postoji ne-tehnički faktor. Naime, računala današnjeg doba još uvijek su probabilistička i nisu razvila ni svijest ni samosvijest te ne mogu odlučivati bez programiranja. Čovjek je taj koji programira računala te je upravo on predstavnik ne-tehničkog aspekta. I *blockchain* je izgrađen od ljudi za ljude i poput svake druge tehnologije, uspješnom se može smatrati ako se integrirao u društvo i »živi« od ljudi. Nastojao sam pronaći etiku koja bi bila najviše podesna za ispitivanje *blockchain* tehnologije, pritom uzevši u obzir i tehnički i ne-tehnički aspekt.

3.2. Identificiranje etika korisnih za razumijevanje *blockchain* tehnologije

Vjerojatno se logičnim čini da u problematiku krenem iz pozicije primijenjene etike. Naime, Peterson se slaže da je jako bitno razdvojiti normativnu i primijenjenu etiku jer normativna etika želi pronaći uzročno opravdanje, dok se primijenjena etika tiče specifičnih situacija u stvarnim događajima.[101] Također navodi da odgovor na rješenje praktičnih moralnih problema možemo tražiti iz oba aspekta (primijenjena etika i normativna etika) i to u samom početku ne znači da će naš rezultat istraživanja biti nevaljan. Međutim, Peterson razvija svoju teoriju dalje i smatra da etičke teorije ne mogu donijeti konačnu moralnu presudu u pitanjima primijenjene etike. Kod primijenjene etike ne možemo znati postoji li ikoja točna etička teorija. Upravo iz tog razloga smatra da treba primijeniti pet specifičnih principa za određenu domenu (eng. *domain–specific principles*). Upravo to predstavlja središnji dio njegove knjige *Ethics of Technology*. Dakle, prema Petersonu, u svijetu tehnologije postoji pet specifičnih principa koji nam pomažu da donesemo odluku u

[101] Martin Peterson, *The Ethics of Technology*. *A Geometric Analysis of Five Moral Principles*, Oxford University Press, New York 2017., str. 5.

pojedinom slučaju gdje postoji moralna dilema: *cost–benefit* princip, princip opreza, princip održivosti, princip autonomije i princip poštenosti.[102]

Ukoliko želimo pronaći odgovor na pitanje je li opravdano da se sprovede napad 51 posto[103] u *blockchain* sustavu, utoliko bismo ga trebali provući kroz spomenutih 5 principa. Međutim, to nam i dalje ne govori ništa o ne-tehničkom aspektu:

»Svaki princip navodi nužan uvjet da tehnološka intervencija bude moralno ispravna, ali ni jedan pojedinačni princip nije dovoljan za određivanje ispravnosti intervencije samostalno. Ispravnost nekih tehnoloških intervencija ovisi o nekoliko načela.«[104]

Nas u ovom momentu ne zanima moralna implikacija upotrebe *blockchaina* kao tehnologije u pozadini, primjerice, digitalnog sustava glasovanja. Zanimaju nas vrijednosti koje su ugrađene u srž tehnologije, a Peterson ih u opisivanju pet principa uzima kao dane i piše primarno o ispravnosti upotrebe, kao što se može iščitati iz citata. Nadalje, opisivanje potencijalnih napadača bilo bi u domeni deskriptivne etike. Budući da je razvijanje *blockchain* tehnologije još uvijek u tijeku, imamo premalo informacija prema kojima možemo dati opis na temelju kojeg bismo mogli utemeljiti potencijalnu primijenjenu etiku za *blockchain*. Zadržao bih se na onome što znam. Nalazimo se u domeni primijenjene etike te smo ušli u jedan njen dio – etiku tehnologije. U tom području Luciano Floridi iskovao je dva veoma zanimljiva termina koja će nam pomoći smjestiti problematiku ovog rada u kontekst. On govori o info-sferi (eng. *infosphere*) i re-onologizaciji (eng. *re-ontologizing*).[105]

Infosfera je termin koji je nastao po uzoru na biosferu. On obuhvaća cjelokupni informacijski okoliš koji se sastoji od informacijskih entiteta te njihovih svojstava, interakcija, procesa koji obavljaju i međusobne povezanosti. Floridi navodi kako je ovo koncept koji rapidno evoluira. Upravo radi toga u informacijskom okolišu koji se sastoji od svih informacijskih entiteta dešava se re-inženjering koji ne utječe samo na tehničke aspekte sustava nego fundamentalno mijenja i intrinzičnu narav, odnosno ontologiju ili bit tog

[102] Isto, str. 14.
[103] O problematici napada 51 posto raspravit ću detaljnije u posebnoj cjelini rada.
[104] M. Peterson, *The Ethics of Technology*, str. 14.
[105] Luciano Floridi, »Ethics after the Information Revolution«, u: Luciano Floridi (ur.), *The Cambridge Handbook of Information and Computer Ethics*, Cambridge University Press, New York 2010., str. 6.

sustava. Jedan od najboljih primjera re-ontologizacije infosfere jest tranzicija s analognih na digitalnu vrstu podataka. Jedan od glavnih problema koje Floridi navodi jest i *ontologijska frikcija* (eng. *ontological friction*), pri čemu se u sustavu ne distribuiraju informacije. Rješenje vidi u tome da se čovječanstvo osvijesti da je upravo ono najodgovornije u dobu rapidnog porasta informacijsko-telekomunikacijske tehnologije te Floridi nudi prijedlog u vidu okolišne etike (eng. *e-nvironmental ethics*)[106] koja miri prirodu (grč. *physis*) i tehnologiju (grč. *techne*).[107] Taj je suživot nužan jer upravo infosfera predstavlja zajednički prostor koji se treba očuvati u korist svih ljudi.

Razrada teme dalje kreće prema članku Philipa Breyja koji se pita o vrijednostima (eng. *values*) u tehnologiji.[108] Taj nam je članak važan jer govori o vrijednostima koje sam detektirao u samoj srži *blockchain* tehnologije (eng. *integrity and trust*).

Brey govori o ugrađenim posljedicama (eng. *built-in-consequences*)[109] koje nisu apsolutne nego ovise o kontekstu uporabe određene tehnologije. Ugrađena vrijednost (eng. *embedded value*) specijalna je vrsta ugrađene posljedice.[110] Kada govori o vrijednostima, tehnološki entiteti mogu promicati ili štetiti realizaciji određenih vrijednosti. Kada se ovo djelovanje, bilo na štetu, bilo na korist, odvija sistematično u svim tehnološkim entitetima u nekom sustavu, onda govorimo o tendenciji da se promovira određena vrijednost te se takva tendencija (eng. *built in tendency*) naziva *ugrađena vrijednost*. Te i takve vrijednosti, budući da se nalaze u svim entitetima, potom oblikuju sustav jer se često fokusiraju na moralne norme. Norme su najčešće temeljene na vrijednostima, u njima imaju uporište i referentnu točku. Ako postoji promocija određenih ugrađenih vrijednosti u sustavu, onda možemo zaključiti da je to pravilo ugrađeno u sustav (eng. *embedded norms*).[111] Ugrađene vrijednosti

[106] »Pojam *ekopoiesis* odnosi se na moralno informiranu izgradnju okoliša na ekološki orijentiranoj perspektivi. Da bi se pomaknuli od individualnih vrijednosti do globalnih vrijednosti potreban je ekološki pristup koji prepoznaje odgovornosti subjekta prema okolišu (uključujući sadašnje i buduće stanovnike) kao prosvijetljenog nadzornika, a ne samo kao njegovog vrsnog korisnika i potrošača.« Vidi: isto, str. 17. Floridi u igri riječi kada razdvaja pojam okoliša (eng. *e-nvironment*), kod početnog slova »e« misli upravo na pojam *ekopoiesis*.
[107] Isto, str. 18–19.
[108] Philip Brey »Values in technology and disclosive computer ethics«, u: L. Floridi (ur.), *The Cambridge Handbook of Information and Computer Ethics*, str. 41.
[109] Isto, str. 45.
[110] Isto, str. 46.
[111] Isto, str. 47.

mogu biti intencionalne.[112] Ovo je posebno važno za decentralizirane sustave, a kod *blockchaina* možemo reći da definitivno postoji intencija kod ugrađenih vrijednosti integriteta i povjerenja koje imaju za namjeru postići sigurnost. Stoga možemo zaključiti da *blockchain* s tehničke strane fundamentalno želi promovirati korisne vrijednosti. Brey smatra da je zasluga otkrivajuće računalne etike upravo to da se moralne značajke mogu jasnije iskristalizirati na »površini« i postati transparentnije.[113] Nesumnjivo je njena uspješnost povećana u decentraliziranim mrežama ravnopravnih računala. Upravo je zasluga otkrivajuće računalne etike ta da je dizajniranje informacijskih sustava općenito, smatra Brey, postalo senzibilno i svjesnije vrijednosti koje se intencionalno nastoje ugraditi u sustav. Tako dolazimo i do pojma vrijednosno senzibilnog dizajna (eng. *value sensitive design*). Evo što o VSD-u kaže Brey:

»U etici (VSD) predstavlja zanimljiv pomak fokusa s čovjekovog djelovanja na tehnološke artefakte i sustave. U računalnoj znanosti (VSD) predstavlja zanimljiv pomak od utilitarnih i ekonomskih interesa na brigu za ljudske vrijednosti u dizajnu. Kao rezultat, (VSD) obećava bolju i potpuniju računalnu etiku kao i poboljšanu dizajnersku praksu u računalnoj znanosti i inženjerstvu što može rezultirati tehnologijom koja ide u korak s našim moralnim i javnim vrijednostima.«[114]

Ukratko, VSD je značajan jer doprinosi općem boljitku naših vrijednosti. Ukoliko se radi o boljitku vrijednosti, dakle propagiranju dobrih svojstava, utoliko možemo zaključiti da se radi o propagiranju *vrlina*.[115] Stoga bi za naše daljnje istraživanje bilo najprikladnije da se uputimo u smjeru etike vrlina. No prije toga, spomenut ćemo ukratko i konzekvencijalističku i deontološku etiku. To će zasigurno pridonijeti boljem razumijevanju zašto je za *blockchain* najbliža etika vrlina.

[112] Isto, str. 50.
[113] Isto, str. 53.
[114] Isto, str. 42.
[115] »Vrlina (grč. *ἀρετή*, lat. *virtus*): stečena i postojana karakterna osobina ili dispozicija koja predstavlja osnovu za vrjednovanje. Suprotnost joj je mana ili porok. Izraz vrlina može imati veoma široko značenje, koje ne upućuje samo na karakterne osobine ljudi, tj. na moralne vrline« Vidi: »Vrlina«, *Hrvatska enciklopedija*. Dostupno na http://www.enciklopedija.hr/Natuknica.aspx (pristupljeno 28. 8. 2018.). Usporedi: »Sokrat pokušava pokazati kako je pravednost zapravo temeljna vrijednost (*arete*) koja ne može u jednom času imati jedno obilježje, a u drugom biti suprotnost od toga, kao što primjerice netko ne može biti istodobno malen i velik, zdrav i bolestan, bogat i siromašan.« Vidi: Jure Zovko, »Uvod«, u: Platon, *Država*, preveo Martin Kuzmić, Naklada Jurčić, Zagreb 2004., str. 13.

