# Može lli blockchain tehnologija zamijeniti birokraciju?

**Ovničević, Tea**

**Master's thesis / Diplomski rad**

**2019**

*Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj:* **University of Zagreb, Department of Croatian Studies / Sveučilište u Zagrebu, Hrvatski studiji**

*Permanent link / Trajna poveznica:* https://urn.nsk.hr/urn:nbn:hr:111:688658

*Rights / Prava:* In copyright / Zaštićeno autorskim pravom.

*Download date / Datum preuzimanja:* **2024-04-25**

SVEUČILIŠTE U ZAGREBU
HRVATSKI STUDIJI
UNIVERSITY OF ZAGREB
CENTER FOR CROATIAN STUDIES

*Repository / Repozitorij:*

Repository of University of Zagreb, Centre for Croatian Studies

zir.nsk.hr

DIGITALNI AKADEMSKI ARHIVI I REPOZITORIJI

SVEUČILIŠTE U ZAGREBU
HRVATSKI STUDIJI

Tea Ovničević

# MOŽE LI BLOCKCHAIN TEHNOLOGIJA ZAMIJENITI BIROKRACIJU?

DIPLOMSKI RAD

Zagreb, 2019.

SVEUČILIŠTE U ZAGREBU
HRVATSKI STUDIJI
ODSJEK ZA SOCIOLOGIJU

Tea Ovničević

# MOŽE LI BLOCKCHAIN TEHNOLOGIJA ZAMIJENITI BIROKRACIJU?

DIPLOMSKI RAD
Mentorica: doc. dr. sc. Marija Brajdić Vuković

Zagreb, 2019

Sadržaj

1. UVOD ..... 4
2. NOVA INDUSTRIJSKA REVOLUCIJA? ..... 5
3. *BLOCKCHAIN* TEHNOLOGIJA ..... 7
3.1 Bitcoin ..... 7
3.1.1 Kratka povijest Bitcoina ..... 8
3.1.2 Glavni koncepti Bitcoin sustava ..... 10
3.1.3 Uloga rudara i čvorišta ..... 14
3.1.4 Zašto Bitcoin sustav funkcionira? ..... 18
3.2 Ethereum ..... 19
3.3 Distribuirani konsenzus ..... 21
3.4 Vrste *blockchaina* ..... 23
3.5 Problemi *blockchain* tehnologije ..... 25
4. BIROKRACIJA ..... 27
4.1 Stanje birokracije u Hrvatskoj ..... 33
*5. BLOCKCHAIN* KAO BIROKRACIJA 21. STOLJEĆA ..... 34
6. ZAKLJUČAK ..... 40
7. LITERATURA: ..... 43
**Sažetak** ..... 47
**Summary** ..... 48

# 1. UVOD

Na spomen Bitcoina[1] mnogi će se sjetiti medijskih napisa od prije nekoliko godina kada se govorilo o kriptovaluti koja će poharati svijet i zauvijek promijeniti smjer financijskog sustava, ili će se prisjetiti one kratke vijesti o poznatom glazbeniku koji je postao instant milijunaš jer je valuta skoro preko noći skočila u velike visine, ili će se, u krajnjem slučaju, sjetiti priče o nekom čovjeku koji s nekakvim uređajem doma sam sebi stvara novac. S druge strane, na spomen *blockchaina* (lanac blokova - eng. block – hrv. blok; eng. chain – hrv. lanac), mnogi će ustuknuti pred neznanjem i nejasnim, teško razumljivim informacijama ili će, pak, imati negativan stav o toj novoj tehnologiji koja je odjednom došla s nekim vjerojatno opakim ciljem.

Realnost je, premda ima neke veze s gore napisanim, ipak nešto drugačija. Ideja ovog rada jest pojasniti, na primjeru sustava Bitcoina, kako funkcionira *blockchain* kao jedna od tehnologija četvrte industrijske revolucije. Pojava Bitcoina i *blockchain* tehnologije za svijet računalne tehnologije značila je ogromnu prekretnicu pa ne čudi zainteresiranost za sudjelovanjem stručnjaka različitih područja u njezinom razvoju. S druge strane, za ostatak društva pojava ove tehnologije došla je prilično tiho, a njezino postojanje svi su osvijestili prije nekoliko godina kada je vrijednost kriptovalute bitcoin naglo porasla.

Cilj ovog rada je, osim šireg pojašnjenja tehnologije *blockchaina*, metodom misaonog eksperimenta objasniti kako bi se upravo ta tehnologija mogla iskoristiti za stvaranje velike promjene koja može imati iznimno veliki utjecaj na daljnji razvoj društva. U tom smislu, pokušat će se domisliti rješenje za obuzdavanje birokracije, kako je poimana u klasičnoj sociološkoj teoriji, kroz upotrebu *blokchain* tehnologije.

U prvom dijelu rada kratko ću se osvrnuti na društveni i tehnološki kontekst u kojem se *blockchain* tehnologija pojavila. Riječ je o novoj, četvrtoj po redu industrijskoj revoluciji, koja je, premda se povezala na onu prethodnu, donijela revolucionarne pomake u razvoju tehnologije i nevjerojatan zamašaj za daljnji razvoj društva. U drugom dijelu radu predstavit ću *blockchain* tehnologiju i objasniti kako funkcionira na sustavu Bitcoin, najvećem postojećem kriptovalutnom sustavu. U tom dijelu objasnit ću i mnoštvo novih pojmova, većinom iz računarskog područja, čije je poznavanje ključno za potpuno razumijevanje *blockchain* tehnologije.

[1] Zbog razumijevanja daljnjeg teksta, riječju Bitcoin označavat će se cjelokupni sustav kriptovalute koji funkcionira na *blockchainu*, dok će se sama kriptovaluta kao produkt sustava nazivati bitcoinom.

Potom ću se u radu vratiti k sociologiji i pojasniti teoriju birokracije Maxa Webera te predstaviti glavne kritike koje su nastale u sociologiji nakon njega. Nakon toga, pojmu birokracije suprotstavit ću pojam *blockchaina*, a kroz njihovu usporedbu prikazat ću potencijal koji *blockchain* tehnologija ima kao moguća zamjena za birokraciju. Kroz cijeli rad dat ću nekoliko primjera trenutne i moguće implementacije *blockchain* tehnologije.

## 2. NOVA INDUSTRIJSKA REVOLUCIJA?

Povijest čovječanstva obilježilo je nekoliko velikih prekretnica koje su zauvijek promijenile smjer razvoja društva. Svaka od tih prekretnica sa sobom je donijela neku vrst inovacije koja je olakšala ljudski rad i povećala efikasnost proizvodnje hrane i ostalih za život potrebnih sirovina, zbog čega su ljudi dobili vremena i prostora za daljnje istraživanje i razvoj, kako u ekonomskom, tako i u političkom i kulturnom smislu. Prva od tih većih prekretnica bila je agrarna revolucija koja se dogodila između 10. i 8. tisućljeća prije nove ere (Schwab, 2016), a obilježilo ju je prelazak na nomadski način života, prestanak lovačkih i sakupljačkih načina života i prelazak na uzgajački tip. Tada su ljudi počeli kultivirati biljke, a životinje koje su po prvi put uspjeli pripitomiti počeli su koristiti kao izvor hrane, radnu snagu za obradu polja i komunikaciju u smislu prijevoznih sredstava. Ovaj veliki pomak imao je za posljedicu stvaranje prvih većih naroda i gradova te daljnji razvoj i širenje kultura.

Druge velike promjene odnose se na razvoj tehnologija pomoću kojih su ljudi prestali koristiti svoju snagu za proizvodne procese, čime se povećala efikasnost proizvodnje dobara i kvaliteta proizvoda, što je za društveni razvoj imalo dalekosežne posljedice. Prva industrijska revolucija dogodila se između 18. i 19. stoljeća, a najvećim dijelom je obilježena izumom parnog stroja koji je doveo do nastanka prvih tvornica, željeznica i parobrodova. To je imalo velikog utjecaja na urbanizaciju, povezivanje različitih dijelova svijeta i općenito stvaranje novih sustava proizvodnje. Druga industrijska revolucija, koja se dogodila krajem 19. stoljeća, utemeljena je na izumu električne energije čija se primjena ubrzo proširila, što je sa sobom donijelo i korištenje pokretne trake te stvaranje masovne proizvodnje. Treću industrijsku revoluciju obilježio je izum računala i Interneta, a trajala je u razdoblju od 1960-ih do 1990-ih (Schwab, 2016). Ova je revolucija u najvećoj mjeri promijenila smjer društvenog razvoja jer je povezala ljude na dotada nezamislive načine i stvorila infrastrukturu za različite nove načine ljudskog djelovanja.

Govoreći o tri industrijske revolucije, moguće je razlikovati i dva strojna doba (van Est et al., 2015). Prvo strojno doba pokriva prve dvije industrijske revolucije, a karakterizira ga

zamjena mišićne snage onom strojnom. U tim razdobljima većinski manualni posao zamijenili su strojevi, čime je čovjek bio oslobođen teškog fizičkog rada. Treća industrijska revolucija spada u drugo strojno doba gdje su strojevi zamijenili kognitivnu snagu. Osim što ljudi više ne moraju raditi teške fizičke poslove, strojevi su preuzeli i određeni misaoni rad, odnosno, može se reći da su računala dovela do svojevrsne kognitivne automatizacije (van Est et al., 2015). Zahvaljujući tome danas je moguće računati i najteže matematičke funkcije, rješavati logičke zadatke ili isplanirati cijelo putovanje s troškovima goriva i cestarina uz pomoć računala.

Treća industrijska revolucija postavila je temelje za daljnji razvoj, koji je unazad 20 godina strelovitom brzinom pomakao granice zamislivog i doveo nas do nove, četvrte industrijske revolucije. Karakteristike ovog novog razdoblja su sveprisutan i mobilni Internet, manji, snažniji i jefitniji senzori, umjetna inteligencija i strojno učenje. Digitalne tehnologije koje počivaju na hardveru, softveru i mreži nisu novost ovog razdoblja, ali su postale sofisticiranije, puno više integrirane u druge sustave te kao rezultat imaju snažan utjecaj na globalnu ekonomiju i društvo u cjelini (Schwab, 2016). Razdoblje četvrte industrijske revolucije obilježeno je pojavom kibernetičko-fizičkih sustava (Bloem et al., 2014) pomoću kojih je moguće pomaknuti granicu između realnog i virutalnog, prebacujući materijalne stvari u virtualni svijet. Danas je moguće spojiti uređaje, strojeve, stvari, cijele tvornice i ostala industrijska postrojenja na Internet. Sukladno tome, velik broj djelatnosti koje su u prošlosti obavljali ljudi danas su automatizirane. Roboti obavljaju teške, prljave i dosadne poslove, i to mogu činiti kontinuirano, iznimno precizno i kvalitetno (Bloem et al., 2014), ostvarajući pri tome puno veću razinu produktivnosti. Četvrta industrijska revolucija drugačija je od svih prijašnjih jer uključuje različita područja, od sekvenciranja genoma, preko nanotehnologije i novih održivih oblika energije, do kvantnog računarstva, a djelokrug tih tehnologija proširio se i na biološko, fizičko i digitalno područje (Schwab, 2016). Tako je u današnje vrijeme moguće pročitati kako je netko cijelu kuću samostalno izgradio pomoću 3D printera[2] ili kako su znanstvenici spojili ljudske i životinjske stanice[3]. Granice zamislivog se svakodnevno pomiču.

Jedna od tehnologija novog doba koja ima potencijal iz korijena promijeniti način ljudskog odnosa prema informacijama je *blockchain*. To je tehnologija koja po prvi put omogućava decentralizirane i transparentne informacijske sustave u kojima nije potreban

[2] The world's first family to live in a 3D-printed home. Preuzeto s: https://www.bbc.com/news/technology-44709534. Učitano 16. kolovoza 2019.
[3] Human-Pig Hybrid Created in the Lab—Here Are the Facts. Preuzeto s: https://www.nationalgeographic.com/news/2017/01/human-pig-hybrid-embryo-chimera-organs-health-science/. Učitano 16. kolovoza 2019.

autoritet. U *blockchain* sustavu odnosi mikro i makro razina nisu ustanovljeni društvenim ugovorom ili nekim ustaljenim odnosom moći, već se ovaj aglomerat informacija može koordinirati kroz skalabilne i javno dostupne računalne resurse (Kavanagh i Miscione, 2015). *Blockchain* je nastao iz kriptografije kao tehnologija koja omogućava sustav kriptovaluta, a potencijal koji je pokazala vrlo brzo je potresao kako stručnu i akademsku zajednicu, tako i šire društvo. Financijski je sustav, kao prvi na udaru, s *blockchainom* dobio priliku riješiti se problema centralizacije, što bi za krajnje korisnike značilo da mogu slobodno izvršavati transakcije bez uplitanja autoriteta ili neke treće strane koja, osim što uzima proviziju za nadzor, prikuplja podatke o korisnicima te im oduzima nezavisnost. Zbog *blockchain* tehnologije tržište kriptovaluta je procvjetalo pa je tako i najveća društvena mreža, Facebook, pokrenula svoj projekt kriptovaluta i ubrzo će biti omogućeno plaćanje njihovom valutom i u dućanima. Daljnjim razvojem sustava na *blockchain* tehnologiji razvili su se i pametni ugovori koji omogućavaju izvršavanje određenih zadataka odmah po ispunjenju unaprijed zadanih uvjeta. To je omogućilo implementaciju *blockchain* tehnologije u puno većim sustavima, kao što su sustavi lanaca opskrbe, zdravstveni sustavi te brojni drugi koji svakodnevno obrađuju velike količine podataka.

Cijela priča *blockchaina* započela je 2009. godine kada je do danas nepoznati pojedinac, ili više njih, pod nadimkom Satoshi Nakamoto, svijetu predstavio Bitcoin, prvu kriptovalutu zasnovanu na *blockchain* tehnologiji. Ovaj „narodni heroj informacijskog doba“ (Kavanagh i Miscione, 2015) iskoristio je sve akumulirano znanje kriptografskog svijeta i pronašao način na koji mreža može funkcionirati bez središnjeg autoriteta, nešto o čemu su takozvani kripto-anarhisti sanjali od pojave Interneta. I ostalo je povijest, o kojoj će biti više rečeno u poglavljima koja slijede.

# 3. *BLOCKCHAIN* TEHNOLOGIJA

## 3.1 Bitcoin

O konceptu decentraliziranih valuta u računalnom se svijetu govori već desetljećima. Decentralizacija sredstva plaćanja za društvo bi značila odmak od kontrole središnjeg autoriteta, bilo u obliku financijske institucije ili u obliku države, te bi pojedincima donijela osjećaj veće slobode. Društvo kojemu je potrošnja jedan od glavnih oblika djelovanja, društvo 21. stoljeća, vjerojatno će težiti ostvarivanju što demokratičnijeg i pravednijeg sustava u koji mogu imati povjerenja. Unazad 30 godina društvo je na ovaj ili onaj način pokušavalo pronaći riješenje za ostvarivanje ideje otvorenog, uključivog i transparentnog sustava koji bi olakšao i

demokratizirao način na koji troši, a 2009. godine dogodila se prekretnica koja je uzdrmala kako financijski, tako i računalni svijet iz korijena. Kao što je ranije spomenuto, anonimni korisnik Satoshi Nakamoto svijetu je 2009. godine predstavio Bitcoin, prvu kriptovalutu temeljenu na *blockchainu*. Nešto što se činilo kao *silver bullet* za decentralizaciju monetarnog sustava, *blockchain* tehnologija, ubrzo je uzdrmala brojne druge sektore čiji je glavni kapital informacija (Ølnes et al., 2017), a euforija među programerima koji rade na razvoju ove tehnologije ne prestaje. No, kako je već napomenuto, razvoj *blockchain* tehnologije započeo je puno prije 2009. godine, a Satoshi Nakamoto donio je revoluciju tako što je posložio slagalicu koja je samo čekala da bude posložena.

### 3.1.1 Kratka povijest Bitcoina

Prva spominjanja decentraliziranih valuta sežu u osamdesete godine prošlog stoljeća. Tadašnji anonimni *e-cash* protokoli koristili su slijepi potpis[4] koji je omogućavao stvaranje valuta s visokom razinom privatnosti, ali nisu nikad privukle dovoljnu pažnju zbog oslanjanja na središnjeg posrednika. *Blockchain* tehnologija osmišljena je 1991. godine kada je objavljen znanstveni članak Stuarta Habera i W. Scotta Stornetta koji su rješenje pronašli u stavljanju vremenskih oznaka na podatke kako bi se sačuvali izvorni podaci, kao i vrijeme nastanka istih (Beyer, 2018). Osmislili su način na koji se grupe podataka smanjuju i šifriraju te nadovezuju na ostale grupe podataka. Prema njima, tako kriptirani podaci bi bili dostupni svima koji imaju ključ kojim mogu otvoriti i vidjeti izvorne podatke. Na sličan način funkcionira i današnja *blockchain* tehnologija. Također, njihovo rješenje uključivalo je i stvaranje decentraliziranih konsenzusa (Beyer, 2018). Radi se o načinu provjere vjerodostojnosti podataka koji ulaze u sustav koji se zasniva na zajedničkom radu svih uključenih u mrežu, umjesto na jednom središnjem autoritetu. Kako se stvaraju, bit će objašnjeno kasnije u radu.

Krajem 20. stoljeća, 1997. godine, Adam Back je predstavio *Hashcash*, koristeći shemu *proof-of-work* (dokaz rada) i tako uveo rudare (*miners)* u cijelu priču (Dannen, 2017), a upravo je ova tehnologija danas jedna od glavnih okosnica Bitcoina (Chohan, 2017). Sljedeće ime koje je pridonijelo razvoju tehnologije koja podržava kriptovalute je Wei Dai koji je 1998. dao prijedlog za *b-money*, valutu koja bi se mogla kovati i stvarati decentralizirane konsenzuse kroz

[4] U kriptografiji, slijepi potpis je vrsta digitalnog potpisa u kojemu je sadržaj poruke sakriven (zaslijepljen) prije nego što se potpiše.

rješavanje računalnih zadataka, ali detalji oko implementacije decentraliziranog konsensuza nikad nisu potpuno otkriveni i zbog toga ova tehnologija nije zaživjela. Zatim je 2005. godine Hal Finney predstavio koncept *reusable proof-of-work* (višekratnog dokaza rada), što bi bio sustav nastao na idejama *b-money* u kombinaciji s računalno zahtjevnim *Hashcash* zadatcima, a koji bi mogao stvoriti koncept kriptovaluta, ali ni tada nije pronađen način kako izbjeći kontrolu nekog središnjeg autoriteta (Buterin, 2013). Glavna mana svih prethodnih računalnih protokola bila je ta što su se njihovi kreatori najviše fokusirali na rješavanje takozvane Bizantske greške[5], čime su rješavali samo dio problema. Naime, ti protokoli su pretpostavljali međusobno povjerenje svih sudionika mreže te su stoga imali vrlo slabe zaštite od napada. Napadi, u tom smislu, bi se dogodili kada bi samo jedan korisnik mogao simulirati velik broj drugih korisnika i na taj način 'lažirati' konsenzus koji je, kako je već navedeno, ključan za rad kriptovalutnih sustava.

Već spomenuti Satoshi Nakamoto 2009. godine je na *mailing* listu stručnjaka koji su se bavili kriptografijom poslao članak pod nazivom „*Bitcoin: A Peer-to-Peer Electronic Cash System*“. U članku je predstavio sustav za elektronske transakcije koje se nisu morale oslanjati na međusobno povjerenje zainteresiranih strana (Chohan, 2017), nazvavši prvu kriptovalutu koja radi na ovaj način Bitcoin. Do danas nije sigurno tko je Satoshi Nakamoto budući da se nakon što je svoj rad predstavio ostalim stručnjacima kriptografije jednostavno povukao. Donio je inovaciju u rješavanju problema središnjeg autoriteta u online transakcijama tako što je povezao računalni protokol za decentralizirani konsenzus, koji je osnova za stvaranje *blockchaina*, s *proof-of-work* mehanizmom putem kojeg pojedinci uključeni na mrežu rade na održavanju iste te mreže. Svojim riješenjem Nakamoto je riješio problem duple naplate koja je mučila sve ranije izumitelje decentraliziranih valuta, uvevši *first-to-file* sustav, odnosno prihvaćanje one transakcije koja prva stigne (Buterin, 2013). Nakamoto je napravio prvi blok u *blockchainu* Bitcoina, tzv. *genesis block*, a prva osoba kojoj je prebacio bitcoine bio je sam Hal Finney na prvoj platformi za transakciju bitcoinom *Bitcoin-Client*, što je danas poznato kao prva Bitcoin transakcija u povijesti (Beyer, 2018).

U početnoj fazi Bitcoin sustava, mrežom su dominirali rudari koji su stvarali blokove i na taj način zarađivali bitcoine. Najčešći oblik komunikacije tada je bilo rudarenje, a nakon toga odmah i transakcije iz jednog novčanika u drugi. Vrijednost Bitcoina se po prvi puta

[5] Bizantska greška (*Byzantine fault*) je stanje računalnog sustava, ponajprije distribuiranog računalnog sustava, gdje neki dijelovi mogu biti krivi, ali je teško utvrditi je li nešto uistinu krivo zbog manjka povjerenja na mreži (wiki).

povezala s vrijednosti američkog dolara 2010. godine kada se na web stranici *New Liberty Standard* otvorila prva burza za razmjenu ove kriptovalute. Tada je jedan dolar vrijedio 1309,03 bitcoina, a taj iznos je dobiven izračunom potrošnje električne energije potrebne za izradu jednog bitcoina rudarenjem. Već nekoliko dana nakon toga, zbog tržišnih kretanja, cijena bitcoina je porasla 19 puta, a ubrzo su se počele otvarati i nove burze za razmjenu kriptovalutama (Woo, 2019). Jedna od tih burzi je Bitcoin Market, koji je i danas otvoren i dostupan za razmjenu, dok se New Liberty Standard zatvorio.

Prve kriptovalute nastale nakon Bitcoina su Litecoin i Namecoin, obje na istim principima i istom otvorenom kodu Bitcoina, ali s nekim izmjenama u kodiranju (Steadman, 2013). Danas[6] na cijelom tržištu kriptovaluta postoji preko dvije tisuće različitih kriptovaluta koje zajedno vrijede preko 250 milijardi američkih dolara. Što se tiče samog Bitcoina, trenutno je najvrijednija kriptovaluta - 1 bitcoin vrijedi 9609,53 američkih dolara[7], na tržištu je trenutno preko 17 milijuna iskovanih bitcoina, a trenutni broj blokova u njegovom *blockchainu* je prešao 592 tisuće[8].

### 3.1.2 Glavni koncepti Bitcoin sustava

U kratkom pregledu povijesti razvoja *blockchain* tehnologije i Bitcoina predstavljeno je nekoliko novih pojmova koje je potrebno dodatno razjasniti. Počevši od *blockchaina*, objasnit ću osnovne koncepte na kojima ova tehnologija počiva, kao što su rudari (*miners*), čvorišta (*nodes*), asimetrično šifriranje, procesi stvaranja decentraliziranog mrežnog konsenzusa (Champagne, 2014), a sve navedeno ću oprimjeriti kroz sustav Bitcoina te kasnije kroz sustav Ethereuma. Navedena dva sustava trenutno su dva najveća kriptosustava zasnovana na *blockchainu*, a svaki od njih donio je novinu koja je zadala novi smjer razvoju *blockchain* tehnologije.

*Blockchain* je računalna tehnologija za čuvanje računalnih podataka. To je način čuvanja podataka na distribuiranoj mreži, čime nestaje potreba za velikim centraliziranim serverima na kojima se spremaju podaci, budući da se podaci cijele ove mreže nalaze na različitim računalima korisnika diljem svijeta. *Blockchain* najjednostavnije možemo zamisliti kao knjigu u koju se upisuju podaci, koji se potom ne mogu više mijenjati i postaju javno dostupni (Champagne, 2014). Podaci su distribuirani na način da se kopija cijelog *blockchaina*

[6] Preuzeto s: https://coinmarketcap.com/all/views/all/ Učitano: 29. kolovoza 2019.

[7] Preuzeto s: https://coinmarketcap.com/all/views/all/ Učitano: 29. kolovoza 2019.

[8] Preuzeto s: https://www.bitcoinblockhalf.com/ Učitano: 29. kolovoza 2019.

nalazi na čvorištima koje pokreću pojedinci unutar mreže, a koji uz pomoć drugih korisnika, rudara, koji mogu i ne moraju imati vlastito čvorište, održavaju cijelu mrežu. Na taj je način cijeli sustav decentraliziran, jer ne uključuje posrednika ili središnji autoritet koji može svojatati te podatke. Informacije koje se unesu na *blockchain* dijele se sa svim ostalim uključenim korisnicima, zbog čega ovaj sustav možemo nazvati transparentnim. Dodatno, svi korisnici unutar mreže su anonimni, što cijelom sustavu daje sigurnost (Yli-Huumo et al., 2016). *Blockchain* je rastuća baza podataka, budući da sadrži sve podatke ikad upisane bez mogućnosti promjene istih, a istovremeno ti podaci su dostupni svima, zbog čega *blockchain* možemo nazvati i svojevrsnom javnom knjigom.

Bitcoin je bio prvi sustav koji je koristio *blockchain* tehnologiju, stvorivši temelje za razvoj decentraliziranih kriptovaluta (Yli-Huumo et al., 2016). Kako je riječ o kriptovalutnom sustavu, podaci koji se nalaze na *blockchainu* Bitcoina su podaci o provedenim transakcijama. Zbog toga se *blockchain* Bitcoina može promatrati kao knjiga platnog prometa, knjiga svih uplata i isplata ikad provedenih unutar ovog sustava (Champagne, 2014). Razvojem *blockchain* tehnologije osmišljeni su načini kako pohraniti podatke koji su puno veći i kompleksniji od samih transakcija, a veliku ulogu u tome odigrao je Ethereum, o čemu će kasnije biti više rečeno.

*Blockchain*, ili u slobodnom prijevodu lanac blokova, sastavljen je od puno manjih dijelova, koji se nazivaju blokovima. Te blokove možemo zamisliti kao stranice knjige na kojima se nalaze neki podaci. U slučaju Bitcoina, na tim se stranicama nalaze podaci o transakcijama. U *blockchainu* Bitcoin sustava nalaze se sve transakcije ikad napravljene u tom sustavu, otkad je predstavljen javnosti u siječnju 2009. Svi ti podaci su javno dostupni i svatko im može pristupiti (Champagne, 2014). Kako je riječ o decentraliziranom sustavu, znači da ne postoji središnji server na kojem se nalazi *blockchain* Bitcoina, već se taj *blockchain* nalazi na velikom broju čvorišta (*nodes)* unutar mreže. Sva ta čvorišta sadržavaju istu kopiju *blockchaina* i u međusobnom su dosluhu, što znači da kada se stvori novi blok ta informacija odlazi do svih čvorišta na mreži koji ažuriraju svoju kopiju *blockchaina*[9]. Blokove stvaraju rudari koristeći računalne funkcije pomoću kojih obrađuju podatke, a u suradnji s vlasnicima čvorišta vrše nadzor nad cijelim *blockchainom*[10].

[9] Preuzeto s: https://www.binance.vision/blockchain/what-are-nodes Učitano: 2. kolovoz 2019.
[10] Preuzeto s: https://lisk.io/academy/blockchain-basics/benefits-of-blockchain/what-is-decentralization Učitano: 2. kolovoza 2019.

Kako je već rečeno, *blockchain* Bitcoina sastoji se samo od informacija o provedenim transakcijama. Za bolje razumijevanje stvaranja pojedinih blokova, prvo ću objasniti kako se događaju transakcije unutar Bitcoin sustava. Za svaku transakciju u ovom sustavu potrebne su tri stvari: 1) Bitcoin adresa platitelja, na kojoj se nalaze resursi kojima će se izvršiti plaćanje; 2) Bitcoin adresa primatelja na koju će se prebaciti resursi nakon transakcije; 3) određeni broj bitcoina koji će se u transakciji prebaciti s jedne adrese na drugu. Dakle, za transakciju su potrebna dva zainteresirana korisnika i sredstva koja se prebacuju. Nema treće strane koja ima nadzor nad transakcijom i zbog toga se ovakva vrsta mreže naziva *peer-to-peer* mrežom, odnosno mrežom ravnopravnih računala (Champagne, 2014). Transakcije se odvijaju na posebnim burzama kriptovaluta, poput ranije spomenutog Bitcoin Marketa.

Da bi se transakcija uopće mogla provesti, platitelj treba imati dovoljno sredstava na svom računu, odnosno u svom novčaniku (*wallet*). Novčanik može otvoriti bilo tko na bilo kojoj od postojećih burzi za kriptovalute. Ima li platitelj dovoljno sredstava za transakciju nadgledaju i verificiraju rudari. Isto tako, bilo tko s pristupom nekoj od kriptovalutnih burzi može vidjeti koliko sredstava se nalazi u svakom pojedinom novčaniku. Iako je identitet svakog vlasnika novčanika sakriven, svatko tko ima pristup sustavu može vidjeti koliko sredstava se nalazi u pojedinom novčaniku (Champagne, 2014). Budući da je Bitcoin jedna od kriptovaluta, to znači da nikakav autoritet nema nadzor nad time niti je moguće otkriti sadržaj i vlasnika poruke, već je sigurnost korištenja kriptovalute zagarantirana tehnologijom (Narayanan et al., 2015). Zbog toga, svaka informacija, odnosno transakcija koja se događa unutar takvog sustava mora biti kriptirana, odnosno šifrirana.

Šifriranje je proces u kriptografiji u kojem se poruka koja želi biti odaslana „sakrije“ iza algoritamskog koda koji je poznat samo pošiljatelju i primatelju. Na ovaj je način omogućena komunikacija između dvije strane, a koja je zaštićena od nekoga trećega, odnosno onoga koji neku informaciju ne smije vidjeti (Ibrahimpašić, 2005). Tako se može slati tekst, numerički podaci ili, kao u slučaju Bitcoina, vršiti transakcija, a da nitko osim dvije zainteresirane strane ne zna koja je informacija poslana: „Pošiljatelj transformira otvoreni tekst, koristeći unaprijed dogovoreni ključ. (…) Nakon toga pošiljatelj šalje šifriranu poruku putem nekog komunikacijskog kanala. Protivnik prisluškujući dozna sadržaj šifrirane poruke, ali ne može odrediti otvoreni tekst i razumjeti poruku. Za razliku od njega, primatelj, koji zna ključ kojim je poruka šifrirana, može dešifrirati šifriranu poruku i odrediti otvoreni tekst“ (Ibrahimpašić, 2005:102).

S obzirom na tajnost ključa, mogu se razlikovati simetrični i asimetrični kriptosustavi. Simetrični kriptosustavi se još nazivaju i kriptosustavi s tajnim ključem. Kod tih kriptosustava ključ za dešifriranje se može izračunati ako poznajemo ključ za šifriranje. Najčešće su oba ključa identična, a sigurnost ovakvog kriptosustava leži u tajnosti ključa. Druga vrsta kriptosustava je asimetrični kriptosustav, a za prijenos neke informacije potrebna su dva ključa. Kod ovih kriptosustava ključ za dešifriranje neke poruke se ne može odrediti iz ključa za šifriranje. Ključ za šifriranje je javni ključ, odnosno, bilo tko može šifrirati poruku pomoću njega, ali samo osoba koja poznaje odgovarajući ključ za dešifriranje može dešifrirati poruku (Ibrahimpašić, 2005). Ključ za dešifriranje ovdje je tajni ključ.

Šifrirani ključevi koriste se za transakcije unutar Bitcoin sustava. Ključevi su kodovi sačinjeni od nizova brojki i slova koji sami po sebi ništa ne znače, a njih stvara algoritam, praveći razliku između javnih ključeva kojim se određena poruka šifrira i njima pripadajućih tajnih ključeva za dešifriranje iste poruke. No, prepoznati koji tajni ključ pripada kojem javnom ključu je računalno gotovo nemoguće, zbog čega javni ključ može ostati dostupan svima (Champagne, 2014).

Asimetrično šifriranje najlakše je za shvatiti na primjeru transakcije bitcoina. Recimo da korisnik A želi poslati određenu svotu bitcoina korisniku B. Oba korisnika imaju svoje javne i privatne ključeve, javni koji je dostupan svima i služi za šifriranje poruke namijenjenu isključivo njemu, i privatni koji služi za dešifriranje te iste poruke. Korisnik A pripremi svotu bitcoina koju želi poslati u novčanik korisnika B, a zatim tu poruku šifrira javnim ključem korisnika B. Nakon što korisnik B dobije obavijest da je primio transakciju, koristi svoj privatni ključ kako bi dešifrirao poruku i saznao informaciju koliko je bitcoina dobio od korisnika A. Nakon što korisnik A šifrira poruku javnim ključem korisnika B, više ne može vidjeti sadržaj te poruke, budući da do njega može doći jedino privatnim ključem korisnika B. Jedino korisnik B može vidjeti sadržaj poruke jer samo on zna svoj privatni ključ (Decuyper, 2017). Na ovaj način su transakcije unutar Bitcoin sustava osigurane od napada.

Nakon što se transakcija provede, informacija o provedenoj transakciji odlazi do svih rudara koji trenutno rade na stvaranju bloka. Nakon što se prikupi dovoljno podataka i ispune ostali uvjeti, koje ću podrobnije objasniti kasnije, rudari provjeravaju je li sve što se dogodilo na mreži validno te povezuju taj jedan blok na cijeli *blockchain* (Champagne, 2014). No najzanimljivija priča *blockchain* tehnologije tek slijedi, a u glavnim ulogama su rudari i čvorišta.