Konzekvencijalistička etika i deontološka etika spadaju u normativnu etiku. Konzenkvencijalistička etika fokus stavlja na posljedice te je prema tome dobila i ime. Sažeto rečeno, radi se o tome da je moralno opravdano sve što maksimizira dobre posljedice.[116] Prema tome, u konzekvencijalističke etike ubrajao bi se i utilitarizam.[117] Utilitaristička etika, prema Grahamu, ima dva bitna aspekta: hedonistički (koji se tiče užitka i sreće) i konzekvencijalistički (koji se tiče posljedica djelovanja).[118] Hedonistički aspekt ću zanemariti i spomenuti da konzekvencijalistički aspekt u svoja dva važna momenta ubraja intenciju onog koji djeluje i lanac odgovornosti koje takvo djelovanje podrazumijeva. Posljedice su bitne s moralnog aspekta,[119] međutim, što je to »dobro« ipak ostaje nedorečeno. John Stuart Mill pokušao je dati odgovor na ovo pitanje kroz dokaz o principu utilitarnosti.[120] Kada razmotrim njegov dokaz i pokušam ga kontekstualno smjestiti u temu rada, dolazim do zaključka da se Millov zakon tiče onog što smo ovdje riješili s tehničkog aspekta. Naime, *blockchain* tehnika na temelju svojih dviju komponenata predstavlja korisnu podlogu mnogim projektima u aktualnim primjenama *blockchaina*. U tom slučaju, korisnost koju tehnologija ima s tehničke strane na temelju tehničko-izvedbenih rješenja je ekstenzija *blockchaina* koja prolazi iz srži u kojoj su upravo ugrađene vrijednosti integriteta i povjerenja. Mill se fokusira na korisnost:

»Valja istaknuti da odbacujem sve, što bi koristilo mojem razmatranju ako izvire iz ideje o apstraktnom pravu, koje je neovisno od korisnosti. Pozdravljam korisnost kao konačni priziv u svima etičkim pitanjima, ali to mora biti korisnost–u najvišem smislu, utemeljena na stalnim interesima čovjeka kao bića napretka.«[121]

---

[116] H. J. Gensler, *Ethics*, str. 110.
[117] »Utilitarizam smatra da se sve radnje moraju prosuđivati isključivo po posljedicama koje imaju za sreću (...).« Vidi: Gordon Graham, *Theories of Ethics*. *An Introduction to Moral Philosophy with a Selection of Classic Readings*, Routledge, New York 2010., str. 103.
[118] G. Graham, *Theories of Ethics*, str. 103.
[119] Isto, str. 109.
[120] »Utilitaristička doktrina nalaže da je sreća jedini krajnji poželjni cilj; sve druge stvari su poželjne samo kao sredstva do tog cilja. Što se treba tražiti od ove doktrine – koje bi uvjete doktrina trebala ispunjavati – da bi se moglo vjerovati u dobrotvornost koju obrazlaže? Jedini dokaz koji se može dati tome u prilog jest da je objekt vidljiv ako ga ljudi zapravo vide. Jedini dokaz da se zvuk može čuti jest da ga ljudi čuju; i tako redom i iz drugih izvora iskustva. U istoj maniri shvaćam jedinstveni dokaz, a taj je da je moguće bilo što učiniti poželjnim, ako ljudi to zapravo žele. Ako cilj koji ulititarizam zagovara na kraju ne bi bio uvažen teoretski i praktički kao takav, ne bi bilo moguće obrazložiti zašto je opća sreća poželjna, osim što svaka osoba, ukoliko vjeruje da je sreća dostižna, priželjkuje vlastitu sreću. Budući da je rečeno činjenica, imamo ne samo potreban dokaz u ovom slučaju nego i u svim drugim (slučajevima) u kojima je moguće tražiti potvrdu da je sreća dobra: da je osobna sreća dobra svakome ponaosob i da opća sreća znači dobro svim ljudima.« Vidi: John Stuart Mill, *Utilitarianism*, Oxford University Press, New York 1998., str. 88. Usporedi: G. Graham, *Theories of Ethics*, str. 114.
[121] Vidi: John Stuart Mill, »O slobodi«, u: John Stuart Mill, *Izabrani politički spisi*, preveo Adam Krlić, Informator, Fakultet političkih znanosti, Zagreb 1988., str. 119.

Stoga je ono najbliže našem interesu upravo proučavanje vrijednosti, odnosno vrlina kod ljudi. U *blockchain* su vrijednosti ugrađene (eng. *embedded values*) i istraživanje će se nastaviti u tom smjeru.

Prije nego u potpunosti prijeđem na etiku vrlina, spomenut ću još i deontološku etiku čiji je najznačajniji predstavnik Immanuel Kant. Za razliku od Milla, Kant će naložiti da radimo dobro jer nam je to dužnost.[122] Kod Kanta postoje kategorički imperativi koji konstruiraju pravila moralnog ponašanja.[123] Kanta bismo mogli sažeti njegovim vlastitim riječima na sljedeći način:

»Osnovni zakon čistog praktičkog uma: djeluj tako da maksima tvoje volje u svako doba ujedno može važiti kao princip općega zakonodavstva.«[124]

Kant također raspravlja o dobru[125] te o važnosti koje intencija[126] ima u postizanju dobra. Kant će smatrati da su moralne koncepcije *a priori*.[127] Za daljnji istraživački smjer smatram nužnim

---

[122] Immanuel Kant, *Kritika praktičkog uma*, preveo Viktor D. Sonnenfeld, Naprijed, Rijeka 1974., str. 123.
[123] Isto, str. 50.
[124] Isto, str. 64.
[125] »Ništa na ovom svijetu – doista, ništa ni van ovoga svijeta – ne može se zamisliti da bi se moglo nazvati dobrim bez ograničenja osim dobre volje. Inteligencija [eng. *intelligence*], dosjetljivost [eng. *wit*], rasuđivanje [eng. *judgement*] i drugi talenti uma, ma kako god se zvali, ili hrabrost, odlučnost i ustrajnost kao svojstva temperamenta, nesumnjivo su u mnogočemu dobri i poželjni. Međutim, mogu postati izuzetno loši i škodljivi ako volja, koja bi inače nalagala da se iskoriste darovi prirode, a oni se u svom posebnom ustroju nazivaju karakterom, nije dobra.« Vidi: Immanuel Kant, *Foundations of the metaphysics of morals*, preveo Lewis White Beck, Bobbs-Merrill Educational Publishing, Indianapolis 1959., str. 9. Usporedi: G. Graham, *Theories of Ethics*, str. 79.
[126] »Namjera i ishod se stoga trebaju najaviti s rezultatom, tako da se ne doima da je najvažnija uspješna radnja u konačnici.« Vidi: G. Graham, *Theories of Ethics*, str. 80. Usp.: »Svojstvo kauzaliteta po kojemu on može djelovati nezavisno od tuđih uzroka koji bi ga određivali, kao što je prirodna nužnost svojstvo kauzaliteta svih bezumnih bića da ih utjecaj tuđih uzroka određuje na djelovanje (…).« Vidi: I. Kant, *Kritika praktičkog uma*, str. 3.
[127] U ovom slučaju *a priori* ne znači vremensko, nego logičko – označava općost i nužnost valjanosti koje je neovisno o iskustvu. Kant nema namjeru postavljati nov princip moraliteta. Analizom moralne savjesti dolazi do pojma dobre volje. Ona je jedina na svijetu dobra po sebi te je dobra bez ograničenja. Ona u sebi nosi svoju svrhu, a to je ispunjenje dužnosti. Dužnost je nužnost djelovanja iz poštovanja prema zakonu (ne misli se na podložnost pozitivnim društvenim zakonima nego na poštovanje zakona u nama samima). Kod Kanta um (lat. *intellectus*) ne otkriva zakonitosti zbilje nego ih postavlja. Um je zakonodavac i on se prema zbilji odnosi neposredno djelatno i stvaralački. Da još spomenem i tu distinkciju, razum (lat. *ratio*) je sposobnost razboritog mišljenja. Zaključujemo da je um je aktivno oblikovna moć koja usmjeruje misaonu djelatnost. Imperativ je formula zapovijedi uma te imperativ može biti hipotetičan ili kategoričan. Hipotetičan je ako upućuje na neko djelovanje kao dobro. Kategoričan je ako upućuje na neko djelovanje kao po sebi dobro. Kategoričan imperativ glasio bi, kao što sam već i naznačio: radi prema onoj maksimi za koju ujedno možeš htjeti da postane općim zakonom. Svatko u sebi nosi načelo djelovanja, a sigurnost se temelji u savjesti. Drugim riječima, svatko zna što

uvesti jednu bitnu distinkciju koja će opravdati i olakšati shvaćanje odabira daljnjeg smjera istraživanja:

»Aristotel je bio zaokupljen karakterom subjekta koji djeluje, a ne karakterom samoga djelovanja i po tome se razlikovao od Kanta koji je smatrao da se dobro i zlo prije svega odnose na samu radnju, a tek naknadno možemo govoriti o dobrom čovjeku kao *djelatno-dobroj* osobi.«[128]

Čini mi se da se najprije valja osvrnuti na vrijednosti koje je potrebno prethodno posjedovati baš kao što smo to uočili s ugrađenim vrijednostima u tehnologiji. Iako Kant u Metafizici ćudoređa piše o moralnim koncepcijama, svoje istraživanje temelji na slobodi koja je uvjet volje iz koje se tek potom izvode dobre ili loše radnje po savjesti svakog pojedinca koji se ravna po maksimi zlatnog pravila.[129] *Želim* je nadvladano onime što se *mora* učiniti i kod Kanta primat preuzima kategorički imperativ.[130] Odlučio sam krenuti u smjeru etike vrlina jer se fokus istraživanja stavlja upravo na vrijednosti. Detektirane ugrađene vrijednosti u *blockchain* su paradigmatski najsličnije i iz tog razloga krećem dalje u smjeru istraživanja vrijednosti, prije svega vrlina.

Blockchain tehnologija nastoji postići integritet i povjerenje u sustavu s tehničkog aspekta usađenim vrijednostima u sustav. Da bi se te vrijednosti ugradile s ne-tehničkog aspekta, izuzetno je bitno pokrenuti raspravu o vrijednostima, napose vrlinama i objasniti zašto one mogu pozitivno utjecati na sustav.

3.3. Utvrđivanje etičkih temelja *blockchain* tehnologije

je dobro i zlo. Ako se čini zlo volja je u proturječju jer sebi dopušta grijeh, a od drugih zahtijeva poštivanje općeg dobra. Pojam dobra i zla za Kanta ne mora se odrediti prije moralnog zakona (koji radi po dužnosti) nego samo poslije njega i pomoću njega. Maksima djelovanja je ispred teorijske spoznaje dobra i zla. Usp.: I. Kant, *Kritika praktičkog uma*, str. 49–75.

[128] Barbara Horvat, *Kantova metafizika ćudoređa* (diplomski rad), Filozofski fakultet Osijek, Odsjek za filozofiju, Osijek 2017.

[129] »Osim toga, moralni je zakon, takoreći, dan kao fakat čistoga uma, kojega smo *a priori* svjesni i koji je apodiktički izvjestan, pretpostavivši da se u iskustvu i ne bi mogao pronaći primjer, gdje je on točno izvršen« Vidi: I. Kant, *Kritika praktičkog uma*, str. 83

[130] Vidi: isto, str. 50.

U ne-tehničkoj domeni, vrlina se može okarakterizirati kao dobra navika[131] ili izvrsno svojstvo karaktera.[132] Iz općih izvora o etici vrlina možemo saznati da je ta disciplina uvijek naglašavala važnost edukacije o moralu (počevši s Platonovom *Politeiom* i Aristotelovom *Nikomahovom etikom*) i to ne kao primjenu određenih pravila, nego treniranje našeg karaktera.[133] Također, navodi se u općim izvorima da, iako su istraživanja u sklopu etike vrline mnogo uznapredovala u posljednjih 35 godina, ona i dalje nije toliko aktualna, pogotovo u polju primijenjene etike.[134] Međutim, ono što etiku vrlina razdvaja od konzenkvencijalizma i deontološke etike jest to da ona upravo vrline kao osobnosti karaktera stavlja u fokus svojih istraživanja. Naravno, treba imati na umu da je granica koju smo povukli između vrlina, posljedica i pravila umjetna i svaki od etičkih teorija ima mjesta i za vrline i za konzenkvencijalizam i za principe iz kojih kreće naše moralno djelovanje.