### 3.1.3 Uloga rudara i čvorišta

Kad bi Bitcoin sustav bio centralizirani sustav, za gore navedene transakcije bio bi odgovoran jedan autoritet, a *blockchain* Bitcoina bi se nalazio na jednom serveru. Budući da je Bitcoin sustav decentraliziran, priča je nešto drugačija i kompliciranija. Oni koji nadgledaju transakcije, stvaraju nove blokove i odgovorni su za sve što se događa na mreži su rudari (eng. *miners*) (Champagne, 2014) koji to rade pomoću čvorišta (eng. *nodes*). Rudari su pojedinci unutar *blockchain* sustava koji putem svojih računala, oslanjajući se na čvorišta, rade na održavanju istog. Najveći dio posla rudara odvija se kroz automatski rad računalnog koda, a pojedinac koji stoji iza toga osigurava da sve funkcionira. Bilo tko može postati rudarom, ako za to ima prikladnu hardversku opremu. Čvorišta su komunikacijska sjecišta unutar mreže na kojima pojedina informacija može biti napravljena i odaslana. Svaki uređaj spojen s Bitcoin sustavom može se promatrati kao čvorište ako se u obzir uzme da ono na neki način komunicira s ostalima na mreži. No, svako čvorište može imati različite funkcije pa prema tome postoji nekoliko različitih vrsta čvorišta[11], čiju ću raščlambu objasniti malo kasnije.

U počecima Bitcoin *blockchaina* za rudarenje je bilo dovoljno imati računalo s dobrom grafičkom karticom. Kako je vrijeme odmicalo, sve je više ljudi počelo rudariti, a kompleksnost samog rudarenja je porasla te se pojavila potreba za jačim procesorima koji iziskuju manje električne energije. Tada su rudari počeli koristiti programljive logičke sklopove, odnosno FPGA (eng. *field-programmable gate array*) uređaje koji su mogli brže doći do rješenja i biti učinkovitiji, a prelaskom na te komponente rudari su morali izdvojiti malo više novaca za svoju opremu. No, kako se tehnologija širila i postajala još kompleksnija, i ovi su uređaji postali preslabi te su se na tržištu pojavili novi uređaji, potpuno namijenjeni rudarenju, tzv. ASIC *(*eng. *Application – Specific Integrated Circuit*) uređaji (Matijević, 2018). Zbog tehnoloških mogućnosti ovih uređaja učinkovitost svih prethodnih je nadmašena, a od pojave prvih ASIC uređaja 2012. do danas se radi na njihovom konstantnom poboljšanju uz veliko tržišno natjecanje vodećih proizvođača.

Rudari u Bitcoin sustavu imaju nekoliko zadaća: 1) provjeravaju jesu li transakcije koje se dogode valjane, 2) prikupljaju podatke o provedenim transakcijama i slažu ih u blok, 3) provjeravaju rad ostalih rudara i 4) rješavaju matematičke zadatke kako bi baš njihov blok postao dio *blockchaina* (Champagne, 2014.) Način na koji oni rade upisan je u komunikacijski protokol kojeg je zadao Satoshi Nakamoto prilikom objave Bitcoin sustava. Isto tako, svaki

[11] Preuzeto s: https://www.binance.vision/blockchain/what-are-nodes Učitano: 2. kolovoza 2019

rudar ima barem dva razloga za to što radi, a u oba slučaja riječ je o svojevrsnim nagradama. Prvo, iz svake transakcije koja se dogodi odvaja se dio provizije za rudare, koju mogu pokupiti ako njihov blok postane dio *blockchaina*. Drugo, nakon što se baš njihov blok poveže s *blockchainom*, dobivaju *block reward*, svojevrsnu nagradu za svoj trud (Draupnir, 2016). Nagrada koju dobivaju ujedno je i jedini način na koji nastaju novi bitcoini, odnosno na taj način oni otkrivaju, to jest, kuju nove bitcoine. Način na koji se ti bitcoini dijele jedno je od središnjih pravila ove mreže i nemoguće ga je promijeniti, osim ako se svi sudionici mreže s time ne slože, što je gotovo nezamislivo.

Bitno je napomenuti kako je Nakamoto prilikom pokretanja Bitcoin sustava odredio konačni broj mogućih bitcoina koji će cirkulirati ovim sustavom na 21 milijun bitcoina (Draupnir, 2016). Nagrada za odrađen blok u početku je bila 50 bitcoina i toliko su rudari dobivali sve dok nisu riješili 210 000 blokova. Tada se nagrada prepolovila i iznosila je 25 bitcoina, koja je vrijedila za sljedećih 210 000 blokova. Nakon toga, nagrada se opet prepolovila. Kako se novi blokovi nadodaju na *blockchain* otprilike svakih 10 minuta, u jednom danu na *blockchain* se može dodati najviše 144 blokova. To znači da je ovim tempom, od 144 bloka dnevno, potrebno otprilike četiri godine kako bi se nagrada ponovno prepolovila (Draupnir, 2016). Od 2009., kada je cijeli sustav pokrenut, iskovano je preko 17,6 milijuna bitcoina, a trenutno nagrada za rudare iznosi 12.5 bitcoina (bitcoinblockhalf.com). Kako će se nagrada, ali i sami broj bitcoina koji će se kovati smanjivati, pretpostavlja se kako će 21 milijun bitcoina na ovoj mreži biti 2140. godine (Meiklejohn et al. 2013). Kako je sam Nakamoto napisao, trebalo je osmisliti način na koji će se bitcoini distribuirati, a konstantna brzina nastajanja novih bitcoina činila se kao najbolja formula (Draupnir, 2016).

Nadalje, kako je već navedeno, osnovni zadatak rudara jest traženje određenog rješenja. To je zapravo složena matematička operacija, a za rješavanje tog matematičkog problema potrebno je puno energije utrošene u rad računala koji radi na algoritmima. Ukoliko rudar koristi uređaje s većim kapacitetom energije za izvršavanje ovih složenih matematičkih operacija, utoliko će taj rudar biti uspješniji od drugih. Kada jedan rudar riješi problem, svi ostali rudari kreću u provjeru tog rješenja. Ako se više od 51% uključenih rudara složi da je rješenje valjano, blok se dodaje na *blockchain*, a svi rudari kreću u izgradnju novog bloka (Lantz, 2016). U tom se trenutku *blockchain* na svim čvorištima ažurira, a rudari od čvorišta preuzimaju sve prihvaćene transakcije koje su se dogodile od prethodnog bloka kako bi krenuli u izgradnju novog.

Zbog unaprijed dogovorenih pravila u opisanom komunikacijskom protokolu, moguća je suradnja svih rudara. Ako svaki rudar radi za istu nagradu, osigurano je da ostali rudari na mreži prihvaćaju rad samo jednog rudara. Isto tako, drugi rudari ne dobivaju ništa ako odbiju valjan blok te na takav način ne mogu osigurati da njihov blok bude odabran. Da rudari odbijaju sve blokove osim svojih, nikad ne bi bio moguć konsenzus, zbog čega se nikad ne bi mogao izgraditi *blockchain*, a sva vrijednost koja se nalazi u tom sustavu bi se uništila i niti jedan rudar nikada više ne bi mogao profitirati. Dakle, svi rudari mogu profitirati samo ako poštuju unaprijed određen protokol unutar Bitcoin sustava. Za razliku od rudara koji dobivaju nagradu za svoj rad, vlasnici čvorišta ne dobivaju ništa, osim ako istovremeno i oni nisu rudari. Čvorišta zapravo služe za održavanje ekosustava *blockchaina*, održavanje integriteta sustava, osiguravanje povjerenja, sigurnosti i privatnosti svih korisnika te štite *blockchain* od napada i prijevara[12].

Kako je ranije spomenuto, blok rudara koji prvi riješi kompleksni matematički problem, a koji je povezan s tim blokom, ulazi u *blockchain*. Taj proces selekcije rudara i bloka se naziva dokaz o radu (*proof-of-work*) jer podrazumijeva provjeru rada rudara na rješavanju zadatka. Kako bi taj proces postao jasniji, potrebno je objasniti kriptografski koncept koji se naziva *hash* funkcijom (Champagne, 2014). Kriptografski *hash* predstavlja kompleksni algoritam pomoću kojega se običan tekst transformira u niz brojeva i slova koji se čine slučajno poredani. Dobiveni rezultat ove funkcije, naziva se *hash* i predstavlja svojevrsni sažetak poruke te se to može smatrati digitalnim otiskom dokumenta. (Champagne, 2014) Tekst koji se transformira može biti bilo koje dužine, a *hash* koji se stvara od toga uvijek je iste dužine, odnosno, uvijek se sastoji od 64 znamenke.

*Hash* funkcija služi za transformaciju podataka iz jednog bloka u *hash*. Na taj način se dobiva kod od 64 znamenke u kojemu su spremljeni svi podaci iz željenog bloka. Na primjer, ako se jedan blok sastoji od jedne transakcije, ta transakcija će pomoću ovog algoritma dobiti novi oblik, odnosno dobit će svoj digitalni otisak (Jimi, 2018). Taj otisak služi za povezivanje tog bloka s drugim blokom koji dolazi nakon njega.

Kako je već ranije bilo spomenuto, ne može bilo koji blok biti odabran za nadovezivanje na već postojeći *blockchain*. Da se blok nadoveže na postojeći *blockchain*, rudari rješavaju matematičke zadatke. Ti matematički zadaci zapravo se sastoje od ispunjavanja određenih uvjeta koje mora imati *hash* svakog bloka kako bi se mogao povezati s prethodnim blokom.

[12] Preuzeto s: https://www.binance.vision/blockchain/what-are-nodes Učitano: 2. kolovoza 2019

Prema Bitcoin protokolu, blok će biti prihvaćen na *blockchain* ako njegov digitalni otisak, odnosno *hash*, počinje s određenim brojem nula[13]. Na primjer, samo blokovi čiji *hash* počinje s barem deset znamenki broja 0 mogu se nadovezati na blockchain. Svaki tekst, odnosno upis podataka transakcija koji čine jedan blok, ima svoj jedinstveni *hash*, a on ne mora, i najčešće niti neće, počinjati s točno određenim brojem nula. Stoga, kao takav ne može se nadovezati na *blockchain*. I tu dolazi uloga rudara.

Naime, rudari su ti koji u blok ubacuju neku informaciju sve dok ne 'pogode' koja točno informacija nakon *hash* funkcije ima digitalni otisak koji počinje s deset nula, i kao takav se može nadovezati na *blockchain*. Budući da svaki podatak o transakciji mora ostati nepromijenjen i točan, u blok se dodaje mali podatak koji nema nikakvu ulogu osim da mijenja digitalni otisak na kraju. Taj podatak se naziva *nonce* i predstavlja u potpunosti slučajan podatak koji može biti bilo koji znak, broj, veliko slovo ili čak i razmak (Jimi, 2018). Pojednostavljeno rečeno, blok se sastoji od: 1) informacija o transakcijama, 2) digitalnog otiska prethodnog bloka, 3) *nonce* podatka. Proces u kojem se neprestano mijenja taj *nonce* kako bi se dobio valjan digitalni potpis naziva se rudarenjem. Rudari, dakle, u blok podataka umeću neznačajni simbol, *nonce*, potom taj blok dobiva svoj *hash*, a kada taj *hash* odgovara prethodnom *hashu* u *blockchainu*, nadovezuje se na njega. Prije no što se blok s odgovarajućim *hashom* poveže na cijeli *blockchain*, odlazi na provjeru kod svih ostalih korisnika uključenih na mrežu, kod drugih rudara i na čvorišta, a nakon što oni dođu do konsenzusa da je cijeli proces točan, blok se pripaja *blockchainu*. Rudarenje nije ništa više nego pronalaženje točnog neznačajnog podatka koji može jedan blok spojiti na drugi, što cijeli ovaj proces čini svojevrsnom igrom na sreću. Najviše energije koju rudari troše odlazi upravo na pronalaženje pravog *nonce* podatka koji će u konačnici dati *hash* koji će omogućiti da se njihov blok poveže s *blockchainom* (Jimi, 2018).

Što se tiče vrsta čvorišta u Bitcoin sustavu, mogu se razlikovati tri vrste: 1) potpuno čvorište (eng. *full node*), 2) superčvorište (eng. *supernode*) i 3) lagano čvorište (eng. *lightwight*). Potpuna čvorišta u potpunosti podupiru Bitcoin sustav i jamči sigurnost te su stoga neophodna za funkcioniranje sustava. Ova čvorišta se uključuju u procese provjere valjanosti transakcija i blokova prema pravilima određenima protokolom. Potpuna čvorišta sadržavaju kopiju cijelog *blockchaina* i komuniciraju s ostalim sudionicima na mreži kada se dogodi promjena na *blockchainu*. S obzirom na to komuniciraju li s ostalim sudionicima na mreži, mogu biti javna

[13] Broj znamenki nula određuje razinu težine zadatka pronalaska rješenja. Što je više rudara spojeno na mrežu, odnosno što se više hash kodova izračunava, to će veći broj znamenki nula biti, tj., zadatak će biti teži. Sustav je Postavljen tako da se otprilike svakih 10 minuta novi blok nadoda na blockchain pa će shodno tome i broj znamenki nula biti veći ili manji (Champagne, 2014).

ili sakrivena. Javna čvorišta se nazivaju još i superčvorištima te su to čvorišta koja komuniciraju i prenose informacije s ostalim čvorištima na mreži koja se žele povezati s njime. Prema tome, superčvorište može služiti kao točka redistribucije informacija odnosno kao izvor podataka, ali i kao komunikacijski most između ostalih čvorišta i rudara na mreži. Lagano čvorište ili SPV klijent (*Simplified Payment Verification* klijent) je čvorište pomoću kojega korisnik na mreži može provjeriti u kojem bloku se nalazi koja transakcija, bez da mora skinuti cijeli *blockchain* na svoje računalo. Ovo čvorište ne sadrži kopiju *blockchaina* već se koristi superčvorištima za izvor informacija, a prema tome niti ne sudjeluje u održavanju mreže. Rudari mogu odlučiti žele li imati svoje čvorište s vlastitom kopijom *blockchaina* ili se udružiti s ostalim rudarima i koristiti jedno čvorište. Udruženjem više rudara nastaje rudarski bazen, koji ima svog administratora i vlasnik je čvorišta te jedini njime može upravljati[14].

### 3.1.4 Zašto Bitcoin sustav funkcionira?

Sada kada je jasno na koji način se blokovi vežu jedan s drugim na primjeru Bitcoina, valja pojasniti zašto točno ovaj sustav funkcionira. Nekoliko je glavnih činjenica koje se ovdje trebaju naglasiti:

1. Bitcoin sustav je softver otvorenog koda;

2. Bitcoin softver je utemeljen na unaprijed određenim uputama za rad;

3. Bitcoin softver je definiran i radi na utemeljenom komunikacijskom protokolu;

4. Dijeljenje distribuiranih datoteka unutar *blockchaina* omogućava otvoreno knjigovodstvo. (Champagne, 2014)

Softver otvorenog koda je računalni softver čiji je izvorni kod dostupan svima. Izvorni kod čine naredbe, upute, funkcije i ostalo, napisano programskim jezikom, zbog čega softver može nesmetano raditi. Izvorni kod Bitcoin softvera je otvoren za sve, što čini ovaj softver transparentnim. Osim toga, programiran je na način svima dostupan za modificiranje i korištenje (Champagne, 2014). Zbog toga je moguće jednostavno kopirati taj kod i napraviti novi, prilagođeni softver, što se očituje u brojnim 'imitacijama' Bitcoina, odnosno u drugim kriptovalutama koje funkcioniraju na sličan način.

Nadalje, unaprijed određene upute, odnosno komunikacijski protokol, kojeg moraju pratiti svi rudari i svi koji imaju novčanik unutar sustava, omogućava njegov rad. Svaki rudar

[14] Preuzeto s: https://www.binance.vision/blockchain/what-are-nodes Učitano: 2. kolovoza 2019

točno zna na koji način može rudariti, a isto tako svatko tko želi napraviti transakciju ima određeni broj koraka koje mora ispuniti. Kada bi netko od korisnika unutar ovog sustava prekršio pravilo, rudari bi ga jednostavno diskvalificirali (Champagne, 2014). Protokol je sustav pravila koji opisuje kako se računalo (i programer koji ga koristi) povezuje, sudjeluje u mreži te prenosi informacije preko mreže. Ta pravila definiraju sintaksu i semantiku koda koji pokreće sustav. Protokoli mogu sadržavati hardver, softver i pravila napisana na običnom jeziku (Dannen, 2017). Otvoreno knjigovodstvo označava činjenicu da bilo tko tko se nalazi unutar sustava ima pristup *blockchainu* i može se uvjeriti kako je sastavljen prema određenim pravilima.

## 3.2 Ethereum

*Blockchain* revolucija koju je pokrenuo Satoshi Nakamoto dobila je novu etapu kada je programer Vitalik Buterin zajedno sa suradnicima osmislio Ethereum. To je platforma otvorenog koda utemeljena na *blockchainu*, a koja omogućava izgradnju drugih decentraliziranih projekata bez izgradnje vlastitog *blockchaina* (Thornburg, 2018). Ideja iza Ethereuma je omogućiti i pojednostaviti korištenje sustava *blockchaina* za bilo koga tko želi raditi u decentraliziranom sustavu. Dok je *blockchain* Bitcoina dizajniran samo za razmjenu kriptovaluta, Ethereum koristi isti princip rada, samo ga podiže na novu razinu tako što omogućava pisanje takozvanih pametnih ugovora (eng. *smart contracts*). To je računalni protokol kojim dvije zainteresirane strane mogu sklopiti ugovor koji odmah dobiva svoj digitalni otisak u obliku koda (Frankenfield, 2019). Koristeći računalne kodove, ovi pametni ugovori automatski izvršavaju naredbe kada se dosegnu unaprijed određeni uvjeti. Umjesto da odluku o nekom izvršenom radu i naknadi za to donosi neki središnji autoritet, pametni ugovori provjeravaju i prihvaćaju, odnosno odbijaju izvršeno. To je moguće jer su uvjeti za ispunjavanje određenog 'zadatka' unaprijed zadani i dvije zainteresirane strane koje ga koriste ne moraju imati povjerenja jedno u drugo, već samo u tehnologiju (Thornburg, 2018). Na primjer, pametni ugovor može dati naredbu „Plati Ivanu 10 dolara ako do 15. rujna 2019. preda članak od 1000 riječi na temu stočarstva“, i Ivan će stvarno dobiti 10 dolara kada se ti uvjeti ispune.

Slično kao i Bitcoin, Ethereum radi na *blockchain* mreži u kojoj sudjeluju ravnopravni i raspršeni korisnici. I Bitcoin i Ethereum mreže imaju svoje kriptovalute s kojima se može odvijati razmjena, ali postoje neke ključne razlike između ove dvije mreže. Prvo, Bitcoin koristi *blockchain* kako bi vodio evidenciju vlasništva vlastite digitalne valute, odnosno, kako je već spomenuto, to je otvorena i javno dostupna knjiga platnog prometa. Time je Bitcoin ograničen

na razmjenu valuta, odnosno to je elektronski kriptovalutni sustav ravnopravnih korisnika. Ethereum svoj *blockchain* koristi za pokretanje programskog koda aplikacija (Modi, 2018). To je decentralizirana mreža pomoću koje se mogu graditi druge decentralizirane aplikacije, a koje sve koriste jedan zajednički Ethereum *blockchain*.

Bitcoin je nastao kako bi smanjio dominaciju PayPala i Internet bankarstva kao središnjih autoriteta u novčanim transakcijama, a Ethereum ima za cilj zamijeniti središnje autoritete Interneta, tj. one koji čuvaju naše podatke ili prate naša ponašanja. Može se reći kako Ethereum planira postati 'Svjetskim računalom' koje bi decentraliziralo i demokratiziralo postojeći klijent-server model. Uz Ethereum, serveri i virtualni oblaci su zamijenjeni tisućama komunikacijskih čvorišta iza kojih stoje rudari koji održavaju tu mrežu[15]. Vizija koja stoji iza Ethereuma je pružiti svima na svijetu priliku stvoriti platformu na kojoj će davati neku vrstu usluga koristeći *blockchain*. Također, ideja je oduzeti kontrolu trećih strana (Google, Facebook i sl.) nad informacijama koje prikupljaju od korisnika i vratiti tu kontrolu u ruke vlasnika tih informacija[16]. Time bi se sačuvali i osobni podaci i autorska prava korisnika.

Iako nitko ne posjeduje Ethereum, korištenje nije besplatno. Naime, kako bi mreža mogla raditi potreban je ether, jedinstveni kod koji se može koristiti za plaćanje računalnih resursa potrebnih za rad aplikacije ili programa. Slično kao i bitcoin, ether je digitalni nositelj vrijednosti, decentralizirana kriptovaluta koja se ne oslanja na središnji autoritet u transakcijama[17]. Na primjer, recimo da neka glazbenica odluči napraviti aplikaciju za distribuciju svoje glazbe. Na taj način ona ne mora potpisati ugovor s nikakvom tvrtkom, ne mora računati na slabe isplate putem YouTubea i time štiti svoja autorska prava. Na toj aplikaciji ona napravi svoju glazbu dostupnom, a može postaviti i nekoliko različitih kategorija putem kojih korisnici aplikacije mogu doći do njezine glazbe: samo za slušanje putem aplikacije, za *downloadanje*, za kupnju autorskih prava za korištenje u komercijalne svrhe itd. Korištenje svake pojedine stavke, odnosno kategorije, koštat će određen broj ethera. Korisnik koji, na primjer, želi skinuti jednu njezinu pjesmu na svoj mobitel, uplatit će svotu ethera na njen račun. Nakon što to napravi, pokrenut će se proces skidanja. S druge strane, ti etheri otići će u novčanik glazbenice i to će biti njezina zarada za glazbu koju je napravila. Ona nikome neće morati platiti udio zato što ima svoju aplikaciju ili zato što prodaje svoju glazbu. Sva zarada od glazbe, od njezinog autorstva odlazi direktno njoj (Tapscott, 2016).

---

[15] Preuzeto s: https://www.coindesk.com/information/what-is-ethereum Učitano: 6. lipnja 2019
[16] Preuzeto s: https://www.coindesk.com/information/what-is-ethereum. Učitano: 6. lipnja 2019
[17] Preuzeto s: https://www.coindesk.com/information/what-is-ether-ethereum-cryptocurrency. Učitano: 6. lipnja 2019

Nadalje, ether nazivaju i 'digitalnim plinom', a prateći tu analogiju, može se reći da se transakcijske naknade u etherima računaju s obzirom na to koliko se 'plina' mora emitirati da bi se neka radnja unutar aplikacije dogodila. Svaka radnja košta onoliko 'plina' koliko je potrebno računalne energije za izvršenje te radnje[18].

Struktura *blockchaina* Ethereuma slična je onoj Bitcoina u smislu da je to otvorena i javno dostupna knjiga svih podataka u nju ikad upisanih. Kao i kod Bitcoina, svako čvorište na Ethereum mreži sadrži kopiju cijele povijesti ovog *blockchaina*. Razlika između Ethereum i Bitcoin *blockchaina* leži u tome da čvorišta u *blockchainu* Ethereuma 'skladište' trenutno stanje svakog pametnog ugovora, ali i bilježe sve transakcije koje se događaju s etherima. Ethereum mreža, preko čvorišta i rudara, mora pratiti stanje svega što se u svakom trenutku događa sa svakom pojedinom aplikacijom, pratiti informacije svih tih aplikacija, uključujući i količinu valuta koje imaju, pratiti sve kodove pametnih ugovora i gdje su spremljeni[19].

Sukladno tome, vrijeme stvaranja blokova i pripajanja *blockchainu* kod Ethereuma je znatno manje nego kod Bitcoina te je potrebno otprilike 13[20] sekundi da rudar sakupi podatke, dođe do pravog hasha i stavi blok na *blockchain*. Za razliku od Bitcoina, nije određen konačan broj ethera koji će se iskovati, a trenutno na mreži postoji preko 107 milijuna ethera[21]. Sam *blockchain* sadrži preko 8,2 milijuna blokova, dnevno se na mreži dogodi preko milijun transakcija, a broj čvorišta koji održavaju mrežu trenutno je 8566[22].

## 3.3 Distribuirani konsenzus

Jedna je od većih razlika između Bitcoina i Ethereuma u načinu na koji dolazi do konsenzusa u procesu selekcije rudara i bloka koji će biti povezan na *blockchain*. Kako smo već objasnili, Bitcoin sustav koristi dokaz o radu (*proof-of-work)* u kojemu blok onog rudara koji prvi pronađe odgovarajući *hash* odlazi na provjeru kod ostalih rudara te nakon postignutog konsenzusa da je sve napravljeno prema pravilima bude prihvaćen i povezan na *blockchain*. Ethereum je započeo s takvim sustavom provjere, ali se s vremenom počeo djelomično prebacivati na drugačiji način provjere i stvaranja konsenzusa s ciljem da u konačnici u potpunosti prijeđe na njega. Riječ je o procesu koji se naziva dokaz o udjelu (*proof-of-stake).*

[18] Preuzeto s: https://www.coindesk.com/information/what-is-ether-ethereum-cryptocurrency. Učitano: 6. lipnja 2019
[19] Preuzeto s: https://www.coindesk.com/information/how-ethereum-works. Učitano: 6. lipnja 2019
[20] Preuzeto s: https://ethstats.net/ Učitano: 29. kolovoza 2019.
[21] Preuzeto s: https://bitinfocharts.com/ Učitano: 29. kolovoza 2019.
[22] Preuzeto s: https://www.ethernodes.org/network/1 Učitano: 29. kolovoza 2019.

U takvom sustavu, kreator novog bloka odabire se nasumičnim odabirom, ali vodeći se kriterijem udjela, odnosno koliko pojedini rudar ima kriptovaluta u svom vlasništvu ili koliko dugo drži tu kriptovalutu. Umjesto računalne snage, koja igra glavnu ulogu u procesu dokaza o radu, vjerojatnost da će neki rudar biti odabran za stvaranje bloka proporcionalno je povezana s udjelom kriptovaluta koje taj rudar posjeduje. Na primjer, ako jedan od rudara u sustavu neke kriptovalute drži 20% od sveukupne količine te kriptovalute u sustavu, on će imati 20% vjerojatnosti da bude odabran za stvaranje bloka. Isto vrijedi i za one od 10% ili 40%. Premda postoji određeni kriterij, kao što je veličina udjela u nekoj kriptovaluti, odabir onoga tko će napraviti novi blok je slučajan. Na taj način sustav je siguran od centralizacije, jer ako toga ne bi bilo, najbogatiji pojedinac unutar mreže bi mogao uspostaviti monopol[23]. Najveća prednost ovakvog načina odabira rudara je što je potrošnja energije za rudarenje uvelike smanjena, čime ono postaje puno više isplativije. Budući da je tome tako, smanjuje se i potreba za stvaranjem novih kriptovaluta kako bi se potaknulo rudare da održavaju mrežu. Kako je ranije spomenuto, Ethereum nije u potpunosti prešao na ovaj način provjere blokova, nego je najavljeno da će to napraviti početkom 2020. Za sad, još uvijek se dijelom oslanja na *proof-of-work* proces stvaranja konsenzusa (Williams, 2019).

Osim navedena dva načina stvaranja konsenzusa, *proof-of-work* te *proof-of-stake*, 2014. osmišljen je i novi, puno demokratičniji način provjere blokova i stvaranja konsenzusa, a on se naziva *delegated-proof-of-stake*, u slobodnom prijevodu delegirani dokaz o udjelu. To je konsenzusni algoritam koji može dovesti do nepobitnog sporazuma unutar mreže i potvrđivati transakcije, istovremeno tvoreći digitalnu demokraciju. *Delegated-proof-of-stake* koristi kombinaciju glasovanja u stvarnom vremenu i društveni sustav reputacije kako bi se postigao konsenzus. Pretpostavlja se da je to najmanje centraliziran način stvaranja konsenzusa na mreži jer uključuje najviše korisnika. Delegati su pojedinci unutar sustava, rudari i vlasnici čvorišta koji održavaju cijeli sustav[24]. Te delegate odabiru drugi korisnici (eng. *stake-holders*), koji imaju udio u određenoj kriptovaluti, a njihova glasačka vrijednost je određena količinom udjela koje drže u sustavu te kriptovalute. Važno je da odabrani delegati rade za najbolji interes cijele mreže jer upravo o njima ovisi brzina i sigurnost cijelog sustava. Delegati prikupljaju glasove na temelju reputacije koju imaju u mreži, a koju najčešće stvaraju tako da dobro rade svoj posao. Glasači, *stake-holderi* to prepoznaju i daju svoj glas onome koga smatraju najboljim. Delegati

[23] Preuzeto s: https://lisk.io/academy/blockchain-basics/how-does-blockchain-work/proof-of-stake. Učitano: 6. lipnja 2019
[24] Preuzeto s: https://lisk.io/academy/blockchain-basics/how-does-blockchain-work/delegated-proof-of-stake. Učitano: 7. lipnja 2019

nakon što odrade svoj posao i stvore blok koji se poveže na *blockchain* dobivaju nagradu, odnosno *block reward*, koji je određen protokolom tog određenog sustava kriptovaluta[25].

Delegati samo prikupljaju podatke koji se razmjenjuju na mreži i nemaju moć ih mijenjati ili na bilo koji način utjecati na izmjenu sadržaja istih. No, ono što mogu napraviti jest isključiti određenu transakciju, tj. ne staviti u blok koji će se povezati na *blockchain*, čime samo produžuju vrijeme transakcije jer prvi sljedeći delegat može uzeti tu informaciju i pohraniti ju na *blockchain*. No, prvome delegatu se to ni ne isplati jer time samo narušava svoju reputaciju, što mu ne donosi ništa dobro. Ovo je samo jedan mali primjer načina na koji funkcionira sustav decentralizacije, kada svi uključeni u mrežu imaju utjecaj i brinu o najvećem interesu mreže i svih ostalih uključenih (lisk.io). Najveća kriptovaluta koja trenutno koristi ovaj način stvaranja konsenzusa je EOS[26].

## 3.4 Vrste *blockchaina*

Premda su i Bitcoin i Ethereum zamišljeni kao decentralizirani sustavi s transparentnim i javno dostupnim podacima, nisu svi sustavi koji se zasnivaju na *blockchainu* takvi. Naime, razvojem ove tehnologije došlo se do dva dihotomna svojstva *blockchaina* – javni i privatni te otvoreni (bez dopuštenja) i zatvoreni (s dopuštenjem). U tablici 1. prikazana su svojstva *blockchaina* prema razinama otvorenosti i dopuštenju pristupa.

[25] Preuzeto s: https://lisk.io/academy/blockchain-basics/how-does-blockchain-work/delegated-proof-of-stake. Učitano: 7. lipnja 2019

[26] Preuzeto s: https://cryptoslate.com/cryptos/dpos/ Učitano: 3. kolovoza 2019.

| | Otvoreni (bez dopuštenja) | Zatvoreni (s dopuštenjem) |
|---|---|---|
| Javni | Nema zabrane pristupa, unosa podataka, vršenja transakcija ili rudarenja. | Nema zabrane pristupa ili unosa podataka i vršenja transakcija, ali samo oni s dopuštenjem mogu rudariti i održavati mrežu. |
| Privatni | Samo oni s dopuštenjem mogu pristupiti podacima i vršiti transakcije, ali ne postoji zabrana u sudjelovanju na održavanju mreže i rudarenju. | Zabranjen pristup podacima, unosu podataka, vršenju transakcija i održavanju mreže. Samo oni s dopuštenjem mogu sudjelovati. |

Tablica 1. (Ølnes et al., 2017)

Svojstvo javnog ili privatnog *blockchaina* određuje tko ima pristup bazi podataka na *blockchainu*, a svojstvo otvorenog i zatvorenog određuje tko ima dopuštenje da unosi podatke u *blockchain*. Kod javnog *blockchaina* svatko može vidjeti koji se podaci nalaze na *blockchainu* te mogu sudjelovati u transakcijama, stvarati pametne ugovore ili koristiti takve aplikacije, čime su i svi korisnici anonimni, dok kod privatnog, vlasnik *blockchaina* određuje koji korisnik to sve može raditi, čime je i upoznat s podacima tog korisnika. S druge strane, kod otvorenog *blockchaina* svatko može postati rudar, stvarati blokove ili imati vlastito čvorište sa cijelim *blockchainom*, dok je kod zatvorenog to omogućeno samo za one koji imaju dopuštenje vlasnika *blockchaina* (Ølnes et al., 2017). U tom smislu javni i otvoreni *blockchain* nema vlasnika koji ima kontrolu nad podacima, dok je u bilo kojoj drugoj kombinaciji ovih svojstava vlasnik *blockchaina* taj koji ima autoritet.

Prateći tu analogiju, podaci otvorenog *blockchaina* distribuirani su diljem cijele mreže, dok su kod zatvorenog centralizirani i nalaze se tamo gdje ih vlasnik *blokchaina* postavi. Kod otvorenog *blockchaina* ne postoji problem povjerenja, jer su svi uključeni u mrežu jednakopravni entiteti, dok kod zatvorenog mora postojati povjerenje u središnji autoritet. Zbog toga, kapacitet i brzina protoka informacija je kod otvorenog *blockchaina* ipak niža od one kod zatvorenog, a budući da samo kod otvorenog postoje anonimni dobrovoljci koji rudare i održavaju mrežu, jedino kod otvorenog postoji i proizvod njihovog rada, odnosno kriptovaluta. U zatvorenom *blockchainu* nema potrebe za time budući da se *blockchain* koristi za neke druge svrhe, a rudari su odobreni od strane autoriteta (Ølnes et al., 2017).

Za razliku od Bitcoina i Ethereuma, decentraliziranih i otvorenih sustava koji koriste *blockchain* tehnologiju upravo zbog svojstava decentralizacije i odsustva autoriteta, danas postoje centralizirani sustavi koji rade na *blockchain* tehnologiji, kao što su HyperLedger i Corda, koji koriste, primjerice, svojstva sigurnosti podataka i brzine unosa podataka ali ostaju centralizirani jer žele točno znati što se događa s njihovim podacima. To su uglavnom privatne tvrtke koje koriste *blockchain* za poboljšanje svojeg poslovanja jer mogu određivati tko ima pristup podacima i tko može unositi podatke te na taj način osigurati podatke bitne za poslovanje (Massesi, 2018).