Unatoč dobi njihovih istraživanja, Platon i Aristotel posebno su značajni za etiku vrlina i *blockchain* fenomen. Platon u *Politei* spominje da državu sretnom mogu učiniti samo filozofi-vladari.[135] Svi u državi su sretni kada raspodijelimo radne uloge te Platon drži da postoje tri staleža u državi: proizvođači (radnici); čuvari (vojnici) te vladari (koji su ujedno i filozofi).[136] Dakle, raspodjeljivanjem radnih uloga u državi postiže se pravednost. Platon drži da duša ima razumski, voljni i požudni dio.[137] Postići sklad među trima dijelovima duše također znači pravednost, ali u ovom slučaju pravednost pojedinca. Pravednost pojedinca se ne razlikuje od pravednosti države jer postoji zajednička ideja savršene pravednosti.[138] Ono što je bitno za napomenuti jest da Platon smatra da svu pažnju u državi valja usmjeriti na odgoj i obrazovanje.[139] Platon će ustanoviti da nitko nije zao svojom voljom, nego ga takvim čini, između ostalog, nestručni odgoj.[140] U njegovoj filozofiji najviša ideja je ideja Dobra i sve teži prema njoj.[141] Iz ideja je izveden materijalan svijet te ideje predstavljaju pravu realnost i objektivnost. Iako je svijet ideja za čovjeka transcendentan, to ne znači da on ne treba ustrajati

[131] H. J. Gensler, *Ethics*, str. 139.
[132] Rosalind Hursthouse, Glen Pettigrove, »Virtue Ethics«, *The Stanford Encyclopedia of Philosophy*, 2016. Dostupno na: https://plato.stanford.edu/archives/win2016/entries/ethics-virtue/ (pristupljeno 25. 8. 2018.).
[133] Platon, *Država*, 403d–403e.
[134] R. Hursthouse, G. Pettigrove, »Virtue Ethics«.
[135] Platon, *Država*, 485.
[136] Isto, 441.
[137] Isto, 439e–442c.
[138] Isto, 441c–d.
[139] Isto, 416b–d.
[140] Isto, 419–421c.
[141] Isto, 608e–609b.

u svojoj spoznaji.[142] Ovo nam je također važan moment. Ako bismo Platonov nauk izvadili iz konteksta i pokušali ga primijeniti na ne-tehnički aspekt *blockchain* tehnologije, tada bi valjalo izdvojiti obraćanje velike pažnje na filozofiju odgoja te ustrajnost u želji da budemo boljim čovjekom. Na taj način može se konstruirati sustav koji je povoljan za sve.

Aristotel je uvelike proširio i razradio Platonov nauk. Aristotel smatra da je čovjek dobar kada postupa u maniri obzirnosti, a takvo postupanje podrazumijeva ispravan razum.[143] Ispravan razum djeluje onda kad su naši postupci lijepi, a da bi bili lijepi potrebno je da se držimo tzv. zlatne sredine između onog što je previše i premalo (primjerice, hrabrost je po Aristotelu sredina između plašljivosti i potpune smjelosti).[144] Vrlina se posljedično nalazi upravo u toj zlatnoj sredini. Prema Aristotelu, ako djelujemo po vrlini, postići ćemo blaženstvo (grč. *eudaimonia*).[145] Vrlina je način ponašanja kojim čovjek djeluje dobro, ali i posljedično postaje dobar. Svaki bi čovjek trebao iznalaziti sredinu u odnosu na sebe te ono što predstavlja razumnu sredinu za jednog ne mora vrijediti i za nekog drugog čovjeka.[146] Međutim, ističe Aristotel, ono što pojedinac u određenom trenutku smatra da je za njega dobro može se razlikovati od onoga što je istinski dobro.[147] Postizanje istinskog dobra trebao bi nam biti krajnji cilj, a njegovim ostvarivanjem čovjek postaje krjepostan. Iz tog razloga, budući da je taj put težak, Aristotel je kao bitnu osobinu moralnog čovjeka istaknuo posjedovanje praktične mudrosti kao i sposobnost prosuđivanja.[148] Valja istaknuti kako je vrline Aristotel podijelio na vrline volje i intelektualne vrline.[149] Dok se vrline volje tiču osjećaja, namjere i djelovanja, dijanoetičke se tiču nalaženja istine, odnosno čiste spoznaje.

Za razliku od Kanta,[150] Aristotel nam ne nudi pravila koja trebamo slijediti. Radi se o odgovornosti za djelovanje po vlastitoj prosudbi, a čovjek ima moć da sebe izgrađuje i teži

[142] Isto, 621c–d.
[143] Aristotel, *Nikomahova etika*, preveo Tomislav Ladan, Sveučilišna naklada Liber, Zagreb 1982., 1095b 5–13.
[144] Isto, 1104a 11–26.
[145] Isto, 1098b 19–22.
[146] Isto, 1095a 20–30.
[147] Isto, 1094b 13–27.
[148] Isto, 1179a 22–32.
[149] Isto, 1103a 13–25.
[150] Vidi: »Treće što nalazi u sebi je talent koji bi uz prosvijećenost mogao učiniti čovjeka korisnim u mnogočemu. No, on se nalazi u ugodnim okolnostima i preferira uživati, a ne podnositi veliku bol i nastojati poboljšati vlastite prirodne sposobnosti. Međutim, pita se je li njegova maksima o zanemarivanju njegovih prirodnih darova, osim što povlađuje njegovim sklonostima, suglasna s onim što se zove dužnost. Tada uočava da bi prirodni sustav zaista mogao koegzistirati s takvim univerzalnim zakonom iako ljudi (poput otočana južnih

blaženstvu, to jest, čovjeku je na njemu samome da prosuđuje što je za njega dobro u određenom trenutku, a da pri tome nastoji da njegova pojedinačna dobra budu u skladu s istinskim dobrom. Za takvo, razborito djelovanje čovjek nepobitno mora posjedovati znanje i iskustvo.[151] Upravo nam Aristotel daje smjernicu u kojoj bismo mogli ići kada govorimo o našoj temi. Naime, ulaganje u vlastito znanje i stjecanje iskustva pospješit će donošenje razboritih odluka koje će djelovati krjeposno ne samo za nas nego i za ljude oko nas. Aristotel je kritizirao Platonov nauk o idejama koji svijet ideja razdvaja od materijalnog, osjetilnog svijeta. Aristotel smatra da je slabost u tome što Platon stavlja suštinu u ideje a onda ih smješta u transcendentnost. Suština, naime, ne može egzistirati odvojeno od onoga čega je suština, držat će Aristotel.[152] Unatoč spomenutim razlikama, uvidjeli smo evidentne momente korensponendencije Platonova i Aristotelova nauka s tehnologijom *blockchaina*. *Blockchain* će se s tehničkog aspekta pobrinuti za sigurnost u sustavu, no ostaje naizgled mali manevarski prostor koji itekako otvara velike mogućnosti čovjeku – kako će se ova tehnologija koristiti i hoće li to biti na dobrobit svih ili samo nekih te kako uskladiti tehniku i ljude s vrlinom?

U *blockchain* tehnologiji nikad nisu *physis* i *techne* bili bliži. Nikad nije tehnička i netehnička strana tehnologije bila toliko povezana.[153] Ako, s jedne strane, imamo vrijednosti povjerenja i integriteta koja na temelju inovativne tehnologije žele postići sigurnost, analogno, na drugoj strani, trebamo tražiti vrijednosti koje bi pojedinac trebao imati da te vrijednosti upotpuni, ali i odvede korak dalje. A za to nam treba čovjek koji ima vrline. Štoviše, treba nam više ljudi koji imaju vrline. A da bi do njih došli neprekidno treba raditi na sebi, ulagati u svoje znanje i iskustvo. Samo podizanjem i normiranjem sustava vrijednosti *blockchain* može zaživjeti onako kako bi i trebalo – na korist svih ljudi cijelog svijeta. Pa premda bi kritičari

---

mora) mogu dopustiti da se njihovi talenti odmaraju i odluče posvetiti svoj život samo besposlenosti, zabavi i prokreaciji – jednom riječju, užitku; ali on ne može vjerojatno htjeti da to bude univerzalni zakon prirode ili da se prirodnim instinktom ugradi u nas kao takav. Kao racionalno biće, čovjek nužno želi da se njegove sposobnosti razviju, budući da mu služe i daju mu se za sve moguće svrhe.« Vidi: Immanuel Kant, »Transition from popular moral philosophy«, para. 46, u: *Fundamental Principles of the Metaphysic of Morals*, preveo Thomas Kingsmill Abbott, Project Gutenberg, 2004. [Microsoft Edge, .epub format] Kant u Metafizici ćudoređa rigorozno razrađuje pravila za dužnosti po kojima se ispunjavaju maksime koje se potom mogu poopćiti. Naveo sam u citatu treću od pobrojane četiri koje se javljaju u knjizi.

[151] Aristotel, *Nikomahova etika*, 1142a 5–30.

[152] Aristotel, *Metafizika*, preveo Tomislav Ladan, Globus, Sveučilišna naklada Liber, Zagreb 1988., 1077 b 26.

[153] »Tako, dakle, što smo najmanje predmnijevali, ono bitstveno tehnike krije u sebi mogući rast onoga spasonosnoga. Zato je osobito važno da taj rast promislimo i misleći ga čuvamo. Kako je to moguće? Prije svega tako da u tehnici uočimo ono bitstveno, umjesto da samo piljimo u ono tehničko. Dokle god tehniku predstavljamo kao instrument, držimo se volje da njome zagospodarimo. A tako promašujemo bit tehnike.« Vidi: Martin Heidegger, »Pitanje o tehnici«, str. 244.

rekli da to nije moguće, možemo ih uputiti na platonistički pristup idejama – konstantno pospješivati našu spoznaju i vraćati se u spilju[154] i prosvjećivati ljude. Samo na taj način će uistinu zaživjeti i edukacija mlađih naraštaja, normiranjem i nagrađivanjem pozitivnog sustava vrijednosti. I dalje vrijedi (grč.) *gnothi seauton*[155] jer samo preko toga možemo istinski omogućiti *blockchain* tehnologiji da očuva svoj integritet i postigne konzistenciju tijekom vremena.

[154] Platon, *Država*, 514–517.
[155] U prijevodu: spoznaj sama sebe; moguće natpis na ulazu u Apolonov hram u Delfima.

4. Određenje moralnih izazova *blockchain* tehnologije

4.1. Pozitivna primjena *blockchain* tehnologije

Navest ćemo nekoliko pozitivnih primjera uporabe *blockchain* tehnologije te nekoliko mogućnosti gdje bi se ta tehnologija mogla u budućnosti upotrebljavati.[156]

Već sam spominjao *kriptovalute* – imaju potencijal upravljati vlasništvom i kreiraju inovativan model plaćanja koji može biti neovisan o centralnim entitetima, poput banaka ili Vlada. Mikroplaćanja su još jedan način uporabe *blockchaina*. Radi se o naplaćivanju izuzetno malih suma novaca koje je neisplativo potraživati i plaćati sadašnjim putem preko banaka kao posredničkih institucija. Tehnologija bi se mogla koristiti i kao svojevrsno sigurno skladište identiteta fizičkih osoba koje funkcionira na principu kriptografije. Sve osobne dokumente mogli bismo pohraniti u *blockchain* te bi nestala potreba za izdavanjem dokumenata u fizičkom obliku (primjerice osobna iskaznica, vozačka dozvola, zdravstvena iskaznica itd.). Osim toga, pohranjivati bi se mogli razni dokumenti, pravni spisi, ugovori koji bi se prethodno digitalizirali itd. Još jedna zanimljiva mogućnost javlja se i kod oporezivanja. Izračunavanje i prikupljanje popisa moglo bi se odvijati kroz popis vlasnika u *blockchain* sustavu, čime bi se moglo eliminirati duplo oporezivanje (po uzoru na eng. *double spending*) ili izbjegavanje plaćanja poreza:

»*Blockchain* sam po sebi predstavlja trajni i nepromjenjivi zapis svake transakcije. Postavljanje sveukupnog novčanog kapitala neke države [eng. *country's money supply*] na *blockchain* kojeg kontrolira središnja banka bio bi potpuno transformirajuć jer bi postojao stalni zapis o svakoj financijskoj transakciji koja postoji na nekoj razini unutar blockchaina, čak i ako ti podaci nisu vidljivi javnosti. Blockchain tehnologija i digitalne valute smanjile bi