Kao tehnologija koja omogućava distribuiranu, šifriranu, kronološki složenu i neizmjenjivu bazu podataka, tehnologija koja funkcionira na konsenzusu svih uključenih u mrežu te, naposljetku, tehnologija koja omogućava izravnu interakciju između dva korisnika, *blockchain* se pokazao primjenjivim u različitim sustavima. Budući da je glavna svrha ove tehnologije prikupljanje i čuvanje podataka, svoju primjenu je najprije pronašla u okolinama u kojima se prikupljaju, obrađuju i međusobno izmjenjuju različite vrste informacija, kao što su financijski sustavi, zdravstvo, upravni sustavi, osiguranje, Internet stvari *(Internet of Things)*, organizacijski i savjetodavni sustavi. Pokazalo se kako upravo takve okoline, koje se oslanjaju na vrijednosti kao što su povjerenje, običaji i kultura, a koje su institucionalizirane kroz zakonske ili institucionalne okvire te tradiciju, mogu imati najviše koristi od *blockchain* tehnologije. Sve navedeno može se svesti pod okoline s visoko institucionaliziranim vrijednostima (Meijer, 2017), a svim tim sustavima *blockchain* tehnologija može pružiti transparentnost, povjerenje, brzinu, otvorenost i laku dostupnost, vrijednosti sustava koje su iznimno bitne za krajnje korisnike.

## 3.5 Problemi *blockchain* tehnologije

Premda se čini kako *blockchain* tehnologija ima potencijala zauvijek promijeniti neke sfere ljudskog djelovanja, ipak postoje određeni problemi s kojima su se sustavi na *blockchain* tehnologiji susreli, a koji su postali glavni primjeri slabosti ove tehnologije.

Jedan od njih je potrošnja energije potrebne za pokretanje računala i čvorišta koji rade na održavanju *blockchaina*. Prema nekim podacima jedna Bitcoin transakcija košta 6$ kada se preračuna energija koja je potrebna za rudarenje i rad čvorišta (Gatteschi et al., 2018). Osim toga, ako se konsenzusi unutar mreže vrše prema principu dokaza o radu (eng. proof-of-work) jako puno te energije je uzalud potrošeno jer se priznaje rad samo jednog rudara. Isto tako, oprema za rudarenje i održavanje čvorišta je za sad još uvijek prilično skupa te bi za

prebacivanje nekog sustava na *blockchain* trebala velika ulaganja. Sukladno problemu velike potrošnje električne energije, postoji i problem emisija štetnih plinova zbog načina na koji rudari dolaze do energije. Trenutno je Kina vodeća u broju farmi za rudarenje kriptovaluta, a većinom te farme rade na energiji dobivenoj iz ugljena[27]. S obzirom na otisak koje rudarenje ima, potrebno je prebaciti se na održive izvore energije ukoliko se ova tehnologija implementira u veće sustave.

Drugi problem *blockchain* tehnologije uključuje ljudski faktor, a tiče se sklapanja pametnih ugovora i njihove realizacije u stvarnosti (Stinchcombe, 2018). Teoretski gledano, ako netko kupi kuću preko pametnog ugovora, jednom kada sustav uspostavi da su dosegnuti zadani uvjeti i vlasništvo prebaci s prodavatelja na kupca, nitko ne garantira kupcu da će zaista dobiti kuću. U dosadašnjem sustavu za vjerodostojnost takvih ugovora brinuo se posrednik, odnosno institucije koje su postavljale uvjete za mogućnost takve transakcije, no u *blockchain* sustavu to bi trebao raditi jednostavan softver? Računalo kao takvo ne može vidjeti je li prodavatelj zaista dao ključeve od kuće kupcu ili nije. To dovodi do zaključka da u ovakvim situacijama ipak nedostaje ljudski posrednik.

Treći problem *blockchain* tehnologije su hakerski napadi. Razvojem *blockchaina* pronašlo se rješenje za najčešći oblik napada, distribuirani napad uskraćivanjem resursa (eng. distributed denial-of-service attack, DDoS), i to kroz stvaranje distribuiranih konsenzusa s barem 51% složnih rudara. Da bi se uopće novi podaci unijeli na *blockchain,* barem 51% od svih uključenih rudara moraju verificirati da je blok valjan, kao i da je valjan njemu pripadajući *hash* (Buterin, 2013). Svaki rudar je vezan uz svoj uređaj za rudarenje, stoga je nemoguće da jedan rudar simulira milijune drugih kako bi izvršio napad, što je slučaj u gore navedenom tipu hakerskog napada. No, iako se isprva činio nemogućim, pronađeni su načini kako da se hakiraju *blockchain* sustavi. Jedan od njih je takozvani „51% napad“ (Orcutt, 2019) u kojemu je potrebno upravljati s više od 51% rudarskih uređaja kako bi se izmjene na *blockchainu* mogle verificirati prije nego što ostali rudari primijete da se nešto događa. Iako se to nije dogodilo samo jednom, na taj način napadnut je i Ethereum[28] kada je iz različitih novčanika izvučeno kriptovalute ethera u vrijednosti od preko 1,1 milijuna dolara. Sve učestaliji napadi unazad nekoliko godina postali su ozbiljan problem za vjerodostojnost *blockchain* tehnologije te postaju zaprjeka za daljnje širenje i stvaranje novih korisnika.

[27] Preuzeto s: https://digiconomist.net/bitcoin-energy-consumption. Učitano: 13. kolovoza 2019
[28] Preuzeto s: https://www.technologyreview.com/f/612728/hackers-just-stole-1-million-from-the-ethereum-classic-blockchain-in-a-rare-51/ Učitano: 31. kolovoza 2019.

Sukladno s time, kritičari *blockchain* tehnologije ističu i problem povjerenja, koje je od samih početaka bila glavna označnica ove tehnološke revolucije. Sama ideja *blockchaina* je odmicanje od središnjeg autoriteta i stvaranje mreže jednakih korisnika, gdje ne treba postojati međusobno povjerenje dvaju korisnika jer je ono zagarantirano tehnologijom. Ono što se dogodilo jest da se povjerenje u ljude i institucije prebacilo na tehnologiju, kriptografiju, protokole, softvere itd., i to je predstavljeno na apsolutan način jer računalo gotovo ne može pogriješiti (Schneier, 2019). Tako su korisnici na neki način primorani imati povjerenje u nešto što ne razumiju do kraja. Pojavom problema kao što su hakerski napadi za očekivati je da će se povjerenje u tehnologiju uzdrmati, a nemogućnost *blockchain* tehnologije da reagira na njih kao što reagiraju drugi sustavi koje poznajemo, samo još više može produbiti to nepovjerenje.

No, jednako kao što su se dosadašnji sustavi suočavali, i još uvijek se suočavaju s napadima različitih vrsta, za očekivati je da će i ova nova tehnologija, odnosno ljudi koji je razvijaju, pronaći načine na koje će se suočavati s napadima i ostalim problemima s kojima će se suočavati (Morris, 2019). Svakako treba imati na umu da gore navedeni primjer napada se može dogoditi samo na otvorenom *blockchainu*, kao što je Bitcoin ili Ethereum, dok su zatvoreni u tom smislu sigurniji zbog same naravi sustava. Takvi sustavi zapravo funkcioniraju kao mreža za sebe, budući da ih mogu održavati samo oni s dozvolom autoriteta i da se nalazi samo na provjerenim računalima. Iako su prepoznati određeni problemi, za očekivati je da će se razvojem i širenjem mogućnosti ove tehnologije pojavljivati i mnogi drugi te svakako na *blockchain* ne treba gledati kao na tehnologiju bez rizika. Tu se može postaviti pitanje je li se ijedna postojeća tehnologija pojavila bez rizika? I koliko rizika je „previše rizika“?

# 4. BIROKRACIJA

Na *blockchain* se može kao na tehnologiju iznimnih organizacijskih mogućnosti, zbog čega je usporediv s birokracijom (Kavanagh i Miscione, 2015). Jedan od temeljnih pojmova klasične sociologije pojavom *blockchaina* ima priliku ponovno biti u centru rasprave, a poteškoće i problemi na koje je birokracija nailazila kroz svoju povijest možda napokon dobiju rješenje.

Za Webera je birokracija bila najbolje i neizbježno rješenje u kontekstu racionalnog upravljanja velikim sustavima kao što je bila moderna država. Racionalnost i objektivnost kao dvije od odrednica novog doba ogledale su se u organizaciji velikog broja informacija kroz suradnju velikog broja pojedinaca. Prema Weberu, sastavni dijelovi birokracije su zakoni i pravila te njima određene i standardizirane procedure koje provodi velik broj ljudi uključenih

u tzv. birokratski aparat. Takva 'mašina' bila je tehnički nadmoćna nad svim drugim oblicima organizacije. „Potpuno razvijen birokratski mehanizam odnosi se prema drugim oblicima organizacije isto kao mašina prema nemašinskim oblicima proizvodnje. Točnost, brzina, nedvosmislenost, poznavanje dokumenata, trajnost, uviđavnost, jedinstvo, stroga podčinjenost, ušteda na materijalnim i osobnim rashodima – sve to je podignuto na najviši mogući stupanj u strogo birokratskoj upravi“ (Weber, 1922 u Đurić, 1987: 394). Mašinu koju Weber prepoznaje danas je moguće razumjeti kao računalo gdje je hardver velik broj ureda, softver unaprijed određena i depersonalizirana pravila i procedure, a birokrati su operacijski sustav zbog kojih se to računalo može pokrenuti. Prateći pravila, oni prikupljaju i obrađuju informacije te donose odluke, a sve kako bi se stvorio most između vladajućeg tijela i građana (Kavanagh i Miscione, 2015), odnosno kako bi svakom građaninu bio osiguran pristup samoj državi.

Kako bi to 'društveno računalo' radilo bez greške, moralo je počivati na određenim principima:
1) postojanje službi i kompetencija koje su strogo definirane pravilima ili zakonima; 2) hijerarhija funkcija; 3) odvojenost između funkcije i čovjeka koji je obavlja; 4) regrutiranje službenika plaćom koju propisuje država (Đurić, 1987). Weber govori kako iza svakog akta istinske birokratske uprave stoji sustav razloga o kojima se racionalno može raspravljati i to ili podvođenjem pod više norme ili odmjeravanjem ciljeva i sredstava. Hijerarhija funkcija podrazumijeva podjelu i specijalizaciju rada unutar birokratskog sustava, gdje onda možemo razlikovati npr. uloge ravnatelja institucija, voditelja ureda, pa sve do pojedinaca zaposlenih na šalteru koji imaju izravan odnos sa zainteresiranim građanima. No, Weber prepoznaje i drugačiji hijerarhijski odnos unutar ovoga, a tiče se nadmoći stručnjaka. Bez obzira tko se nalazi na čelu birokratskog sustava, narod koji izabire službenike, parlament ili predsjednik, prema školovanom i profesionalnom službeniku taj vlastodržac se uvijek nalazi u položaju diletanta prema stručnjaku. Ova nadmoć stručnjaka za svaku birokraciju znači granicu koja se uvijek može dalje pomaknuti, a to čini time što drži u tajnosti njihovo znanje i njihove namjere. Po svojoj tendenciji, birokratska uprava je oduvijek bila uprava koja isključuje javnost. Kako navodi Weber, „birokracija uvijek skriva svoje znanje i djelovanje od kritike“ (u Đurić, 1987: 415).

Nadalje, dolazak pojedinca na administrativne funkcije odvija se na temelju zakonski propisanih procedura koje definiraju njihovu kompetentnost da obavljaju određenu dužnost, pri čemu je njihova individualnost posve irelevantna. Te se funkcije ispunjavaju neovisno o osobi koja ih obavlja i neovisno o osobama ili grupama na koje se određeni postupci odnose, odnosno

funkcije su u potpunosti depersonalizirane. „U specifičnom smislu, za potpuno razvijenu birokraciju vrijedi i princip *sine ira et studio*[29]. Svoju osobitu prirodu, koja je kapitalizmu dobro došla, birokracija razvija sve potpunije što se više dehumanizira, tj. što više uspijeva osloboditi vršenje službenih poslova od ljubavi, mržnje i drugih čisto osobnih i emocionalnih elemenata koje je nemoguće izračunati“ (Weber, 1922 u Đurić, 1987: 396). Upravo zbog racionalnosti koja leži iza ovog principa birokrati mogu postati alijenirani, što može imati brojne negativne posljedice.

Svaki službenik zaposlen u birokratskom sustavu za svoj rad dobiva plaću. Da bi birokracija mogla tako funkcionirati, Weber govori kako je potreban izvor prihoda za vlastito održavanje. Birokratski organizirana privatna poduzeća to su rješavala iz privatnog profita, a za države je to značilo porast izdataka iz javne blagajne. Masovna demokracija, koja je zamijenila prethodne sustave uprava, zbog obima posla upravljanja njome bila je primorana uvesti plaćeni profesionalni rad, a time je porezni sustav postao preduvjet trajnog postojanja birokratske uprave (Đurić, 1987). Danas je održavanje birokratskog aparata postalo preskupo za određene države pa se traže brojni načini kako smanjiti i poboljšati rad javne uprave.

Weber je bio impresioniran nagovaračkim utjecajem (nagovaračkom osobinom) racionalizacije. Uočio je da čak i kada postoji neslaganje s depersonaliziranim pravilima, pojedinci se ipak pokoravaju, bez da su na to bili prisiljeni. Tu snažnu silu Weber je pripisivao racionalnom autoritetu depersonaliziranih pravila, što je za njega bila moralna sila koja je pogonila modernost (Stark, 2014). Racionalno-legitimna vlast, kao jedna od tri vrste vlasti koje Weber raspoznaje, počiva na vjerovanju u zakonitost racionalno uspostavljenih naredbi i onih koji upravo na toj osnovi provode vlast. Legitimnost se ne pridaje posebnoj osobi, već zakonima bezličnog karaktera koji tvore apstraktna i za sve jednako važeća pravila. Zakoni ne crpe svoju legitimnost iz prošlosti nego prije svega iz činjenice da su stvoreni na racionalan način na osnovu formalno mirne rasprave (Đurić, 1987).

No, Weber je smatrao kako racionalna vlast neizbježno dovodi do birokratskog apsolutizma. Naime, one iste odlike koje omogućuju uspješno djelovanje racionalne vlasti, kao što su stroga podjela rada i oštro odvajanje sfere službene dužnosti od sfere privatnih interesa, ugrožava same temelje na kojima počiva ta vlast. Racionalna društvena organizacija, prema Weberu, priprema društvo na novi oblik ropstva, kroz produbljivanje suprotnosti između pojedinca u društvu i stručnjaka, poistovjećivanje pojedinca s njegovom funkcijom u društvenoj podjeli rada, ili kroz činjenicu da takva društvena organizacija od svojih članova zahtjeva da

[29] lat.: bez srdžbe i pristranosti

izvršavaju dužnosti čiji dublji smisao ne poznaju i u potpunosti ne razumiju (Đurić, 1987). Takva društvena organizacija lako može postati otuđena od čovjeka kojemu treba služiti i postati nekakva vrsta tradicionalizma.

Suvremene analize Weberove teorije došle su do zaključka kako njegovo poimanje racionalnosti birokracije dovodi do dvije različite pojave. Prvo, racionalnost birokracije se ocrtava u maksimalnom povećanju tehničke učinkovitosti. Pravila se kontinuirano osuvremenjuju novim stručnim spoznajama čime se iznova pronalazi najprikladnije rješenje za probleme organizacije, a ponašanje članova se time usmjerava u najučinkovitijem smjeru. Drugo, u društvu se pojavio 'racionalno-zakonski' sustav vrijednosti zbog kojeg članovi društva nametnuta pravila i norme smatraju racionalnim, pravednim i nepristranim, čime je birokracija postala svojevrsni sustav društvene kontrole (Abercrombie et al., 2008).

Jednom kada je birokratski aparat uspostavljen, prema Weberu, oni koji nisu na vlasti ne mogu pronaći način da ga se odreknu niti da ga zamijene. Istovremeno, svaki službenik je „prikovan za birokratsku mašinu“ (Weber, 1922 u Đurić, 1987: 411) i jedino o čemu brine je da ta mašina nastavi neprekidno funkcionirati i održavati postojeće društvene odnose. Birokracija kao takva ne može pojedincu u sustavu pružiti osobni rast i razvoj osobnosti (Bennis, 1965) što može dovesti do potpunog osjećaja bezvrijednosti i otuđenja tog pojedinca, ali posljedično može škoditi i cijelom društvu.

Nadalje, istraživanja provedena u 20. stoljeću pokazala su kako mnoge birokratske organizacije djeluju neučinkovito na načine koje Weber nije mogao zamisliti. Birokratske organizacije postale su nefleksibilne, a Robert K. Merton je uzrok tog problema pronašao u samoj strukturi organizacije. Kolege jednog ureda razvit će osjećaj zajedničke sudbine zbog istog i opetovanog načina rada, što posljedično dovodi do dobre suradnje, odnosno do dobro podmazane mašine koja pozitivno djeluje na funkcioniranje birokracije. Ali, to dovodi i do razvoja neformalne društvene organizacije kojoj su njeni vlastiti interesi bitniji od drugih. Suradnici razvijaju osjećaj lojalnosti i grupni interes koji može imati negativne posljedice po samu organizaciju. Počinju razumijevati da oni imaju moć nad informacijama unutar svog odjela i na taj način mogu uspostaviti kontrolu, što bi se očitovalo u usporavanju procesa, davanju nepotpunih informacija i sl., bez obzira radilo se o njima nadređenima, ili o klijentima (Merton, 1968). Isto tako, službenici se počinju nekritički odnositi prema pravilima, ritualno ih slijediti i uzdižu ih na višu instancu od ciljeva čijem su ostvarenju namijenjena. Dolazi do toga da prate pravila bez obzira vode li u pogrešnom smjeru ili jesu li učinkovita s obzirom na okolnosti (Abercrombie et al., 2008). Autoritet racionalnih pravila tada pokazuje svoju

neosjetljivost na promjene ili inovaciju, a konačni rezultat je stvaranje administrativnog vrtloga i još veće kompliciranje procedura.

Michel Crozier diskutirao je o birokraciji kao zatvorenom, začaranom krugu kojem se zbog same racionalne naravi smanjuje uspješnost i učinkovitost. Čak i kada nepravilnosti unutar sustava budu primijećene, nadređeni ne mogu proizvoljnom akcijom utjecati na pogrešku, već za to moraju osmisliti nova pravila kako bi spriječila takve pogreške u budućnosti. Nova pravila cijeli sustav čine još rigidnijim, ali niti to ne jamči uspješan nadzor nad podređenima. Na taj način birokracija postaje još manje učinkovita i ne omogućuje potpuni nadzor nad sustavom (Abercrombie et al., 2008). Istovremeno, nemoguće je iskoristiti puni potencijal ljudskih resursa koje birokracija ima zbog izostanka povjerenja među zaposlenima (Bennis, 1965), a to onda dovodi i do slabosti prilagodbe na nepredvidljivosti.

Bauman je govoreći o etici modernosti, ustanovio da je birokracija jedna od institucija modernosti koja je pospješila izgradnju svijeta slobodnog od moralne dvosmislenosti (dvoznačnosti). U birokraciji se jedino depersonalizirana i racionalna pravila smatraju u potpunosti istinitima i pravednima, zbog čega se pojedinac unutar sustava jednostavno pokorava naredbama svojih nadređenih. Iako snosi odgovornost za svoje postupke, službenik se ne susreće s moralnim dilemama tijekom svojeg djelovanja, jer je ono u potpunosti podređeno pravilima (prema Kelemen i Peltonen, 2001). On, zapravo, ne dovodi u pitanje ispravnost svojih postupaka, jer su za njega oni sigurno ispravni ako prate pravila. Zbog toga službenik postaje dehumanizirani stroj bez ikakvih moralnih kriterija, a to, prema Baumanu, može dovesti i do genocida.

S druge strane, Foucault je na birokraciju gledao kao na alat za uspostavljanje nadzora sa svrhom da se moralno i materijalno nametne moć norme. Smatrao je kako pojedinac doživljava svoju 'formalizaciju' jedino ulaskom u dokumentarno polje, odnosno onda kada sve ustanove kojih smo dio kroz svoj život, metodom administrativne dokumentacije uspostave nadzor nad nama (prema Kalanj, 1993). Predindustrijske države nisu imale učinkovita sredstva nadzora pa su se više oslanjale na fizičku prisilu. Moderne države su u dobro razvijenim informacijskim sustavima, koji su najčešće bili u rukama birokratskih aparata, pronašle način na koji mogu imati nadzor nad svojim stanovnicima. Podaci koji se nalaze u rukama državnog aparata, bilo socijalnim službama, policiji ili lokalnoj samoupravi, ali i u rukama privatnih poslovnih subjekata kao što su banke, između ostalog služe za stvaranje ovisnosti pojedinca u društvu i sustava, ali i za uspostavljanje određene kontrole nad njihovim životima (Abercrombie et al., 2008).

Navedene kritike birokracije uklapaju se u ono što je Weber nazvao 'željeznim kavezom'. Čista racionalnost, mehanizacija procedura i dehumanizacija pojedinaca uključenih u birokratski sustav doista mogu stvoriti osjećaj zatvora. Umjesto da im racionalno osmišljena pravila i procedure pomažu, čovjek biva zatočen u ovoj „ljušturi tvrdoj kao čelik“ (Weber, 1922 u Đurić, 1987), otjeran u beznađe iz kojeg ne vidi izlaz. Dok s jedne strane birokracija doista omogućava organizaciju na način nezamisliv u prijašnjim fazama razvoja društva, zbog čega je iznimno korisna tehnologija za upravljačka tijela, s druge strane upravo to pretvara sve uključene u robote, ili veliko računalo u kojemu su ljudi postali ništa više vrjedniji od operacijskog sustava koji pokreće naše mobitele. Zbog toga je za Webera svaka ideja pronalaska alternative birokraciji bila čisto utopistička, no tu nije bio u pravu.

Razvojem tehnologija i načina poslovanja unazad 50 godina tvrtke su shvatile da robotizirani zaposlenici neće ostvariti zacrtane ciljeve i dovesti do velike zarade. Tako su poduzeća postala svjesna važnosti ljudske dobrobiti i dobrih međuljudskih odnosa te su razvili koncept ljudskih potencijala. Također, postale su fleksibilnije u radu s klijentima i pružanju usluga, a prešli su i na horizontalnu organizaciju upravnih poslova (Johnston, 1993). Mali pomaci u odnošenju prema zaposlenicima i klijentima stvorili su neko novo i za Webera nezamislivo radno okruženje.

Alvesson i Thompson (2006) kada govore o post-birokraciji i na taj način organiziranim sustavima govore o novom dominantnom sustavu vrijednosti unutar struktura uprave. To su decentralizirani, fleksibilni, horizontalni, fluidni i labavo povezani sustavi koji funkcioniraju na temelju prilagodljivih horizontalnih i vertikalnih mreža, vođenih zajedničkom vizijom i vrijednostima, umjesto strogim pravilima i snažnom kontrolom. Takvi sustavi mogu se onda nositi s izazovima s kojima se susreću, kao što su povećanje konkurencije, deregulacija, globalizacija proizvodnje, rastući broj novih proizvoda, nova znanja i razvoj informacijske tehnologije, diferencirana i brza promjena preferencija kupaca, dominacija nematerijalnih usluga i raznolikost radne snage (Alvesson i Thompson, 2006). Sa svime navedenim, stara i zakržljala birokracija se ne bi znala nositi. Ipak, možda najveći utjecaj na nove organizacijske sustave je imala informacijska tehnologija koja sa svojom tehničkom logikom stvara temelje za demokraciju unutar procesa donošenja odluka.

Tu je i pojava 'tehnokratske racionalizacije' koja se temelji na unaprijed programiranim i internaliziranim sustavima pravila, procedura i izvanjskim sustavima kontrole, a posljedica toga je stvaranje neformalnih odnosa, generalnih pravila i minimalne podjele rada (Taylor, 1994; Heydebrand 1989, u Alvesson i Thompson, 2006). Nove informacijske tehnologije danas imaju moć preobraziti nekadašnje sustave, s velikim brojem zaposlenih ljudi koji rade na

provođenju depersonaliziranih i racionalnih pravila i procedura, u sustave s doslovno depersonaliziranim i racionalnim pravilima i procedurama koji su utkani u računalni kod, spašavajući mase ljudi od zatvora željeznog kaveza.

## 4.1 Stanje birokracije u Hrvatskoj

Kako ne bi sve ostalo na pukoj teoriji, dosege birokracije i pojavu post-birokracije objasnit ću na primjeru hrvatske javne uprave. Birokraciju je Hrvatska naslijedila još od doba Habsburške monarhije, a tada zadane strukture samo su ojačale u dobu socijalizma. Za promjenu tog velikog i krutog naslijeđa potrebna je velika politička, ali i građanska volja, koja se još uvijek nije prikazala u pravom smislu (Koprić, 2018). Kada se studenti sociologije susretnu s Weberovom teorijom birokracije čini im se vrlo realna i suvremena, budući da je svatko imao više ili manje mukotrpno iskustvo s ulaskom u željezni kavez. Da nije samo stvar dojma, potvrđuje i statistika.

Prema Izvještaju o kvaliteti javne uprave Europske komisije, u kojem se analiziralo šest elemenata javne uprave, od upravljanja i organizacije vlade do pružanja usluga i digitalizacije, Hrvatska se smjestila na 26. od 28 mjesta, čime je Hrvatska na začelju Europske unije kada je riječ o učinkovitosti javne uprave[30]. Kao glavni nedostaci hrvatske javne uprave ondje se ističu veličina, prevelika centralizacija, administrativna opterećenost i ovisnost o politici. Iako načelno postoji strategija za digitalizaciju sustava, jedina veća reforma u tom smjeru bilo je uvođenje e-Građanin sustava (Koprić, 2018).

Prema podacima iz 2015. u državnim tijelima je zaposleno oko 317 tisuća ljudi, što čini 18% zaposlenih u Hrvatskoj. U samom upravnom sektoru države zaposleno je oko 75 tisuća ljudi, što je 23,7% od svih zaposlenih u državnim tijelima. Iako se nakon pojave krize 2008. govorilo o reformama koje bi trebale donijeti smanjenje broja zaposlenih u državnim tijelima, veći pomaci se nisu napravili (Koprić, 2018). Nadalje, prema podacima iz 2017.[31] Hrvatska je za javnu upravu izdvojila 7,8% svog BDP-a, odnosno 27,8 milijardi kuna. U to se računaju izvršni i zakonodavni organi, financijski i fiskalni poslovi, vanjski poslovi, opće usluge, transakcije javnog duga itd. Najveći dio ovih izdvajanja, oko 14,9 milijardi kuna, odlazi na

[30] Preuzeto s: https://faktograf.hr/2018/10/30/je-li-hrvatska-javna-uprava-po-efikasnosti-stvarno-samo-ispred-venezuele/ Učitano: 10. kolovoza 2019.
[31] Preuzeto s: https://slobodnadalmacija.hr/novosti/hrvatska/clanak/id/597445/hrvatski-paradoks-standard-na-dnu-javni-sektor-meu-najskupljima-u-europi-najvise-od-svih-izdvajamo-za-religijske-zajednice-a-time-se-ne-mozemo-pohvaliti-kada-su-u-pitanju-zdravstvo-i-obrazovanje Učitano: 10. kolovoza 2019.

zakonodavne i izvršne vlasti u koje se računaju Sabor, ministarstva financija i vanjskih poslova i Državno izborno povjerenstvo. Za javnu upravu kao država izdvajamo puno više od Europskog prosjeka, gdje sveukupno izdvajanje iznosi 5,8% BDP-a, a od toga izdvajanje za zakonodavne i izvršne vlasti 1,8%.

Neke od glavnih kritika u izvješću Europske komisije govore kako je hrvatska javna uprava još uvijek u znatnoj mjeri formalizirana, sklona velikim procedurama, tajnosti i poslušnosti, otporna je na promjene, hijerarhijski posložena te izostaju inicijative, inovacije i fokus na rezultat. Promjene koje su se u zadnjih 10 godina događale u ovom području bile su usmjerene na poboljšanje odnosa između vlade i građana, ali i općenito odnosa u društvu, dok su se pitanja unutarnjih promjena birokratskog aparata ostavljala sa strane. Ipak, veliki pomak prema modernizaciji javne uprave uvođenje je sustava e-Građanin, čiji su rezultati postali vidljivi u većoj brzini pružanja usluga, smanjenju birokratskih troškova, nepristranosti u javnim službama te povećanju zadovoljstva građana. U kontekstu Europske unije ovi pomaci su i dalje vrlo skromni, a glavni razlozi zaostajanja Hrvatske s razvojem e-usluga su: veliki napori na razini središnje vlade, dok na lokalnim razinama zbog nedovoljnog kapaciteta razvoj kasni; alokacija odgovornosti iz glavnog tijela kao što je Ministarstvo uprave i stvaranje Središnjeg državnog ureda za razvoj digitalnog društva; kompleksni i vrlo proceduralni zakoni koji otežavaju promjenu te općenito slaba kvaliteta državnih usluga (Koprić, 2018).

Dakle, unatoč malim pomacima u modernizaciji, čini se kako Hrvatska i dalje ima prilično velik problem s birokratskim tijelima. Velik broj zaposlenih znači i velika izdvajanja za održavanje takvog sustava, a iako je postojala inicijativa za digitalizaciju dijela uprave, što bi utjecalo i na smanjenje zaposlenih, nakon prvih koraka ta reforma se zaustavila. Prema tome, govoriti o uvođenju *blockchain* tehnologije kao digitalizirane birokracije u Hrvatskoj čini se kao optimističan, ali nedostižan cilj, barem prema trenutnom stanju stvari. No, kao što je to uvijek stvar s novim informacijskim tehnologijama, treba proći proces upoznavanja i navikavanja građana na njih, a tu ulogu u društvu će i ovaj put, čini se, odigrati privatni sektor.

## 5. *BLOCKCHAIN* KAO BIROKRACIJA 21. STOLJEĆA

Nema sumnje da je pojava birokracije imala velikog utjecaja na razvoj društva. Tada nove moderne države uz pomoć birokracije pronašle su način kako da uspostave red, a kapitalizam kao tvorevina modernosti iskoristio je birokraciju za učvršćivanje svojih struktura. Velika količina informacija koja se pojavila u modernim državama se pojavom birokracije utjelovila i dobila svrhu u obliku sredstva za kontrolu. Danas su upravo informacije pokretač

promjena, sredstvo razmjene, a razvojem informacijskih tehnologija i alat za daljnji društveni razvoj. Ako to prihvatimo kao činjenicu, može li se na jednu od novijih informacijskih tehnologija, *blockchain*, gledati kao na sredstvo za ostvarenje Weberove utopije? Nalazi li se društvo neposredno ispred revolucionarne društvene promjene, onakve promjene koja će zauvijek odrediti smjer kretanja društvenog razvoja?

Kako je već ranije bilo spomenuto, *blockchain* i birokracija su međusobno usporedivi, ako se na njih gleda kao na organizacijske tehnologije. Obje tehnologije primaju, obrađuju i spremaju neku vrstu informacija i obje tehnologije rade na temelju depersonaliziranih i racionalnih pravila. Jedna velika razlika se odnosi na ljudski faktor, odnosno, tamo gdje su ljudi bili operacijski sustav koji je pokretao birokratsku mašinu, sada dolazi računalni operacijski sustav, a uredi i pravila se zamjenjuju pravim hardverima i softverima. Čini se da je došlo vrijeme da racionalizacija poprimi svoj novi, najviše tehnički do sad, identitet, a da ovoga puta ne uključuje gomile 'porobljenih' ljudi.

Kavanagh i Miscione (2015) su iscrtali odnos birokracije i *blockchaina* te usporedbom prikazali nevjerojatan potencijal kojeg kao društvo možemo ostvariti ako implementiramo ovu novu tehnologiju.

Prva usporedba tiče se radnog vremena organizacijskog aparata. U birokraciji službenik premda ima radno vrijeme, svoj posao obavlja u kontinuitetu, a na njegov rad nadovezuju se ostali službenici iz drugih odjela. *Blockchain*, odnosno rudari na *blockchainu*, također kontinuirano prikupljaju informacije, slažu ih u blokove i vežu na *blockchain*. Ako se samo jedan rudar isključi iz mreže, svi ostali samo će nastaviti sa svojim radom.

Drugo, u birokraciji su radne dužnosti napravljene prema depersonaliziranim objektivnim kriterijima, iza kojih stoji, kako je već ranije spomenuto, sustav razloga. Pravila se ne donose u odnosu na bilo kojeg zaposlenika, već se traži univerzalno pravilo kojeg svi mogu slijediti. Kod *blockchaina* se pravila koja rudari moraju pratiti nalaze u komunikacijskim protokolima koji su također depersonalizirani, jer se odnose na računalne algoritme i ono što rudari putem njih mogu raditi. U sustavu Bitcoina, komunikacijski protokol se sastoji od uputa za rad *proof-of-work* konsenzusa, *hash* funkcija, obavljanje transakcija i sl.

Treće, u birokraciji je službeniku omogućen autoritet koji mu je potreban kako bi mogao izvršiti dodijeljene dužnosti. U hijerarhijskom lancu zna se tko, što i kako može raditi, a na vrhu stoji glavni autoritet kojemu su svi ostali podređeni. Kod *blockchaina* je situacija nešto drugačija jer svi rudari uključeni u mrežu rade jednak posao i međusobno se natječu u izvršenju zadatka. U javnim i otvorenim *blockchain* sustavima ne postoji autoritet, već on proizlazi iz komunikacijskog protokola, odnosno iz samih racionalnih pravila zadanih na početku.

Četvrto, kako svaki službenik ima dodijeljen autoritet, tako ima dodijeljena i sredstva prinude, odnosno ima zadane načine na koji može obaviti zadatak kako bi ispunio zadani zadatak. Uvjeti upotrebe takvih sredstava su strogo definirani. Kod *blockchaina* je, ponovno, sve određeno u komunikacijskom protokolu. Jednom postavljen način funkcioniranja sustava se ne može mijenjati, tako da rudari strogo znaju što mogu, a što ne mogu raditi te ih sustav sam po sebi sprječava da naprave išta drugačije.

Peto, u birokraciji odgovornosti i ovlasti svakog službenika proizlaze iz vertikalne hijerarhije autoriteta, a s njima i odgovarajuća prava nadzora i žalbi. S druge strane, u *blockchainu* rudari djeluju u horizontalnoj organizacijskoj strukturi gdje autoritet proizlazi, ponovno, iz komunikacijskog protokola, a rudari se međusobno razlikuju jedino u računalnoj snazi koju posjeduju. Pojmovi nadzora i žalbe zapravo ne postoje, niti su potrebni.