[156] Usporedi: R. Jesse McWaters, »The future of financial services: How disruptive innovations are reshaping the way financial services are structured, provisioned and consumed; an Industry Project of the Financial Services Community«, *World Economic Forum* 2015. Dostupno na: http://www3.weforum.org/docs/WEF_The_future__of_financial_services.pdf (pristupljeno 23. 8. 2018.).

rizik i prijevare te pružile ultimativnu kontrolu u izvršavanju monetarne politike i oporezivanja.«[157]

Glasovanje bi se također moglo provoditi putem *blockchain* tehnologije. Od stvaranja glasačkih listića do njihove distribucije po cijelom sustavu te prikupljanja glasova. *Blockchain* može poslužiti kao pozadinska tehnologija za provođenje tog procesa kao što služi kao pozadinska tehnologija u mnogim projektima digitalnog novca. Uostalom, takvi projekti već su pokrenuti.[158] Tapscotti smatraju da će se premještanjem paradigme glasovanja na *blockchain* osigurati pošteno, sigurno i lagodno glasovanje[159] te neizravno i dotaknuti problem pasivnog građanstva. Tapscotti također smatraju da mogućnosti koje *blockchain* u tome segmentu ne staju samo na glasovanju:

»Svatko ima pravo sudjelovati u Vladi, izravno ili glasovanjem. Tko bude izabran, mora obavljati poslove transparentno kao jedan među jednakima. S internetom, građani su preuzeli veću odgovornost za svoje zajednice, naučili i utjecali na izabrane dužnosnike i obrnuto. Uz *blockchain*, građani mogu ići korak dalje: oni se mogu zalagati za arhiviranje svih akcija Vlade u javnoj knjizi salda. Pritom se ne misli samo na provjeravanje potencijalnih kandidata za javne pozicije, već i na postizanje konsenzusa među širokim masama za, primjerice, provođenje pozadinskih provjera potencijalnih vlasnika oružja (među potencijalnim kandidatima za javne pozicije).«[160]

Zvuči li ovo kao scenarij u koji je teško povjerovati valja upozoriti da Estonija i Ukrajina već imaju pokrenute projekte u javnom sektoru koji su bazirani na *blockchain* tehnologiji.[161]

Nadalje, reputacija je jako važna u poslovnom svijetu,[162] a *blockchain* tehnologija uvelike može na to utjecati. Primjerice, kao svojevrsna pomoćna tehnologija može se koristiti

[157] T. Laurence, *Blockchain for Dummies*, str. 132.
[158] Vidi: M. Swan, *Blockchain*, str. 49.
[159] A. Tapscott, D. Tapscott, »The second era of democracy«, para. 1, u: *Blockchain Revolution*. [Microsoft Edge, .epub format]
[160] A. Tapscott, D. Tapscott, »Something is rotten in the state«, para. 12, u: *Blockchain Revolution*. [Microsoft Edge, .epub format]
[161] W. Mougayar, V. Buterin, »Governments and Governance«, para. 4–5, u: *The Business Blockchain*. [Microsoft Edge, .epub format]

kod *pametnih ugovora* pomoću kojih se može vidjeti koliko se puta neka fizička ili pravna osoba nije držala svoje strane ugovora, što bi se u konačnici moglo riješiti povratom novca za oštećenu stranu.[163] Ovo je jedan od primjera zašto *blockchain* tehnologija dobro funkcionira zahvaljujući njenoj transparentnosti.[164] Također, Drescher izlaže svoje mišljenje da će *blockchain* tehnologija sasvim sigurno omogućiti više ljudi na svijetu da participiraju na globalnom tržištu, bilo kupnjom, bilo prodajom.[165]

4.2. Tehnička i ne-tehnička ograničenja *blockchain* tehnologije[166]

4.2.1. Tehnička ograničenja *blockchain* tehnologije

Jared Norton navodi da *blockchain* tehnologija, iako inovativna, i dalje je probabilistička tehnologija. Drugim riječima, može služiti odlično u svrhu sigurnosti i pohrane podataka, ali pojedincu ne može ponuditi odgovore na pitanja poput: »Trebam li izbaciti podstanare ako ne plaćaju račune šest mjeseci zaredom?«. Zaključuje da se na tu tehnologiju ne možemo osloniti u potpunosti.[167] U *blockchain* sustavu, ukoliko se nalazi u pozadini *kriptovaluta*, utoliko se podrazumijeva postojanje javne knjige salda. Sve su transakcije javne i svima dsotupne. Uz to, znamo da se stalno mogu priključivati novi čvorovi u sustav. Na taj način *blockchain* tehnologija nastoji postići transparentnost. Međutim, iako transparentna, u tome slučaju prigovor može ići u smjeru da nema dovoljno privatnosti. Štoviše, to je konstitutivni element ove tehnologije – točka napetosti se nalazi između transparentnosti i privatnosti. Postavlja se pitanje kako *blockchain* tehnologija može biti dostupna svima, a da sačuva privatnost pojedinca?

Sljedeći prigovor može biti iz sigurnosnog aspekta. Naime, jedina stvar koja povezuje stvarnog vlasnika s njegovim vlasništvom u *blockchainu* jest privatni ključ. Privatni ključ je apsolutna nužnost utoliko ukoliko se želi pristupiti svojem vlasništvu, ali i transferirati podatke nekome drugome u sustavu. Ukoliko se on izgubi, bilo slučajno, bilo nekom

[162] J. Norton, *Blockchain*, str 16.
[163] Isto, str. 16.
[164] »Dakle, ako je nužan pouzdan i transparentan način vođenja evidencije, *blockchain* se može koristiti kao baza za izradu aplikacije upravo za navedenu svrhu.« Vidi: isto, str. 17.
[165] Isto, str. 27.
[166] D. Drescher, *Blockchain Basics*, str. 205.
[167] J. Norton, *Blockchain*, str. 22.

nesretnom okolnošću, utoliko stvarni vlasnik ne može više doći do svojeg vlasništva. Ne postoji ni jedan drugi način da se vlasnik u tom slučaju domogne onoga što mu pripada. Zatim, da biste priključili čvor ili nekoliko njih u decentralizirani sustav s bazom *blockchain* tehnologije, potrebno je uložiti financijska sredstva u nabavu računalnih dijelova. Računala troše mnogo računalne energije za rješavanje *hash* slagalica te to u konačnici zahtijeva znatan utrošak električne energije. To znači da je potrebno uložiti financijska sredstva da bi se decentralizirani *blockchain* sustav uopće pokrenuo. To nas dovodi do sljedećeg problema – ako su troškovi veliki onda to znači da ne može svatko uložiti u taj proces. Otpočetka se onemogućavaju ljudi bez početnog kapitala da uđu u tržišnu utakmicu i budu sudionici *blockchaina* (u smislu individualnog čvora u sustavu). Tada se pojavljuje scenarij u kojem jedan čovjek, ili mala grupa ljudi u dogovoru kontroliraju većinu čvorova u mreži. Stvara se prikriveni centralni entitet za kojeg ostali čvorovi u mreži ne znaju. Pretpostavka u *blockchainu* jest da su čvorovi poštenih namjera ili da će to barem postati. Jedan od načina kako se oduprijeti napadu interesne skupine ili pojedinca je rast same tehnologije do točke gdje će taj napad biti gotovo nemoguće izvesti.[168] Međutim, do napada neće ni doći ako će u društvu prevladavati razboriti ljudi. Razboritost je etički spoznajni organ, moć promišljanja stvari koje su probitačne za dobar život, činidbena sposobnost prema razumu u pogledu dobrih i loših stvari, ona je zapravo sama »dobra činidba« (grč. *εὐπραξία*).[169] Vrlina razboritosti, ali i sve druge vrline, ne predstavljaju samo neke antičke zapise koji su predmet suhoparnog studiranja. Dapače, do njih dolazimo, u ovom slučaju, zaobilaznim putem, preko tehnike. Tehnika (kao nadređeni pojam tehnologijama), prema Heideggeru, upućuje nas na samu sebe:

»Tako, dakle, što smo najmanje predmnijevali, ono bivstveno tehnike krije u sebi mogući rast onoga spasonosnoga.«[170]

Heidegger svoju misao razvija pišući da se iz tehnike uz ono spasonosno neminovno pojavljuje i ono opasno.[171] No to ne predstavlja znak za uzbunu i zaustavljanje. On će napomenuti da »što se više bližimo opasnosti, to jasnije počinjemo osvjetljavati put u ono

[168] Misli se na konzistentnost koja u *blockchainu* jača tijekom vremena (eng. *eventual consistency*).
[169] Aristotel, *Nikomahova etika*, 1140 b 6.
[170] M. Heidegger, »Pitanje o tehnici«, str. 244.
[171] Isto, str. 246.

spasonosno, to više postajemo onima koji pitaju«[172] jer, po njemu »pitanje o tehnici je pitanje o konstelaciji u kojoj se stječe otkrivanje i skrivanje, u kojoj se stječe ono bitstveno istine«.[173] Deduciranjem ćemo zaključiti: ako se složimo s Heideggerom, onda to vrijedi za svaku tehnologiju, pa tako i za *blockchain* tehnologiju. Budući da Heidegger istovremeno upozorava i potiče na uporabu tehnike, smatram da je prijedlog ovog rada, u kojem smo detektirali etike vrlina kao najpodesnije za raspravu o *blockchainu*, još više dobio na snazi. Vrijednosti koje se nalaze inkorporirane u *blockchain* moći će sjati u punom svjetlu, kao vrline, ako i ljudi koji tehnologijom upravljaju budu radili po vrlini:

»Naime, ona zaključivanja koja se tiču činidbe posjeduju počelo, kao *budući je svrha ono najbolje, takvo i takvo,* pa kakvo god bilo (i neka radi dokaza bude bilo što), a takvo što niej bjelodano osim onomu tko je dobar; jer nevaljalost izopačuje i obmanjuje što se tiče činidbenih počela. Tako te je jasno kako je nemoguće biti razborit ako čovjek nije dobar.«[174]

Još jedan prigovor koji se tiče tehničkog aspekta *blockchain* tehnologije nemogućnost je nadogradnje postojeće tehnologije (prvenstveno se misli na komponentu kriptografije) ili izmjene, odnosno zamjene tehničkih komponenti.[175] To bi značilo da tehnologije koje čine osnov *blockchaina* moraju trajati koliko i on sam, a taj vijek se ne može egzaktno predvidjeti – može trajati stoljećima. Naime, teško je raditi preinake ili popravljati greške u sustavu *blockchain* tehnologije, a ta karakteristika čini ovu tehnologiju izuzetno nefleksibilnom.[176]

4.2.2. Ne-tehnička[177] ograničenja *blockchain* tehnologije

Kod ne-tehničkih ograničenja izdvojit ćemo dva aspekta: legalna ograničenja te ograničenja u uporabi. Vidjeli smo da *blockchain* tehnologija zadire i u koncept vlasništva. Jedna od njenih prvih, nužnih i najzanimljivijih primjena je u području *kriptovaluta*. Zakoni

[172] Isto, str. 247.
[173] Isto, str. 245.
[174] Aristotel, *Nikomahova etika*, 1144a 31–36.
[175] *Hash* vrijednosti i kriptografija prihvaćaju se kao dvije komponente koje se ne mogu konceptualno mijenjati.
[176] »Postoji i problem za developere u sustavu blockchaina zbog načela nepromjenjivosti jer je teško popraviti greške ili napraviti prilagodbe u protokol blockchaina. Radi tog ali i drugih razloga blockchain je manje fleksibilan u poredbi s drugim tehnologijama.« Vidi: D. Drescher, *Blockchain Basics*, str. 208.
[177] »Ne-tehničkim ograničenjima *blockchaina* mogu se smatrati društveni, ekonomski, pravni i psihološki vidovi prilagodbe novoj tehnologiji.« Vidi: Isto, str. 209.

pojedinih država još se nisu u potpunosti prilagodili na ovo novo i brzorastuće tržište.[178] Da bi tehnologija mogla napredovati i dalje, zakonodavstvo i upravno-pravno uređenje država, ukoliko žele iskoristiti beneficije koje se ovom tehnologijom nude, utoliko će definitivno morati razmišljati o uvođenju određenog zakonskog okvira koji bi definirao upravljanje vlasništvom ne samo u domeni *kriptovaluta* nego moguće i *blockchain* tehnologije u cjelini.[179] Ako i razriješimo do neke mjere konfuziju koja se stvara nepostojanjem zakonskog okvira, svejedno ostaje bojazan, ili bolje reći rizik, hoće li ova tehnologija zaživjeti. Ako ljudi neće pokazati interes za ovu tehnologiju, onda je ni neće biti. Ukoliko neće postojati čvorova koji rješavanjem teških matematičkih zadataka stvaraju nove blokove, utoliko je svaki daljnji napor bezuspješan.