Šesto, birokratski službenici ne posjeduju resurse potrebne za obavljanje dodijeljenih funkcija, no odgovorni su za njihovu upotrebu. Birokrati svoj posao obavljaju u uredima njima nadređene institucije i koriste dodijeljen pribor za rad. Kod *blockchaina* je drugačija situacija, jer svaki rudar, odnosno pojedinac koji upravlja uređajem za rudarenje, ima vlasništvo nad tim uređajem. Taj uređaj radi neovisno o tome nalazi li se pojedinac uz njega ili ne, a rudarenje se može odvijati s bilo kojeg mjesta na svijetu, potrebna je samo veza za Internet.

Sedmo, u birokraciji su službeni posao i privatnost pojedinca strogo odvojeni. Službenik svoju dužnost obavlja u određenom radnom vremenu, a njegov privatan život ni na koji način ne bi smio utjecati na njegov posao. S druge strane, budući da *blockchain* može biti javan, svi korisnici, uključujući i rudare, ali i sve ostale korisnike, imaju osiguranu anonimnost i privatnost. Kod javnih *blockchaina* to je osigurano kroz enkripciju svih podataka. Kod privatnog i zatvorenog *blockchaina* ne postoji anonimnost i privatnost, jer je u interesu vlasnika *blockchaina* da zna što i kako njegovi rudari rade.

Osmo, u birokraciji službenici nemaju mogućnost prisvajanja ureda i alata s kojima rade, tj. ne mogu ih kupiti ili naslijediti. Sve potrebno za njihov rad pripada njihovoj nadređenoj instituciji. Za održavanje sustava na *blockchainu* pojedinci mogu kupiti svoje uređaje za rudarenje, pa tako i prodati ili naslijediti alat za obavljanje svog rada.

Deveto, službeni posao u birokratskom sustavu odvija se na temelju pisanih dokumenata i protokola. Ti dokumenti i protokoli doneseni su na temelju izračuna učinkovitosti i mogu se mijenjati ako se pronađe neko novo i bolje rješenje za izvršavanje dužnosti. Ta odluka onda dolazi odozgora. Protokol *blockchaina* je automatizirani algoritam, koji jednom kad je postavljen postaje autoritet za sve uključene na mrežu. U pravilu se ti protokoli ne mijenjaju,

jer su osmišljeni baš i isključivo za izvršavanje određenih funkcija, no moguće ih je promijeniti ako se svi rudari i vlasnici čvorišta slože s tim.

Deseto, postoji podjela moći između političara (onih koji drže birokratski aparat u rukama) i birokrata. Na vrhu birokratske organizacije nužno postoji element koji nije strogo birokratski. Kod *blockchaina* postoje različiti odnosi moći s obzirom na to radi li se o javnom ili privatnom *blockchainu*. U javnom *blockchainu* ne postoji jasna podjela moći, niti postoje jasni mehanizmi upravljanja, osim onih upisanih u komunikacijski protokol. Iako postoji Bitcoin fundacija koja radi na implementaciji Bitcoina u drugim sustavima, kolaps ove neprofitne organizacije ne znači nužno i propast Bitcoin sustava, budući da je to projekt otvorenog koda i ne postoji vlasnik ovog sustava. U privatnom *blockchainu* najveću moć ima njegov vlasnik.

Jedanaesto, birokrati za svoj rad dobivaju plaću, koju im je dodijelio autoritet prema određenim kriterijima. U otvorenim *blockchain* sustavima rudari također dobivaju svojevrsnu naknadu za svoj rad, takozvani *block reward*, ali i udio od transakcija čiji podaci su ušli u blok. Kod zatvorenih *blockchain* sustava ne postoji naknada za rad rudara, ali nije niti potrebna jer se podrazumijeva da su uređaji za rudarenje pod kontrolom osobe odobrene od vlasnika *blockchaina*.

I posljednje, birokracija radi u službi građana i onih kojima je dato to pravo od strane države ili druge birokratski organizirane institucije. Ako pojedinac želi koristiti usluge takve organizacije, mora proći određene procedure kako bi se njegovi podaci mogli koristiti i obrađivati. *Blockchain* regulira i sakuplja sve informacije svih korisnika bez ikakvih distinkcija. Jedino što je potrebno imati je pristup mreži, što svatko može dobiti.

Vidljivo je kako *blockchain* u nekom smislu funkcionira na sličan način kao birokracija jer su obje tehnologije za organizaciju podataka i obje se temelje na strogoj racionalnosti te automatiziranim procedurama. Ljudski rad je velika razlika između ove dvije tehnologije, a izostanak potrebe za tolikim brojem zaposlenih ljudi u birokraciji, *blockchain* tehnologiji omogućava ostala svojstva, kao što su decentralizacija ili transparentnost. Za potpuno razumijevanje mogućih dosega *blockchain* tehnologije, potrebno je pogledati cijeli kontekst četvrte industrijske revolucije. *Blockchain* možemo smatrati alatom, zajedno s ostalim tehnologijama kao što su umjetna inteligencija, autonomna vozila ili Internet stvari pomoću kojih se polako pomiču granice između fizičkog i kibernetičkog prostora (Aste et al., 2017). Sve to može donijeti veliku promjenu u brojnim poslovnim sektorima, a za društvo u cjelini to znači revolucionarnu promjenu u svakodnevnom djelovanju.

Za razliku od birokracije, *blockchain* ima puno veću operativnu efikasnost zbog stvaranja i održavanja distribuiranih i nepromjenjivih baza podataka (Aste et al., 2017). Danas države i tvrtke koriste centralizirane baze podataka koji i dalje iziskuju manualni rad stručnjaka, a tako čuvani podaci izloženi su napadima i izmjenama. Pojedinci kojima je potrebna neka informacija se i dalje moraju oslanjati na posrednika kako bi došli do onoga što traže. Distribuirane i nepromjenjive baze podataka to mogu promijeniti u smislu da je kontrola nad vjerodostojnosti podataka na *blockchainu* podijeljena između svih na mreži, pa čak i kada se radi o zatvorenim *blockchain* sustavima to znači puno veću kontrolu i sigurnost podataka. S druge strane, za pojedince to znači izravan pristup *blockchainu* i podacima koji im trebaju, čime bi se mogle olakšati administrativne procedure koje i danas, bez obzira na sve veću digitalizaciju, ostaju veliki problem suvremenih birokratskih organizacija. Naravno, ovdje treba uzeti u obzir i digitalnu pismenost cijelog društva koje možda još uvijek nije spremno za potpunu digitalizaciju.

Nadalje, *blockchain* je na glasu radikalno transparentne tehnologije (Ković, 2017; Davidson et al., 2016). Ideja iza *blockchaina* je omogućiti svima na mreži uvid u bazu podataka, ali i mogućnost nadgledanja onoga što se trenutno na mreži događa. Ković (2017) je radikalnu transparentnost objasnio na primjeru implementacije *blockchaina* za e-glasovanje, odnosno glasovanje na građanskim izborima putem Interneta. Koristeći *blockchain* osmišljen samo za svrhu glasovanja, putem pametnih ugovora moguće je prikupljati i slagati glasove. Građani mogu pristupiti tom *blockchainu* putem posebne web stranice sa svojim podacima, koji su im potrebni i za glasovanje. Nakon što daju svoj glas, ta informacija bude šifrirana i nitko ne može vidjeti tko je kako glasovao, čime su podaci glasača osigurani. No, umjesto da se glasovi prikupljaju kroz cijeli dan i na kraju zbroje, moguće je odmah vidjeti kako se akumuliraju glasovi. Osim što to može vidjeti središnje izborno povjerenstvo, to mogu vidjeti i svi građani s pristupom. Oni ne mogu vidjeti tko je kako glasao, ali mogu vidjeti za koga ostali glasači glasaju i na taj način mogu sudjelovati u *real-time* brojanju glasova. To je radikalna transparentnost jer svi koji imaju interes mogu vidjeti što se događa u svakom trenutku. Na sličan način mogu funkcionirati i transakcije ili kompleksnije procedure koje se rade putem pametnih ugovora.

Što se tiče povjerenja, do sad su se države bile te koje su kroz institucije održavale povjerenje, brinule o sigurnosti građana i zaštiti imovine. Velikim dijelom države su to radile kroz birokraciju, a glavni jamac sigurnosti i povjerenja su bile one same. *Blockchain* jamči povjerenje kroz računalnu tehnologiju. Bitcoin transakcije su sigurne zato što su podaci kojima se trguje šifrirani, a napadi na mrežu su minimizirani kroz distribuiranu odgovornost svih na

mreži. Ta svojstva može iskoristiti država kako bi poboljšala svoj birokratski aparat, pogotovo u onim institucijama čija je jedina funkcija čuvanje podataka. *Blockchain* se tako može koristiti za upravljanje sustavima građanskih isprava (osobne iskaznice i putovnice), za ovjeravanje i licenciranje, za registre katastarskih imovina i slično, za razmjenu i trgovinsku infrastrukturu, operativno upravljanje javnom imovinom i komunalnim uslugama ili za javne financije (Potts, 2019). Za sve navedene sustave potrebna je velika administrativna i ekonomska infrastruktura, a s *blockchainom* procedure u tim sustavima mogu biti automatizirane, time i operativno efikasnije.

Bez obzira na potencijal *blockchaina*, radi se o relativno novoj tehnologiji s malim brojem razvijenih patenata te se može reći kako još uvijek traje razvojna faza. Jedan od razloga leži u samoj edukaciji stručnjaka za rad s *blockchainom*, jer se smatra da je to pomalo 'ezoterična' tehnologija, stvorena na konceptima kriptografije, teoriji igara, mreži jednakih korisnika, algoritmima za konsenzus i inženjeringu baze podataka. Programeri koji sudjeluju u razvoju platformi na *blockchainu* u većini slučajeva su samouki, a tvrtke koje su uspjele prebaciti svoje poslovanje na *blockchain* to su uglavnom radile kroz eksperimentalno učenje (Potts, 2019). U budućnosti će biti potrebno uložiti puno napora u stvaranje educiranih stručnjaka, prvenstveno programera, ali i ostalih znanstvenika koji će raditi na implementaciji i upoznavanju društva s *blockchain* tehnologijom.

Odnos novih tehnologija i zaposlenosti dvojakog je karaktera (van Est et al., 2015). S jedne strane, inovacija dovodi do ekonomskog rasta, povećanja radnih mjesta i sveukupnog napretka. Tehnološke inovacije dovode do veće produktivnosti i jeftinijih proizvoda, što dovodi do veće potrošnje i povećanja moći tržišta. S druge strane, povećanje produktivnosti pomoću tehnoloških inovacija dovodi do smanjenja zaposlenosti, smanjenja potrošačke moći i moći tržišta. Unazad 20 godina informacijske tehnologije su imale velikog utjecaja na zaposlenost, a ono što se iz ove povijesti može naučiti jest da oba gore navedena scenarija postaju realnost. Iako doista dolaskom novih informacijskih tehnologija ljudi ostaju bez poslova, ubrzo se zbog utjecaja upravo tih tehnologija stvaraju nova radna mjesta. Ekonomskim jezikom, događa se 'efekt drugog reda' čime se ušteda koja se stvorila povećanjem efikasnosti zbog novih tehnologija vraća natrag na tržište (van Est et al., 2015). Nove tehnologije stvaraju nova ozračja u kojima dolazi do potrebe za novim stručnim znanjima koja same tehnologije ne mogu nadomjestiti, pa tako se kroz nekoliko godina od inovacije stvaraju nova radna mjesta.

# 6. ZAKLJUČAK

Vrijeme u kojem živimo puno je zanimljivih ideja i rješenja za sveukupno poboljšanje kvalitete života. Umreženost, koje je donijelo 21. stoljeće, a koje uključuje i ljude i uređaje, svakodnevno pomiče granice realnosti i nudi brojne dosad nezamislive mogućnost. Informacije koje proizvodimo kao društvo nemjerljivo rastu iz dana u dan, a s time se pojavljuje i potreba za njihovom regulacijom. *Blockchain* kao jedna od tehnologija četvrte industrijske revolucije može koristiti upravo za to. U ovom radu pokušala sam ponuditi rješenje za klasični sociološki problem birokracije u implementaciji nove tehnologije *blockchaina* u tijela javne uprave. Birokraciju se najlakše može oprimjeriti kroz stroj kojem za pokretanje energiju daju sami ljudi, koji neprestano rade na ispunjavanju pravila i izvršavanju zadaća. Tako gledajući, može se zaključiti kako birokrati nisu ništa drugo nego radnici u tvornicama s boljom plaćom. Jednako kao i radnici tvornica, oni svakodnevno i opetovano izvršavaju iste zadaće te postaju otuđeni od svojeg rada, od proizvoda svoga rada, od svojih kolega i od samih sebe. Kao što je u radu spomenuto, birokrate možemo promatrati kao operacijski sustav koji radi na ljudsku mišićnu i kognitivnu energiju.

Pojava tehnologije koja može zamijeniti njihov rad čekala se skoro dva stoljeća, a iako se u Weberovo vrijeme doista činila utopistička, uvidom u mogućnosti *blockchaina*, možemo reći da ta mala revolucija kuca na vrata. Ako potpuno plastično pogledamo način rada *blockchain* tehnologije, možemo primijetiti nevjerojatne sličnosti s birokracijom. Sve ono što su u birokraciji morali raditi ljudi, prikupljati papire, raspisivati podatke i slagati ih u registratore, tražiti potrebne podatke u velikim šifriranim ladicama i naposljetku određeni dio dana biti na usluzi svim građanima, sada može raditi računalo, a uz uporabu tehnologije Internet stvari, i roboti.

Glavne odlike ove tehnologije mogu se promatrati s obzirom na vrste *blockchaina*, odnosno s obzirom na to radi li se o otvorenom ili zatvorenom te o privatnom ili javnom *blockchainu*. Svojstvo decentralizacije koje ima otvoreni *blockchain* kao što je Bitcoin sustav ogledat će se u izostanku autoriteta tijekom provođenja transakcija, što kao posljedicu može imati smanjenje troškova transakcije kao i izostanak ograničenja količine vrijednosti koja se prenosi. Kod zatvorenih *blockchain* sustava neće postojati decentralizacija jer postoji središnji autoritet kojemu je u cilju nadgledati što se događa unutar sustava. Takav *blockchain* bit će najkorisniji zbog načina na koji se podaci spremaju te, ako se u obzir uzmu pametni ugovori, brzine kojom se određeni zadaci mogu rješavati. Transparentnost, kao još jedno od svojstava,

kod javnih *blockchain* sustava može odigrati veliku ulogu u pomicanju granica demokracije, kao što je ranije naveden primjer sustava e-glasovanja. Što se tiče same birokracije, kao što je već navedeno, uvođenje *blockchain* tehnologije uvelike bi moglo olakšati državni aparat u smislu broja zaposlenih i količine i vrste posla koju bi trebalo odrađivati. Osim što bi smanjio i automatizirao procese unutar samog birokratskog sustava, za građane kao krajnje korisnike to bi značilo smanjenje utrošenog vremena i pojednostavljenje birokratskih procedura. Kao glavni produkt ove promjene pokazala bi se povećana učinkovitost samog sustava, odnosno države.

Kao glavne nedostatke hrvatskog birokratskog sustava, hrvatske javne uprave u radu sam istaknula veličinu, preveliku centralizaciju, administrativnu opterećenost te ovisnost o politici. Uz preduvjet digitalizacije cijelog sustava, *blockchain* tehnologija mogla bi riješiti velik dio problema koji nastaju zbog navedenih nedostataka. Na primjer, za izdavanje građevinske dozvole u današnjem sustavu je potrebno dostaviti izvadak iz zemljišne knjige, dva ugovora, odluku nadležne vlasti te dvije pisane suglasnosti[32]. Pod pretpostavkom da već postoji u potpunosti digitaliziran administrativni sustav građana, do nekih dokumenata jednostavno bi se moglo doći u nekoliko klikova, dok bi druge dokumente trebalo pribaviti na neki način. Samo izdavanje građevinske dozvole moglo bi se riješiti putem pametnih ugovora, u kojem postoje dvije zainteresirane strane, pojedinac koji želi dobiti građevinsku dozvolu i država koja izdaje građevinsku dozvolu. Nakon što pojedinac sakupi potrebnu dokumentaciju, unosi ih u sučelje pametnog ugovora, a koji onda pomoću svog algoritma pregledava jesu li svi dokumenti validni. Nakon što program dokaže da je sve u redu, da je pojedinac donio sve potrebne dokumente, da je sve u redu s česticom za koju pojedinac traži dozvolu te da ne postoji druga zapreka za izdavanje građevinske dozvole, računalo bi jednostavno izdalo građevinsku dozvolu. Ta informacija otišla bi u druge registre povezane s tim pojedincem te bi on odmah mogao početi s gradnjom. Na taj način bi se procedura koja u današnje vrijeme može potrajati i godinama, a u koju se mogu uplesti i politički interesi, jednostavno obavila, izostavljajući danas bitne elemente kao što su dostavljanje biljega, stavljanje u proceduru ili sastanci upravnog vijeća koji odlučuje prolazi li nešto ili ne. Koristeći *blockchain* tehnologiju na ovaj način procedura bi se ubrzala, pojednostavila i rasteretila ljudskog doticaja, a sam sustav postao puno učinkovitiji.

[32] Preuzeto s: https://gradnjakuce.com/gradevinska-dozvola-za-sto-je-sve-potrebna-i-kako-do-nje/ Učitano: . rujna 2019.

Ipak, postoje ozbiljne kritike *blockchain* tehnologije kao takve, i pri ovakvim utopističkim misaonim putovanjima potrebno ih je uzeti u obzir. Prvi je problem potrošnje energije, odnosno zagađenje okoliša koje nastaje zbog načina trošenja energije za pokretanje uređaja za rudarenje. Premda se rješenje tog problema čini prilično jednostavno - prelazak na obnovljive izvore energije – kao i u drugim sferama djelatnosti, bit će potrebno mnogo godina da se dođe do nekih pomaka. U tom smislu sam pesimistična oko daljnjeg razvoja *blockchain* tehnologije. Drugi je problem održavanja vjerodostojnosti tehnologije, odnosno osiguravanja *blockchain* sustava od napada i jamčenja sigurnosti krajnjim korisnicima. Kako se sama tehnologija nalazi u razvojnim fazama, tako se i načini na koji se može naštetiti tehnologiji nalaze u razvojnim fazama. Za očekivati je da će se svakim pronalaskom rješenja za neispravnost tehnologije pronaći novi način da se nanese nova šteta, ali mišljenja sam da je to rizik kojeg trebamo prihvatiti, ako računamo na napore koje stručnjaci ulažu u daljnji razvoj. Treće, veliki problem je daljnja robotizacija društva i gubitak radnih mjesta koji su izgledna posljedica implementacije ove tehnologije. Ne samo zbog otpora društva na takvu promjenu, koji se može pretpostaviti, nego i zbog same činjenice da bi ljudi mogli izgubiti svoja radna mjesta. No, kako je u radu bilo spomenuto, povijest razvoja novih tehnologija naučila nas je da je društvo ipak sklono prilagodbi i kako ne možemo točno predvidjeti na koji način će se ono razvijati uz sve nove tehnologije koje će se tek razviti.

Na valu novih tehnologija četvrte industrijske revolucije za očekivati je da će se one međusobno isprepletati, a kako će konačni rezultat biti ponovno 'olakšanje' ljudskog rada, kao što je bilo u svim industrijskim revolucijama ranije. U kontekstu birokracije, *blockchain* tehnologija zahtjeva potpunu digitalizaciju sustava i automatizaciju procedura, a ljudski rad zamjenjuje radom računalnog operacijskog sustava. Hoće li doista doći do takvih velikih promjena teško je za pretpostaviti, no barem se pojavio tračak nade za oslobađanje od željeznog kaveza. A to je nešto što Weber nikako nije mogao zamisliti.

7. LITERATURA:


Abercrombie, N.; Hill, S.; Turner, B. (2008). *Rječnik sociologije*. Zagreb: Jesenski i Turk

Alvesson, M., Thompson, P., Ackroyd, S., Batt, R., Tolbert, P. S. (2004). Post-bureaucracy? *The Oxford handbook of work and organization*, str: 485-507

Aste, T.; Tasca P.; Di Matteo, T. (2017). Blockchain Technologies: The Foreseeable Impact on Society and Industry. *Computer*. Vol 50, No. 09, str: 18-28

Bennis, W. G. (2017). Beyond bureaucracy. *American Bureaucracy*. New York: Routledge. str: 3-16

Beyer, S (2018). *Blockchain Before Bitcoin: A History*. Preuzeto s: https://blocktelegraph.io/blockchain-before-bitcoin-history/. Učitano: 2. svibnja 2018

*Bitcoin Block Reward Halving Countdown*. Preuzeto s: https://www.bitcoinblockhalf.com/. Učitano: 25. svibnja 2019.

*Bitcoin Energy Consumption Indeks.* Preuzeto s: https://digiconomist.net/bitcoin-energy-consumption. Učitano: 13. kolovoza 2019.

Blakemore, E. (2017). *Human-Pig Hybrid Created in the Lab—Here Are the Facts*. Preuzeto s: https://www.nationalgeographic.com/news/2017/01/human-pig-hybrid-embryo-chimera-organs-health-science/. Učitano 16. kolovoza 2019.

Bloem, J., Van Doorn, M., Duivestein, S., Excoffier, D., Maas, R., Van Ommeren, E. (2014). *The Fourth Industrial Revolution Things to Tighten the Link Between IT and OT*. Groningen: Sogeti

Buterin, V. (2013). *Ethereum White Paper: A next-generation smart contract and decentralized application platform*. Pristupljeno: https://github.com/ethereum/wiki/wiki/White-Paper Učitano: 28. travnja 2019.

Champagne, P. (2014). *The Book of Satoshi: The Collected Writings of Bitcoin Creator Satoshi Nakamoto*. LLC.

Chohan, U.W. (2017). *A History of Bitcoin*. Canberra: University of New South Wales

*Coin Market Cap*. Preuzeto s: https://coinmarketcap.com/all/views/all/. Učitano: 25. svibnja 2019.

Cowan, M. (2018). *The world's first family to live in a 3D-printed home*. Preuzeto s: https://www.bbc.com/news/technology-44709534. Učitano: 16. kolovoza 2019.

Dannen, C. (2017). *Introducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming for Beginners*. Apress Media

Davidson, S., De Filippi, P., Potts, J. (2016). Disrupting governance: The new institutional economics of distributed ledger technology. Preuzeto s: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2811995. Učitano: 8. kolovoza 2019.

Decuyper, X. [Simply Explained – Savjee] (2017) *Asymmetric Encryption – Simply Explained*.[Video] preuzeto s*:* www.youtube.com/watch?v=AQDCe585Lnc. Učitano: 2. kolovoza 2019.

*Delegated Proof of Stake* (2019). Preuzeto s: https://lisk.io/academy/blockchain-basics/how-does-blockchain-work/delegated-proof-of-stake. Učitano: 7. lipnja 2019.

*Delegated Proof-of-Stake (DPoS).* Preuzeto s: https://cryptoslate.com/cryptos/dpos/. Učitano: 3. kolovoza 2019.

Draupnir, M. (2016). *What is the Bitcoin Mining Block Reward?* Preuzeto s: https://www.bitcoinmining.com/what-is-the-bitcoin-block-reward/. Učitano: 2. svibnja 2019.

Đurić, M. (1987) *Sociološka hrestomatija: Sociologija Maksa Vebera*. Zagreb: Naprijed

Frankenfield, J. (2019). *Smart Contracts*. Preuzeto s: https://www.investopedia.com/terms/s/smart-contracts.asp. Učitano: 6. lipnja 2019.

Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C., & Santamaría, V. (2018). To blockchain or not to blockchain: That is the question. *IT Professional*, Vol. *20,* No. 2, str: 62-74.

*Građevinska dozvola – za što je sve potrebna i kako do nje?* Preuzeto s: https://gradnjakuce.com/gradevinska-dozvola-za-sto-je-sve-potrebna-i-kako-do-nje/ Učitano: 1. rujna 2019.

Hertig, A. (n.d)a *What is Ethereum?* Preuzeto s: https://www.coindesk.com/information/what-is-ethereum. Učitano: 6. lipnja 2019.

Hertig, A. (n.d)b *What is Ether?* Preuzeto s: https://www.coindesk.com/information/what-is-ether-ethereum-cryptocurrency. Učitano: 6. lipnja 2019.

Hertig, A. (n.d)c *How Ethereum Works?* Preuzeto s: https://www.coindesk.com/information/how-ethereum-works. Učitano: 6. lipnja 2019.

Ibrahimpašić, B. (2005). *RSA Kriptosustav*, Osječki matematički list, Vol. 5, No 2; str. 101-112.

Jimi, S. (2019) *How does blockchain work in 7 steps — A clear and simple explanation*. Preuzeto s: https://blog.goodaudience.com/blockchain-for-beginners-what-is-blockchain-519db8c6677a. Učitano: 27. travnja 2019.

Johnston, K. B. (1993). *Busting bureaucracy: how to conquer your organization's worst enemy*. Homewood: Bussines One Irwin

Kalanj, R. (1993). Michel Foucault i problem moći, *Revija za sociologiju*, Vol. 24, No. 1-2, str. 77-85.

Kavanagh, D., Miscione, G. (2015). Bitcoin and the Blockchain: a coup d'état in Digital Heterotopia? *Humanistic Management Network, Research Paper Series* Vol. 23, No. 15

Kelemen, M., Peltonen, T. (2001). Ethics, morality and the subject: the contribution of Zygmunt Bauman and Michel Foucault topostmodern'business ethics. *Scandinavian Journal of Management*, Vol. 17, No. 2, str: 151-166.

Koprić, I. (2018). *Public administration characteristics and performance in EU28: Croatia.* Preuzeto s: https://publications.europa.eu/en/publication-detail/-/publication/97f87f51-9608-

11e8-8bc1-01aa75ed71a1/language-en/format-PDF/source-77471233. Učitano: 10. kolovoza 2019.

Kovic, M. (2017). *Blockchain for the people: Blockchain technology as the basis for a secure and reliable e-voting system*. ZIPAR Discussion Paper Series, Vol. 1, No. 1.

Lantz, L. [YOcoin] (2016). *TED Talks: The Blockchain Explained Simply* [Video] preuzeto s: https://www.youtube.com/watch?v=KP_hGPQVLpA. Učitano: 27. travnja 2019

Massesi, D. (2018). *Public Vs Private Blockchain In A Nutshell*. Preuzeto s: https://medium.com/coinmonks/public-vs-private-blockchain-in-a-nutshell-c9fe284fa39f. Učitano: 3. kolovoza 2019.

Matijević, M. (2018). *Hardver za rudarenje kriptovaluta*. Završni rad. Rijeka: Sveučilište u Rijeci

Meijer, D. B. (2017). *Consequences of the implementation of blockchain technology*. Diplomski rad. Delft: Tehničko sveučilište u Delftu

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., Savage, S. (2013). A fistful of bitcoins: characterizing payments among men with no names. *Communications of the ACM,* Vol. 59, No. 4; str: 86-93

Merton, R. K.(1968). *Social theory and social structure*. New York: Simon and Schuster.

Modi, R. (2018). *Introduction to Blockchain, Ethereum and Smart Contracts — Chapter 1*. Preuzeto s: https://medium.com/coinmonks/https-medium-com-ritesh-modi-solidity-chapter1-63dfaff08a11. Učitano: 6. lipnja 2019.

Narayanan, A. (2016). *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction.* New Jersey: Princeton University Press Princeton

Ølnes, S., Ubacht, J., & Janssen, M. (2017). Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. *Government Information Quarterly, Vol. 34;* str: 355-364.

Orcutt, M. (2019). *Hackers may have just stolen $1 million from the Ethereum Classic blockchain in a "51%" attack*. Preuzeto s: https://www.technologyreview.com/f/612728/hackers-just-stole-1-million-from-the-ethereum-classic-blockchain-in-a-rare-51/ Učitano: 30. kolovoza 2019.

Orcutt, M. (2019). *Once hailed as unhackable, blockchains are now getting hacked*. Preuzeto s: https://www.technologyreview.com/s/612974/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/ Učitano: 31. kolovoza 2019.

Pavić, A. (2018). *Je li hrvatska javna uprava po efikasnosti stvarno samo ispred Venezuele?* Pristupljeno s: https://faktograf.hr/2018/10/30/je-li-hrvatska-javna-uprava-po-efikasnosti-stvarno-samo-ispred-venezuele/. Učitano: 10. kolovoza 2019.

Potts, J. (2019). Blockchain and Government. *Data61 'Future of Blockchain'Report*.

*Proof of Stake* (2019). Preuzeto s: https://lisk.io/academy/blockchain-basics/how-does-blockchain-work/proof-of-stake. Učitano: 6. lipnja 2019.

Schneier, B. (2019). *Blockchain and Trust.* Preuzeto s: https://www.schneier.com/blog/archives/2019/02/blockchain_and_.html Učitano: 31. kolovoza 2019.

Schwab, K. (2016). *The fourth industrial revolution*. World Economic Forum.

Stapić, S. (2019). *Hrvatski paradoks: standard na dnu, javni sektor među najskupljima u Europi, najviše od svih izdvajamo za religijske zajednice, a time se ne možemo pohvaliti kada su u pitanju zdravstvo i obrazovanje*. Pristupljeno: https://slobodnadalmacija.hr/novosti/hrvatska/clanak/id/597445/hrvatski-paradoks-standard-na-dnu-javni-sektor-meu-najskupljima-u-europi-najvise-od-svih-izdvajamo-za-religijske-zajednice-a-time-se-ne-mozemo-pohvaliti-kada-su-u-pitanju-zdravstvo-i-obrazovanje. Učitano: 10. kolovoza 2019.

Stark, L. (2014). Declarative Bodies: Bureaucracy, Ethics, and Science in the Making. *Routledge Handbook of Science, Technology, and Society. Declarative Bodies.* New York: Routledge. str: 459-477

Steadman, I. (2013). *Wary of Bitcoin? A guide to some other cryptocurrencies.* Preuzeto s: https://arstechnica.com/information-technology/2013/05/wary-of-bitcoin-a-guide-to-some-other-cryptocurrencies/. Učitano: 2. svibnja 2019.

Stinchcombe, K. (2018). *Blockchain is not only crappy technology but a bad vision for the future*. Preuzeto s: https://medium.com/@kaistinchcombe/decentralized-and-trustless-crypto-paradise-is-actually-a-medieval-hellhole-c1ca122efdec. Učitano: 31. kolovoza 2019.

Tapscott, D. [TED] (2016). *How the blockchain is changing money and business: Don Tapscott.* [Video] preuzeto s: https://www.youtube.com/watch?v=Pl8OlkkwRpc

Thornburg, W. (2018). *What is Ethereum? The Ultimate Beginners' Guide.* Preuzeto s: https://coincentral.com/what-is-ethereum-the-ultimate-beginners-guide/. Učitano: 6. lipnja 2019.

van Est, R., Kool, L. (ur.) (2015). *Working on the robot society. Visions and insights from science about the relation technology and employment*. Den Haag: Rathenau Instituut.

*What Are Nodes?* (2019). Preuzeto s: https://www.binance.vision/blockchain/what-are-nodes Učitano: 2. kolovoza 2019.

*What is Decentralization?* (2019). Preuzeto s: https://lisk.io/academy/blockchain-basics/benefits-of-blockchain/what-is-decentralization Učitano: 2. kolovoza 2019.

Williams, R. (2019). *Ethereum 2.0 Expected To Be Launched In January 2020, Will Allow Integration With PoS Protocol*. Preuzeto s: https://www.cryptonewsz.com/ethereum-2-0-expected-to-launch-in-january-2020-will-allow-integration-with-p-o-s-protocol/26666/. Učitano: 6. lipnja 2019.

Woo, W. (2019). *When did Bitcoin's investment era begin? A study using NVT*. Preuzeto s: https://woobull.com/bitcoins-early-investment-era-under-nvt-ratio/. Učitano: 27. travnja 2019

Yli-Huumo, J., Ko, D., Choi, S., Park, S., Smolander, K. (2016). *Where Is Current Research on Blockchain Technology?—A Systematic Review*. PLoS one. Vol. 11, No. 10

**Sažetak**

Osnovna ideja ovoga rada bila je predstaviti koncept blockchain tehnologije i potencijal koji ova tehnologija ima u rješavanju određenih problema s kojima se birokracija, kao klasični sociološki pojam, susreće u suvremenom dobu. Otkako je 2009. godine koncept blockchain tehnologije predstavljen javnosti, prepoznati potencijal ove tehnologije ne prestaje rasti, a načini primjene svakodnevno se gomilaju. U radu je koncept blockchain tehnologije temeljito objašnjen kroz sustave Bitcoin i Ethereum, a kroz rad dano je nekoliko primjera trenutne i moguće implementacije blockchain tehnologije. Upravo zbog organizacijskog potencijala kojeg blockchain tehnologija ima, usporediva je s birokracijom te se predstavlja kao birokracija 21. stoljeća gdje su određeni dijelovi birokratske mašine koji su u birokraciji sačinjeni od ljudi, zamijenjeni računalnim operacijskim sustavima. Implementacija blockchain tehnologije u birokratske sustave mogla bi imati dalekosežne posljedice kako na sam birokratski aparat tako i na društvo u cjelini, te na taj način postati ostvarenje Weberove utopije društva oslobođenog željeznog kaveza.

*Ključne riječi: blockchain, Bitcoin, birokracija, 4. industrijska revolucija, informacijska tehnologija*

**Summary**

The main idea of this paper was to present the concept of blockchain technology and the potential it has in solving certain problems that bureaucracy, as a classical sociological term, encounters in the modern age. Ever since the concept of blockchain technology was introduced to the public in 2009, the recognized potential and method of application are growing on a daily basis. In the paper, the concept of blockchain technology is thoroughly explained through Bitcoin and Ethereum systems, and through the paper some examples of current and possible implementation of blockchain technology are given. Because of the organizational potential that blockchain technology has, it is comparable to bureaucracy and it presents itself as a 21st century bureaucracy. Now certain human-driven parts of the bureaucratic machine are being replaced with computer operating systems. The implementation of blockchain technology in bureaucratic systems could have far-reaching consequences both on the bureaucratic apparatus itself and on the society as a whole, and thus become the realization of Weber's utopia of a society liberated of iron cage.

*Key words: blockchain, Bitcoin, bureaucracy, fourth industrial revolution, information technology*