Ako to želimo nadići onda je potrebno ljudima pružiti informacije, omogućiti educiranje i shvaćanje potencijala ove tehnologije, uz rizike koje nam također donosi. No s pravom se može postaviti pitanje – zašto bi uopće trebali to nadići? Zasad ne mogu tvrditi da je *blockchain* »moralniji« od neke druge tehnologije. No mogu tvrditi da se unutar *blockchaina* u velikoj bliskosti inkorporiraju *physis* i *techne* te se veliki značaj pridaje ostvarenju vrijednosti integriteta i povjerenja u takvom sustavu. Te vrijednosti nisu puki nusprodukti *blockchaina*, oni predstavljaju njegovu idejnu srž. Osim toga, što se tiče tehničkih rješenja za postizanje sigurnosti, *blockchain* nudi učinkovita rješenja na temelju svojih dvaju komponenti. Prethodno sam spomenuo da ga upravo zbog toga nalazimo u aktualnoj primjeni ne samo kod *kriptovaluta* nego i u tvrtkama koje svoje poslovanje baziraju na *blockchainu*. Ova tehnologija je idejno, teoretski, odlično zamišljena. Ipak, to ne daje nikakvu garanciju da će ona postati apsolutno najbolja tehnologija, bilo po pitanju promoviranja vrijednosti na kojima se temelji, bilo s tehničko–izvedbene strane. Priznajem, postoje dvije strane narativa, ali bez obzira na rizike, bez obzira na prikrivene opasnosti, ponovno ću se pozvati na Heideggera:

> »Ali gdje postoji opasnost, raste također ono spasonosno.«[180]

[178] Usporedi: Luka Lujić, *Pravno uređenje kriptovaluta* (diplomski rad), Pravni fakultet u Zagrebu, Katedra za pravnu informatiku, Zagreb 2017.

[179] »Namjesto toga da inzistiramo da je svrha *blockchaina* održavanje integriteta otvorenih i potpunih decentraliziranih sustava mreža ravnopravnih računala, mogli bismo tvrditi da je njegova svrha postizanje i održavanje integriteta decentraliziranih sustava općenito.« Vidi: D. Drescher, *Blockchain Basics*, str. 219.

[180] M. Heidegger, »Pitanje o tehnici«, str. 240.

Tako će svaki poduzetnik sam za sebe odlučiti isplati li mu se poslovanje prebacivati na *blockchain*. Političari će odlučiti je li na dobrobit njihove države da djelovanje javne uprave i cjelokupan demokratski proces presele na *blockchain* (primjerice, Estonija je zdravstvo prebacila na *blockchain*).[181] Ako je suditi po tome da se paradigma povjerenja seli na digitalnu podlogu te da će na toj podlozi značajnu ulogu poprimiti upravo vrijednost povjerenja,[182] onda se *blockchain* pojavljuje kao savršeni kandidat za ostvarenje takvih nauma.

4.3. Koruptivni elementi *blockchain* tehnologije

S tehničkog se aspekta *blockchain* tehnologija doima gotovo savršenom. Istaknuli smo da je jedan od ciljeva *blockchain* tehnologije da kreira i zadrži integritet i povjerenje u decentraliziranom sistemu mreže ravnopravnih računala koji je sastavljen od nepoznatog broja čvorova i u koje se ne možemo pouzdati i znati jesu li povjerljivi (eng. *reliability and trustworthiness*). Opisivanjem tehničkog aspekta *blockchain* tehnologije ne nazire se manevarski prostor za nepošteno djelovanje. Naime, opisali smo kako asimetrična kriptografija štiti vlasništvo i podatke u sustavu i čini nemogućim korištenje lažnog identiteta. Istražujući *blockchain* algoritam prikazao sam kako je prihvaćanje nevaljanih transakcijskih blokova nemoguće jer prolaze verifikaciju u cijelom sustavu. Iz istog razloga,[183] ne može se ni zamisliti slučaj u kojem određeni čvor namjerno zadržava informacije samo za sebe i ne želi ih proslijediti. Dizajniranjem komunikacije među čvorovima na principu glasina (eng. *gossip*) dokida se mogućnost namjernog neprosljeđivanja informacija. Bez obzira preopteretimo li namjerno određeni čvor kako bi on prestao raditi i natjecati se u sustavu, decentralizirani sistem nastavlja daljnji rad. Kvar jednog čvora ne utječe na decentralizirani sistem radi njegove arhitekture. Iako se s tehničke strane čini odličnim, ne smijemo zaboraviti da *blockchain* u velikoj bliskosti komponira ne-tehnički i tehnički aspekt. Najveća ranjivost

[181] Vidi: Ian Allison, »Guartime Secures over a Million Estonian Healthcare Records on the Blockchain«, *IB Times* (4. 3. 2016.). Dostupno na: http://www.ibtimes.co.uk/guardtime-secures-over-million-estonian-healthcare-records-blockchain-1547367 (pristupljeno 13. 9. 2018.).
[182] Richie Etwaru, »TEDx Talks: Blockchain Massively Simplified«, *YouTube* (15. 5. 2017.). Dostupno na: https://www.youtube.com/watch?v=k53LUZxUF50&t=51s (pristupljeno 13. 9. 2018.).
[183] Misli se na koncept *blockchain* algoritma koji je opisan u prethodnom poglavlju.

nalazi se u intenciji ljudi – u koju svrhu će se upotrebljavati. Intencija[184] je najbitnija značajka, a kod tog pojma, skrenut ću pozornost na Aristotela[185] i kontekst u kojem on upotrebljava taj pojam:

»Ondje pak gdje nema nikakva sporazumka o usluzi, oni koji daju poradi samih prijatelja ti su–kako je rečeno–besprijekorni (jer takvo je prijateljstvo utemeljeno na kreposti) i uzvraćaj valja učiniti prema intenciji (jer on je značajka i prijatelja i kreposti).«[186]

Aristotel će naglasiti da u prijateljstvima koja su utemeljena na krjeposti ne postoji mjesta tužbama:

»U prijateljstvima utemeljenim na krjeposti nema tužbi; tu je mjerilo sama intencija davatelja; jer u intenciji je poglavita značajka i krjeposti i samog značaja.«[187]

Budući da se u prethodna dva citata javio i pojam *prijateljstva*, spomenut ću što Aristotel govori i o prijateljstvu:

»Jer prijateljstvo je nekakva vrlina ili sadržava vrlinu, a uz to je najnužnije za život. Naime, nitko ne bi izabrao živjeti bez prijatelja, pa čak kad bi imao i sva ostala dobra.«[188]

Svaki prigovor koji će reći da u decentraliziranim mrežama ravnopravnih računala ne trebamo biti prijatelji i da pojam *prijateljstvo* nema smisla jer ne poznamo ostale korisnike u sustavu treba imati na umu da grč. Φιλια, osim što znači *prijateljstvo,* može značiti i ljubav, naklonost, a najčešće znači bilo koje ljubazno čuvstvo između ljudi, od prijateljske ljubavi do poslovne naklonosti. Narativ se ponovno pomaknuo u smjeru etike vrlina te rasprava u toj

[184] Grč. προαίρσις znači *izbor*, ali i *nakana, namisao, namjera* (lat. *intentio*); preveo sam ga za potrebe ovog rada – *intencija*.
[185] »Volja nije dobra po onome što postiže ili izvršava, ne po svojoj sposobnosti za postignuće bilo kakvog postavljenog cilja, nego samo po htijenju, tj. po sebi (...) .« Vidi: Immanuel Kant, *Osnivanje metafizike ćudoređa*, preveo Viktor D. Sonnenfeld, Feniks, Zagreb 2003., str. 14.; usporedi: » Dobra volja je sposobnost da se bira samo ono što um nezavisno od nagnuća spoznaje kao praktički nužno, tj. kao dobro.« Vidi: isto, str. 38. Kant smatra da moralni zakon neposredno određuje volju, a ako činimo dobro, tada su volja i namjera uvijek dobre.
[186] Aristotel, *Nikomahova etika*, 1164a 34–37.
[187] Isto, 1163a 22–25.
[188] Isto, 1155a 5–7.

domeni ponovno ima smisla kada nam je fenomen proučavanja *blockchain*. Priložit ću još jedan citat raspravi u ovom potpoglavlju:

»Karakter, dobar ili loš, proizvodi se prema onome što Aristotel naziva *navikama*, to jest, to je rezultat ponovljenog djelovanja koje ima sličnu ili uobičajenu kvalitetu. Takvo ponavljanje koje djeluje na prirodne sposobnosti ili sklonosti postupno ih popravlja u jednom ili drugom pravcu dajući im pristranost prema dobru ili zlu. Zbog toga se djela koja određuju dobro ili loše u karakteru moraju izvesti na određeni način, a da bi se formirao dobar karakter zahtijeva se disciplina i usmjeravanje. Nije da subjekt sam ne pridonosi stvaranju vlastitog karaktera, ali u početku mu je potreban vodič. Poanta nije da se proces ne može sigurno prepustiti prirodi već da se ne može povjeriti samo intelektualnom poučavanju. Taj proces je asimilacija, a podrazumijeva imitaciju koja se usmjerava i kontrolira. Rezultat je sve veće razumijevanje onoga što je učinjeno, usmjerenost k cilju i etabliranje svrhe. Prava djela i osjećaji postaju navikama čije je upražnjavanje sve lakše i ugodnije te činjenje pravih djela postaje *druga priroda*. Subjekt stječe snagu da ih slobodno i dobrovoljno čini sve više od samoga sebe i po sebi.«[189]

Držim da je evidentno da se i ograničenja u uporabi koja nailazimo u *blockchainu* također mogu promatrati iz prizme etike vrlina, a s pojmom *intencije,* koji je detektiran kao ključan, raspravu se može odvesti sve dalje i dalje u smjeru proučavanja Aristotela. Ovaj rad ipak ima drugi cilj te ću se na ovom mjestu zbog toga i zaustaviti.

4.3.1. Napad 51 posto

Kada govorimo o donošenju konsenzusa kod odlučivanja o jedinstvenoj povijesti transakcije podataka, moramo imati na umu da svaki čvor ima pravo glasa (eng. *voting schema*). Većina u ovom slučaju odlučuje o nečemu što je fundamentalno za funkcioniranje i rad bilo koje platforme koja je nastala na *blockchain* tehnologiji. U slučaju da jedna ili više osoba, u naumu da ostvare svoje interese, pokušaju manipulativno kontrolirati povijest transakcije podataka tada se to u domeni *blockchain* algoritma, tj. načina na koji funkcionira

[189] J. A. Smith, »The Ethics of Aristotle«, para. 17, u: Aristotle, *Ethics*, Project Gutenberg, 2005. [Microsoft Edge, .epub format]

ta tehnnologija, zove *napad 51 posto* (eng. *a 51 percent attack*). Već smo naznačili da je takva manipulacija izuzetno skupa jer je potrebno mijenjati cjelokupnu povijest transakcije podataka do korijenskog bloka u Merkleovu stablu, ali je teoretski moguća.[190] Ako se ona dogodi, tada bi mogao nastupiti scenarij u kojem jedan čovjek ili interesna skupina ljudi kontrolira cijelu mrežu i radi po vlastitoj volji:

»Recimo da je neki bogati despot odlučio da je *Bitcoin*, poput interneta prije njega, postao toliko utjecajan da predstavlja prijetnju njegovoj moći. Taj despot bi mogao iskoristiti svu rudarsku moć [eng. *mining power*] te kupiti ostatak (čvorova) od zemalja koje još uvijek toleriraju njegovo loše ponašanje da bi mu pomogli u kontroliranju više od 50 posto mreže. On tada može odlučiti koje će transakcije uključiti u blokove, a koje će odbiti. S dobivenom kontrolom može odlučiti hoće li manipulirati kodom i uvesti nekoliko zabrana (...).«[191]

O ovoj se problematici može govoriti i pisati iz više aspekata. S ekonomskog aspekta, napadači žele promijeniti povijest transakcije podataka da bi osigurali veću količinu vlasništva u svoju korist. Ako govorimo o kolektivnom donošenju odluka, ova manipulacija ima namjeru proizvesti konačan rezultat koji bi išao u korist napadača, ako se o nečemu već treba zajednički odlučiti. S tehničkog aspekta, napad ima za cilj destabilizirati ili potpuno uništiti integritet i povjerenje u sustavu, što će ga učiniti neodrživim i u konačnici besmislenim. Ako problematici pristupamo s pozicije centralizacije, tada ovakav napad zasigurno ima mogućnost izmijeniti arhitekturu sustava i uvesti prikriveni centralitet. Kod svih ovih aspekata, ključ je kontrolirati većinu[192] da bi potencijalni napad uspio, a taj minimum iznosi 51 posto te je po tome i ova problematika dobila ime.[193] Međutim, ako pojedinac ili neka interesna grupacija dođe u mogućnost da kontrolira tehnologiju koja je u svojoj biti dizajnirana da pripada decentraliziranoj mreži, onda je to nepravedno. Ako je

[190] »Žestoko natjecanje je pomaklo rudarenje od pojedinaca s rudarskim platformama prema rudarskim bazenima i prilagođenim *ASIC*-ovima [eng. *Application-Specific Integrated Circuit*] tako da nekoliko velikih rudarskih bazena registrira većinu novih *Bitcoin* blokova i počeli su dosezati prag od 51 posto kontrolirane *hash* snage, što bi moglo rezultirati potpunom prevlasti (rudarskih bazena) u rudarenju.« Vidi: M. Swan, *Blockchain*, str. 66.
[191] A. Tapscott, D. Tapscott, »Powerful incumbents of the old paradigm will usurp it«, para. 6, u: *Blockchain Revolution*. [Microsoft Edge, .epub format]
[192] »Mnogi *blockchain* sustavi djeluju kao demokracije. Nužna je većina čvorova (51 posto) u *blockchain* mreži da bi se sprovela određena promjena.« Vidi: T. Laurence, *Blockchain for Dummies*, str. 134.
[193] »Koncept napada 51 posto jedan je od najvećih slabosti *blockchain* sustava *Bitcoina*. Ako više od 51 posto rudara u mreži *Bitcoina* kontrolira jedna grupa, onda oni mogu manipulirati *blockchain* sustavom u *Bitcoinu.* Ako će mreža biti ugrožena onda će *token* izgubiti svoju vrijednost, a podaci koji su bili osigurani unutar mreže postat će ugroženi.« Vidi: isto, str. 89.

nepravedno onda nije u skladu s pravednošću[194] koja predstavlja najvišu vrlinu.[195] Nikome nije po volji da se izlaže nepravdi,[196] a prema Tapscottima, teško da scenarij ovakvog napada možemo u budućnosti izbjeći.[197] Nesumnjivo je da navedeni problem predstavlja izazov *blockchain* tehnologiji. Jedino rješenje koje se zasad nudi jest da će potencijalnim napadačima cijeli proces biti preskup te da će radi toga sa svojim namjerama odustati prije nego što su napad počeli ozbiljno planirati.[198] Kod *blockchaina* važi načelo transparentnosti i ulazak novih članova omogućen je svima.

4.3.2. Ostali koruptivni elementi

Ulazak novih članova u decentraliziranu mrežu ravnopravnih računala koja ima bazu na *blockchain* tehnologiji se potiče. *Blockchain* je dostupan svima i rado prihvaća nove čvorove u sustav. Jednom riječju, blockchain je transparentan. A načelo transparentnosti je korisno jer više korisnika u sustavu može verificirati transakcije te se mnogo lakše može uočiti i ispraviti problem dvostrukog trošenja (eng. *double spending*). S jedne strane, ukoliko omogućimo otvoreni *blockchain* sustav, utoliko su svi transakcijski podaci dostupni svima te je vlasništvo poprilično sigurno,[199] a kritika se može uputiti u smjeru manjka privatnosti. S druge strane, ako odlučimo ograničiti pristup i prihvaćati samo određene članove, tada se dokida načelo transparentnosti i postoji mogućnost da se razvijaju privatni *blockchain* sustavi. Na ovoj točki rasprave možemo se zapitati koliko ima smisla da se razvija više *blockchain* sustava koji su privatni naspram jednog jedinstvenog i transparentnog. S jedne strane, *blockchain* jamči sigurnost vlasničkih podataka i omogućava direktnu interakciju svih

[194] »Tako je pravedno ono što je zakonito i jednako, a nepravedno ono što je protuzakonito i nejednako.« Vidi: Aristotel, *Nikomahova etika*, 1129a 34–35.
[195] »Dakle, takva je pravednost savršena krepost, ali ne uopće, nego u odnosu prema nekomu drugom. Zbog toga se pravednost često i čini najvećom kreposti *te ni Večernjica ni Danica nije tako divna* i poslovnično kažemo *u pravednosti su skupljene sve prednosti*. I ova je u potpunosti savršena krepost, jer je poraba savršene kreposti.« Vidi: isto, 1129b 25–31.
[196] »Dakle, čovjeku se hotimice škodi i on trpi nepravdu, ali nitko se hotimice ne izlaže nepravednu postupku; naime nitko toga ne želi; jer nitko ne želi ono što ne smatra da je valjano.« Vidi: isto, 1136b 5–9.
[197] A. Tapscott, D. Tapscott, »Powerful incumbents of the old paradigm will usurp it«, para. 6, u: *Blockchain Revolution*. [Microsoft Edge, .epub format]
[198] Može se zamisliti scenarij u kojem se svi ostali čvorovi udruže kako bi odbili napad zlog despota ili male interesne skupine. Vidi: A. Tapscott, D. Tapscott, »Powerful incumbents of the old paradigm will usurp it«, para. 7, u: *Blockchain Revolution*. [Microsoft Edge, .epub format]
[199] »Blockchain definira vlasništvo na temelju cjelokupne povijesti podataka o transakcijama koja je dostupna svima. Rezultat je toga da je blockchain sličan javnom registru transakcija ili javnoj knjizi transakcija. Otvorenost i transparentnost temeljni su pojmovi blockchaina za verifikaciju vlasništva.« Vidi: D. Drescher, *Blockchain Basics*, str. 214.

korisnika, ali pritom zadirući u privatnost na višoj razini,[200] a s druge strane omogućava se pristup samo nekim, probranim članovima pri čemu manjak čvorova znači i nestabilniji sustav koji je više podložan napadu od 51 posto. Sve daljnje implikacije o rješenju ove točke napetosti mogu biti samo nagađanja – hoće li to značiti da će postojati više privatnih *blockchain* sustava ili hoće li fizičke i pravne osobe moći prodavati svoje podatke zainteresiranim dionicima na tržištu? U ovom je trenutku teško zaključiti bilo što osim da je svrha *blockchaina* da nastoji očuvati vrijednosti povjerenja i integriteta u svim decentraliziranim sustavima mreže ravnopravnih računala, bili oni privatni ili javni *blockchain* sustavi.[201]

Pitanje odgovornosti[202] također je pitanje koje može postati potencijalno koruptivni element ove tehnologije. Uzmimo za primjer sklapanje današnjih poslova. Potrebno je najmanje dvoje ljudi koji predstavljaju, primjerice, dva dionička društva na tržištu rada i pronašli su točku interesa te žele surađivati. Potpišu ugovor i eventualne sporove rješavaju pravnim putem. Ako sklapanje poslova prebacimo u potpunosti na *blockchain* tehnologiju (što je moguće jer ukida posredništvo), više neće biti potrebe za sastancima i potpisivanjem fizičkih ugovora. Međutim, ukoliko položimo sve povjerenje u tehnologiju i u nju se u potpunosti oslonimo, utoliko bi to moglo značiti i manjak odgovornosti. Dakako, može se ustanoviti da je problem s tehničke strane riješen pametnim ugovorima (eng. *smart contracts*). Budući da zasad ne postoji čvrsti zakonski okvir koji regulira pametne ugovore zato što bi to značilo prebacivanje cjelokupne paradigme pravne znanosti na digitalnu platformu ili barem njeno djelomično prilagođavanje, možemo također ustanoviti da i s pravne strane postoji rješenje koje leži u reguliranju prava obaveza na digitalnoj platformi i dodatnim donošenjem zakona koji se odnose na *blockchain* tehnologiju. Međutim, ostvarenjem tog scenarija nismo se ni dotaknuli pitanja prebacivanja odgovornosti na tehnologiju i prihvaćanja, tj. poricanja

[200] Isto, str. 245.
[201] Isto, str. 219.
[202] »Nismo navikli da je upravljanje osobna odgovornost i sustav ravnopravnih partnera, za razliku od nečega što je izvana nametnuto od udaljene centralizirane institucije. Nismo se navikli na mnoge vidove *blockchain* tehnologije (…) no znamo se naučiti odgovarajućoj razini stručnosti, konceptima i novim oblicima ponašanja prilikom usvajanja novih tehnologija. Nismo naviknuti na decentralizirani politički autoritet i političku autonomiju.« Vidi: M. Swan, *Blockchain*, str. 52.

odgovornosti jer se subjekt o kojem se raspravlja nalazi u digitalnom, da ne kažemo apstraktnom svijetu, odvojen od realnosti.[203]

Nadalje, sve učestalijom uporabom tehnologije u poslovanju nekih svjetskih korporacija postavlja se i pitanje gubitka poslova. Ljudi će radi automatizacije i standardizacije poslova gubiti poslove, to je neminovno. Međutim, realno stanje stvari je ponekad izuzetno grubo. Što će se desiti, primjerice, s pedesetogodišnjim vozačima ili skladištarima niže stručne spreme koji taj posao rade već tridesetak godina i imaju obitelji? Kakav će to utjecaj imati na tržište rada i mjere države u budućnosti? Hoće li Vlade biti socijalno osjetljive i hoće li država subvencionirati prekvalifikaciju za osobe navedene u primjeru kako bi im se našao adekvatan posao kojim će moći osigurati egzistenciju? Možemo postaviti i općenitije pitanje – kakve će posljedice biti na globalno tržište rada?

Odgovor koji se javlja kao dugoročno rješenje je školovanje ljudi s višom stručnom spremom radi pojave sve specijaliziranijih zanimanja i poslova. Međutim, nisu ni samo ljudi niže ili srednje stručne spreme pod upitnikom:

»Mnogi igrači u financijskoj industriji kao što su banke, brokeri, staratelji financijskih sredstava (eng. *custodians*), *moneytransfer* agencije i bilježnici izravno su vezani za vlastite posredničke uloge. Mnogi poslovi u tim ustanovama mogu biti ugroženi kada se veliki dio financijskih transakcija obrađuje automatiziranim putem preko *blockchaina*.«[204]

4.4. Pitanje morala i moralni izazovi

Postoje timovi ljudi koji konkretnim projektima nude odgovore na neka pitanja koja smo i u ovom radu postavili.[205] Iz tog razloga nezahvalno je predviđati budućnost. Ova tehnologija još je uvijek novina još će se mnogo pitanja pojaviti, mnogo aspekata ili segmenata same tehnologije, njenog utjecaja na društvo, politiku, sport, svakodnevni život, te ih je u ovom trenutku teško predvidjeti. U uvodu sam naglasio da će biti teško apstrahirati

[203] Prebacivanjem odgovornosti na tehnologiju ljudi konceptualno griješe jer tehnologija nije i ne može biti moralni subjekt. Vidi: Philip Brey, »Values in technology and disclosive computer ethics«, str. 87.
[204] D. Drescher, *Blockchain Basics*, str. 246.
[205] Usporedi: T. Laurence, »Ten Top Blockchain Projects«, *Blockchain for Dummies*, str. 193.

pitanje morala vezano uz *blockchain* u zasebno poglavlje. Kroz pozitivnu primjenu vjerujem da sam pokazao da pod pretpostavkom poštivanja ugrađenih moralnih vrijednosti možemo graditi svrsishodne i korisne projekte na *blockchainu*. Nemoguće je i nezahvalno pisati o negativnoj primjeni *blockchaina* jer bi se znanstveni rad pretvorio u, najblaže rečeno, znanstveno-fantastično djelo. Pisao sam o ograničenjima i zatim spomenuo koruptivne elemente. Čitatelju bi se na prvi pogled moglo činiti da je promašen naziv poglavlja – gdje se sakrio moral? Pomnijim isčitavanjem primjera koje sam spomenuo, a napose pitanja koja izviru iz sadržaja koruptivnih elemenata možemo primijetiti da se moral nalazi u svakoj pori svake implikacije koja je povezana s *blockchainom*. No zašto se onda gotovo i ne primijeti? Zašto ga je toliko teško uočiti i zašto smo toliko naglašavali problem apstrahiranja, najprije u uvodu, a potom i na samom početku ovog potpoglavlja? Nalazimo se na prijelazu iz tehnološkog doba u digitalno doba.[206] Tranzicija se neće odviti preko noći. Trebat će proći mnogo godina dok ne probijemo zamišljenu vertikalnu granicu. *Blockchain* je tehnologija koja je svojevrsni glasnik te tranzicije, a njenom potpunom primjenom u svim djelatnim sferama čovjekovog života, označavalo bi da je proces uhvatio nepovratni zalet. Adaptacijom i legitimacijom *kriptovaluta* u onom modelu kakvog smo ovdje opisali, promijenio bi se financijski sektor kakvog poznajemo. Promjena bi potom uslijedila u znanstvenom sektoru, politici itd.

Vratimo se na tezu iz prethodnog poglavlja: *techne* i *physis* su u *blockchainu* izrazito bliski. Ako to spojimo s tvrdnjom da moral izbija iz svake pore *blockchaina*, u spojnici tehničkog i ne-tehničkog moral će se pojavljivati kao kopula, kao vezivna tvar koja to dvoje spaja.[207] Najveći etički regulatori *blockchaina* su upravo inženjeri koji rade na novim projektima sa spomenutom tehnologijom kao bazom. Oni nastoje tehnički poboljšati sustav gdje je to moguće da bi se očuvao integritet i povjerenje, a cjelokupni narativ koji

[206] »Dakle, živimo u tehnološkom dobu [eng. *tech age*] koje će dovesti do doba digitalne valute [eng. *digital currency age*].« Usporedi: Nikolay Syusko, »Is there a chance for blockchain without Cryptocurrencies«, *Hackernoon* (31. 7. 2018.). Dostupno na: https://hackernoon.com/is-there-a-chance-for-blockchain-without-cryptocurrencies-2e6afa924549 (pristupljeno 23. 8. 2018.); Jorge Becerra, »The digital revolution is not about technology – it's about people«, *World Economic Forum* (28. 3. 2017.). Dostupno na: https://www.weforum.org/agenda/2017/03/the-digital-revolution-is-not-about-technology-it-s-about-people/ (pristupljeno 30. 8. 2018.); Alfonso Fernández, »Are we in the Digital Transformation era?«, *Medim Corporation* (21. 4. 2018.). Dostupno na: https://medium.com/@fonso149/are-we-in-the-digital-transformation-era-6a567f8e31cb (pristupljeno 30. 8. 2018.).

[207] »Nekoć nije samo tehnika nosila ime τέχνη. Nekoć je τέχνη značila i ono otkrivanje, koje je istinu pro-iz-vodilo u sjaj sijajućega. Nekoć je τέχνη značila i pro-iz-vođenje istinitoga u lijepo. Τέχνη je značila i ποίησις lijepih umjetnosti.« Vidi: M. Heidegger, »Pitanje o tehnici«, str. 245.

podrazumijeva dosege i implikacije *blockchaina* seli se na digitalnu platformu. Zato nam sada jest teško uočiti pojam morala, a bit će gotovo ekstravagantno kada će se pojavljivati nova, dosad neviđena pitanja koja su s moralom povezana, a dolaze s digitalne platforme. Primjerice, je li moralno opravdano rušiti *blockchain* sustav koji arhivira podatke o eutaniziranim osobama u nekoj bolnici? Ili, je li moralno opravdano trgovati na burzi *kriptovalutom* koja skriva transakcijske podatke, a njome se može kupiti oružje? Da zaključimo: moralni izazovi će i dalje postojati, samo što će u sve većem broju dolaziti s digitalne platforme. Ne postoji naznaka da će moralne vrednote nestati ili se transformirati u nešto nepoznato ili neviđeno, nego će se promjenom konteksta djelatnosti pojavljivati u sve većoj dihotomiji s tehnologijom.

5. Zaključak

Određivanje etike vrline kao etičkog temelja za *blockchain* tehnologiju je samo prvi korak. Nemojmo zaboraviti da je etika, prije svega, studija o moralu. I dalje krajnja, posljednja odluka ostaje na pojedincu. Kada govorimo o moralnosti ulazimo u »dolinu subjektivnosti«. U toj dolini, netko bi svoje akcije, koje negativno djeluju na sustav, mogao opravdavati kao najbolje moguće i reći da upravo njima pokušava izgraditi i zadržati moralni integritet. Ovdje se otvara širok prostor za djelovanje humanističkih znanosti u budućnosti. Upravo će humanisti, napose filozofi, imati priliku iskoristiti širinu prostudirane literature da bi jasno, smisleno i egzaktno postavili problematiku i detektirali specifična pitanja koja treba riješiti. U svakom slučaju, rapidni porast tehnologije značajno će utjecati na razvijanje filozofije odgoja i zahtijevat će prilagodbu školskog sistema. Djecu ćemo zasigurno trebati više učiti kritičkom razmišljanju, komunikaciji i njenoj važnosti, emocijama, fiziologiji i njenom utjecaju na naš svakodnevni život, timskom radu i tzv. mekim vještinama.[208] Tehnologija će nam olakšati život, ali nas i svojevrsno natjerati da spoznajemo sami sebe. Unatoč svim naporima da se normiraju pozitivne vrijednosti te da se kroz edukaciju stavi naglasak na učenje o vrlinama, unatoč svim nastojanjima da poopćimo etiku vrlina i promoviramo jačanje karaktera te sociološku dimenziju čovjeka koja proizlazi iz društvenog života, i dalje će odluke donositi sam pojedinac. Spomenuli smo da u *blockchain* tehnici imamo zanimljiv moment kakvog vjerojatno nikada u povijesti prije nismo imali. Naime, inženjeri koji rade na razvijanju mogućnosti primjena *blockchain* tehnologije i poboljšavanju njenih svojstava ujedno su i etički regulatori. Oni pokušavaju stvoriti sustav koji će ostvariti povjerenje i integritet da bi čvrsto utemeljili sigurnost, a to rade u inovativnom, tehničkom

[208] »Usklađenost [eng. *coherence*] je stanje maksimalne i iznimne učinkovitosti u kojem se tijelo i um sjedinjuju (…). Usklađenost i prosvijećeno vodstvo [eng. *enlightened leadership*] je poziv na ponovno zamišljanje nove budućnosti. Budućnosti koja se ne mjeri samo materijalističkim nagradama nego i onom koja redefinira samu svrhu poslovanja tako da podupire čovječanstvo i ljudsku evoluciju. Trebamo novi način praćenja postignuća u poslovanju, novu krajnju crtu koja predstavlja povratak financijskom kapitalu ali i povratak prirodnom, društvenom i ljudskom kapitalu. Tek tada možemo zaista znati pravu vrijednost poslovanja.« Vidi: A. Watkins, »Conclusion«, para. 1 [Microsoft Edge, .epub format]. Watkins u svojoj knjizi predočuje činjenice kojima dokazuje da je tajna u uspješnom performansu kojeg realni sektor najviše traži u koherentnosti. Ta koherentnost se postiže najprije fiziološkom koherentnošću koja facilitira emocionalnu koherentnost. Tvrdi i obrazlaže da emocije utječu na naše osjećaje koji pak utječu na naše razmišljanje (eng. *thinking*). Razmišljanje utječe na naše ponašanje koje u konačnici utječe na naše rezultate. Watkins, po struci kardiolog, u zaključku svoje knjige piše da činjenice koje obrazlaže za znanstveno-empirijskog stajališta nisu prisutne u većini obrazovnih institucija. Svojim je istraživanjima autor prisutan u konzultantskoj ulozi u realnom sektoru.

okruženju s pretpostavkom da je razina povjerenja u sustavu minimalna. Ništa više ni manje, prijedlog je raditi na vrlinama i zato je apostrofirana etika vrlina. Definicija na početku rada bila je proizvoljna, no isključivo analizom uočio sam nevjerojatne sličnosti unutar sistema *blockchaina* i platonističkog, a nadasve aristotelijanskog učenja o vrlinama. Raditi na etici vrlina tako ima za posljedicu još živopisnije približavanje Heideggera pripadajućem vremenu – uz rapidni porast tehnologije ne izgubiti sebe.[209] Taj bi se fenomenološki nauk mogao u našem prikazanom slučaju ostvariti u traženju vrlina, a onda i njihovom konzistentnom njegovanju. Etika vrlina se s racionalne perspektive nesumnjivo nameće kao model koji je kompatibilan s dosezima *blockchain* tehnologije te je sposobna ponuditi prijedloge koji bi se odrazili u pozitivnom svjetlu kod primjene *blockchaina* u budućnosti. U radu sam mnogo pažnje posvetio objašnjenju i opisivanju tehničkog aspekta *blockchain* tehnologije. Kao što sam u uvodu upozorio, držim da je to bilo od izuzetne važnosti da bismo uopće mogli ući u ne-tehnički, odnosno etički aspekt proučavanja te tehnologije i njezinih dosega. Iako sam u radu predložio da je etika vrlina najbliža fundamentu na kojem je *blockchain* tehnologija napravljena, to nikako ne smije biti apsolutan i isključivi stav. Znamo da ne postoji stroga granica podjele u etici, filozofskoj discplini proučavanja morala. Kao što smo već i naglasili, mjesta za norme, vrline i svrsishodnost ima u svakoj etičkoj perspektivi, razlika je jedino u tome koji je njen fokus. Utvrdio sam da je prema tome etika vrlina najbliža, što ne znači da je to dogmatička pozicija s koje se treba objasniti sadašnju i daljnju primjenu ove tehnologije.

Naprotiv, ovaj rad samo je mali doprinos u počecima proučavanja *blockchaina* i nadam se da će potaknuti daljnje rasprave i analize, čak i neka argumentirana viđenja koja su suprotna onima iznesenim u ovome radu. U tom ću slučaju biti izrazito zadovoljan jer će to ujedno značiti porast interesa za ovo pitanje, kao i pitanje daljnjeg razvijanja tehnologije u suživotu s čovjekom uopće. Ukoliko taj porast interesa preraste u kritičko sagledavanje koje se pretoči u kvalitetnu literaturu na temelju koje će se podučavati djeca i studenti utoliko

[209] »Kao ono bitstveno tehnike, po-stava je ono što traje. Vlada li ona čak u smislu onoga što se obistinjuje? Već je to pitanje, čini se, očit promašaj. Jer po-stava je ipak prema svemu rečenom–usud, koji sabire na izazivajuće otkrivanje. Izazivanje je sve drugo samo ne obistinjavanje. Tako izgleda dokle god ne obratimo pozornost na to da izazivanje u postavljanje zbiljskoga kao *ostave* još uvijek jest nekakvo pućenje, koje čovjeka puti na put otkrivanja. Kao taj usud, ono bitstveno tehnike pušta čovjeka u ono što on sam od sebe ne može ni naći ni uopće praviti: jer, tako nečega kao čovjek, koji je sam od sebe samo čovjek–nema.« Vidi: M. Heidegger, »Pitanje o tehnici«, str. 243. Usp.: Damir Sekulić, »Heideggerovo poimanje tehnike«, *Bilten studentskih radova iz filozofije*, vol. 2, br. 2, 2016., str. 29–52. Dostupno na: https://hrcak.srce.hr/183355 (pristupljeno 30. 8. 2018.).

postoji veća vjerojatnost da ćemo se kao društvo nastojati kretati prema pozitivnim praksama primjene ove, ali i svih drugih tehnologija.

Na temelju proučavanja *blockchain* tehnologije, zaključio sam da ona definitivno neće biti samo prolazna tehnologija u ljudskoj evoluciji. Dapače, smatram da neće postati neka pomoćna tehnologija u određenim informatičkim sustavima. Uvjeren sam da će upravo *blockchain* predstavljati ključnu tehnološku inovativnost u budućnosti, kao što je to svojevremeno predstavljao Internet, ili ranije izum televizije ili radio-prijamnika te da će vremenom ljudi uviđati prednosti koje im onda nudi. Bez ustezanja ću reći da će *blockchain* predstavljati iznimno važnu tehnološku podlogu u informacijskim sustavima u budućnosti te da će utjecati na politiku, ekonomiju, znanost i, općenito govoreći, sve sfere ljudskog života. Ponovit ću, svjestan sam da *blockchain* ima mnogo toga što treba popraviti, ali potencijal i dosadašnji dosezi su preveliki da bi se ta tehnologija ignorirala. Štoviše, ideja *blockchaina* je genijalna i vjerujem da će nam u budućnosti otkriti neke svoje aspekte koje sada još ne možemo predvidjeti.

6. Literatura

- »About Bitfury«, *Bitfury Group Limited*. Dostupno na: https://bitfury.com/about (pristupljeno 23. 8. 2018.).
- »Algoritam«, *Hrvatska enciklopedija*. Dostupno na: http://www.enciklopedija.hr/Natuknica.aspx?ID=1718 (pristupljeno 11. 9. 2018.).
- »All Cryptocurrencies«, *CoinMarketCap*. Dostupno na: https://coinmarketcap.com/all/views/all/ (pristupljeno 11. 9. 2018.).
- »Softver«, *Hrvatska enciklopedija*. Dostupno na: http://www.enciklopedija.hr/natuknica.aspx (pristupljeno 30. 8. 2018.).
- »Tehnika«, *Hrvatska enciklopedija*. Dostupno na: http://www.enciklopedija.hr/Natuknica.aspx (pristupljeno 29. 8. 2018.).
- »Tehnologija«, *Hrvatska enciklopedija*. Dostupno na: http://www.enciklopedija.hr/Natuknica.aspx (pristupljeno 29. 8. 2018.).
- »The Corda Platform, Blockchain for every business in every industry«, *R3*. Dostupno na: https://www.r3.com/corda-platform/ (pristupljeno 23. 8. 2018.).
- »The Story of Openbazaar«, *Openbazzar*. Dostupno na: https://www.openbazaar.org/ (pristupljeno 23. 8. 2018.).
- »Vrlina «, *Hrvatska enciklopedija*. Dostupno na http://www.enciklopedija.hr/Natuknica.aspx (pristupljeno 28. 8. 2018.).
- »What is Dash?« *Dash Core Group, Inc.* Dostupno na: https://docs.dash.org/en/latest/introduction/about.html (pristupljeno 23. 8. 2018.).
- Alan Watkins, *Coherence: The secret science of briliant leadership*, Complete Coherence Limited, London 2014. [Microsoft Edge, .epub format]
- Alex Tapscott, Don Tapscott, *Blockchain Revolution*, Brilliance Audio, 2016. [Microsoft Edge, .epub format]
- Alfonso Fernández, »Are we in the Digital Transformation era?«, *Medim Corporation* (21. 4. 2018.). Dostupno na: https://medium.com/@fonso149/are-we-in-the-digital-transformation-era-6a567f8e31cb (pristupljeno 30. 8. 2018.).
- Aristotel, *Metafizika*, Globus: Sveučilišna naklada Liber, Zagreb 1988.

- Aristotel, *Metafizika*, Globus: Sveučilišna naklada Liber, Zagreb 1988.

- Aristotel, *Nikomahova etika*, Sveučilišna naklada Liber, Zagreb 1982.
- Aristotle, *Ethics*, Project Gutenberg, 2005. [Microsoft Edge, .epub format]
- Vangie Beal, »fixed length«, *Webopedia*. Dostupno na: https://www.webopedia.com/TERM/F/fixed_length.html (pristupljeno 10. 9. 2018.).
- Jorge Becerra, »The digital revolution is not about technology – it's about people«, *World Economic Forum* (28. 3. 2017.). Dostupno na: https://www.weforum.org/agenda/2017/03/the-digital-revolution-is-not-about-technology-it-s-about-people/ (pristupljeno 30. 8. 2018.).
- Robert Angus Buchanan, »History of technology«, *Encyclopaedia Britannica*. Dostupno na: https://www.britannica.com/technology/history-of-technology (pristupljeno 29. 8. 2018.).
- Daniel Cawrey, »How Economist Milton Friedman predicted Bitcoin«, *CoinDesk* (5. 3. 2014.). Dostupno na: https://www.coindesk.com/economist-milton-friedman-predicted-bitcoin/ (pristupljeno 28. 8. 2018.).
- Tim Collins, »The rise of Bitcoin was predicted by Nobel Prize winning economist Milton Friedman in an interview recorded 18 years ago, footage reveals«, *Associated Newspapers Ltd*. (20. 10. 2017.). Dostupno na: http://www.dailymail.co.uk/sciencetech/article-5000260/Bitcoin-predicted-Milton-Friedman-18-years-ago.html (pristupljeno 28. 8. 2018.).
- Charles Dearing, »Nobel Laureate Milton Friedman Predicted Bitcoin Era 17 Years Ago«, *Cointelegraph* (7. 7. 2017.). Dostupno na: https://cointelegraph.com/news/nobel-laureate-milton-friedman-predicted-bitcoin-era-17-years-ago (pristupljeno 28. 8. 2018.).
- Daniel Drescher, *Blockchain Basics*: *A Non-Technical Introduction in 25 Steps*, Apress, Frankfurt am Main 2017.
- Richie Etwaru, »TEDx Talks: Blockchain: Massively Simplified«, *YouTube* (15. 5. 2017.). Dostupno na: https://www.youtube.com/watch?v=k53LUZxUF50&t=51s (pristupljeno 13. 9. 2018.).
- Luciano Floridi, *The Cambridge Handbook of Information and Computer Ethics*, Cambridge University Press, New York 2010.

- David Gerard, *Attack of the 50 Foot Blockchain*, Createspace Independent, 2017. [Microsoft Edge, .epub format]
- Gordon Graham, *Theories of Ethics: An Introduction to Moral Philosophy with a Selection of Classic Readings*, Routledge, New York 2010.
- Harry J. Gensler, *Ethics*: *A Contemporary Introduction*, Routledge, New York 2011.
- John Paul Hampstead, »*Blockchain* without cryptocurrencies«, *Freightwaves* (12. 3. 2018.). Dostupno na: https://www.freightwaves.com/news/blockchain/blockchain-without-cryptocurrencies (pristupljeno 23. 8. 2018.).
- Martin Heidegger, »Pitanje o tehnici«, u: Martin Heidegger, *Kraj filozofije i zadaća mišljenja*, Naprijed, Zagreb 1996.
- Barbara Horvat, *Kantova metafizika ćudoređa* (diplomski rad), Filozofski fakultet Osijek, Odsjek za filozofiju, Osijek 2017.
- Rosalind Hursthouse, Glen Pettigrove, »Virtue Ethics«, *The Stanford Encyclopedia of Philosophy*, 2016. Dostupno na: https://plato.stanford.edu/archives/win2016/entries/ethics-virtue/ (pristupljeno 25. 8. 2018.).
- Immanuel Kant, *Fundamental Principles oft he Metaphysic of Morals*, Project Gutenberg, 2004. [Microsoft Edge, .epub format]
- Immanuel Kant, *Kritika praktičkog uma,* preveo Viktor D. Sonnefeld, Naprijed, Rijeka 1974.
- Immanuel Kant, *Osnivanje metafizike ćudoređa*, preveo Viktor D. Sonnenfeld, Feniks, Zagreb 2003.
- Lorne Lantz, »TED Talks: The Blockchain Explained Simply«, *YouTube* (21. 12. 2016.). Dostupno na: https://www.youtube.com/watch?v=KP_hGPQVLpA&t=22s (pristupljeno 6. 9. 2018.).
- Tiana Laurence, *Blockchain for Dummies*, John Wiley & Sons, Inc., Hoboken, New Jersey 2017.
- Luka Lujić, *Pravno uređenje kriptovaluta* (diplomski rad), Pravni fakultet u Zagrebu, Katedra za pravnu informatiku, Zagreb 2017.

- R. Jesse McWaters, »The future of financial services: How disruptive innovations are reshaping the way financial services are structured, provisioned and consumed; an Industry Project of the Financial Services Community«, *World Economic Forum* 2015. Dostupno na: http://www3.weforum.org/docs/WEF_The_future__of_financial_services.pdf (pristupljeno 23. 8. 2018.).
- John Sutart Mill, *Utilitarianism*, Oxford University Press, New York 1998.
- John Stuart Mill, *Izabrani politički spisi*, Informator, Fakultet političkih znanosti, Zagreb 1988.
- William Mougayar, Vitalik Buterin, *The Business Blockchain*: *Promise, Practice, and Application of the Next Internet Technology*, John Wiley & Sons, Inc., Hoboken, New Jersey 2016. [Microsoft Edge, .epub format]
- Carl Miller, »TEDx Talks: Digital Democracy«, *YouTube* (4. 5. 2016.). Dostupno na: https://www.youtube.com/watch?v=FNL22RvFwn0 (pristupljeno 11. 9. 2018.).
- Satoshi Nakamoto, »Bitcoin: A peer-to-peer electronic cash system«, *Bitcoin Project*, 2008. Dostupno na: https://bitcoin.org/bitcoin.pdf (pristupljeno 16. 8. 2018.).
- Jared Norton, *Blockchain*: *Easiest Ultimate Guide To Understand Blockchain*, CreateSpace Independent Publishing Platform, 2016.
- Martin Peterson, *The Ethics of Technology*: *A Geometric Analysis of Five Moral Principles*, Oxford University Press, New York 2017.
- Platon, *Država*, preveo Martin Kuzmić, Naklada Jurčić, Zagreb 2004.
- Geoff Sayre-McCord, »Metaethics«, *The Stanford Encyclopedia of Philosophy*, 2014. Dostupno na: https://plato.stanford.edu/archives/sum2014/entries/metaethics (pristupljeno 16. 8. 2018.).
- Damir Sekulić, »Heideggerovo poimanje tehnike«, *Bilten studentskih radova iz filozofije*, vol. 2, br. 2, 2016., str. 29–52. Dostupno na: https://hrcak.srce.hr/183355 (pristupljeno 30. 8. 2018.).
- Melanie Swan, *Blockchain*: *Blueprint for a New Economy*, O'Reilly Media, Inc., Sebastopol, California 2015.

- Nikolay Syusko, »Is there a chance for blockchain without Cryptocurrencies«, *Hackernoon* (31. 7. 2018.). Dostupno na: https://hackernoon.com/is-there-a-chance-for-blockchain-without-cryptocurrencies-2e6afa924549 (pristupljeno 23. 8. 2018.).
- Ljiljana Šarić, Igor Čatić, »Raznoznačnost naziva tehnika i tehnologija«, *Mehanizacija šumarstva* 23 (1998) 3–4, str. 157–162.
- Roger Wattenhofer, *The Science of the Blockchain,* Inverted forest publishing, 2016.
- Eric W. Weisstein, »Hash Function«, *MathWorld*. Dostupno na: http://mathworld.wolfram.com/HashFunction.html (pristupljeno 10. 9. 2018.).
- Gavin Wood, »Ethereum: A secure decentralized generalized transaction ledger«, *Gavin Wood,* 2014. Dostupno na: http://gavwood.com/paper.pdf (pristupljeno 15. 8. 2018.).