Aspekti zaštite privatnosti i autentičnosti digitalnih podataka u Blockchain modelu

Balać, Milan

Master's thesis / Diplomski rad

2018

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Josip Juraj Strossmayer University of Osijek, Faculty of Humanities and Social Sciences / Sveučilište Josipa Jurja Strossmayera u Osijeku, Filozofski fakultet**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:142:570609

Sveučilište J.J. Strossmayera u Osijeku

Filozofski fakultet

Diplomski studij informatologije

Milan Balać

Aspekti zaštite autentičnosti i privatnosti digitalnih podataka u *blockchain* modelu

Diplomski rad

Mentor: prof. dr. sc. Damir Hasenay
Sumentor: dr. sc. Tomislav Jakopec

Osijek, 2018.

Sveučilište J.J. Strossmayera u Osijeku
Filozofski fakultet Osijek
Odsjek za informacijske znanosti
Informatologija

Milan Balać

Aspekti zaštite autentičnosti i privatnosti digitalnih podataka u *blockchain* modelu

Diplomski rad

Područje društvenih znanosti, polje informacijske i komunikacijske znanosti, grana informacijski sustavi i informatologija

Mentor: prof. dr. sc. Damir Hasenay

Sumentor: dr. sc. Tomislav Jakopec

Osijek, 2018.

Sadržaj

SAŽETAK

Rad se bavi pojašnjavanjem *blockchain* tehnologije iz perspektive zaštite autentičnosti i privatnosti digitalnih podataka. Posebna pažnja posvećena je mogućnosti prenamjene tehnologije i njezine upotrebe u zaštiti i očuvanju digitalnih podataka. U radu se pojašnjava praksa zaštite i očuvanja informacijskih objekata i njezin prelazak iz analognog u digitalno doba te se razmatra pojam digitalnih podataka kao digitalnih informacijskih objekata kroz pojašnjavanje tri razine koje sačinjavaju jedan takav objekt. Nadalje, razlažu se pojmovi autentičnosti, pouzdanosti, integriteta i upotrebljivosti informacijskih objekata te karakteristika sustava potrebnih za njihovo očuvanje. Potom se pojašnjava informacijska privatnost kao koncept kojem se pridaje sve više značaja, a usko je vezan uz problematiku očuvanja podataka. Drugi dio rada posvećen je definiranju *blockchain* tehnologije, njezine arhitekture i gradivnih elemenata te ilustriranju njezine funkcije kroz primjer transakcije u Bitcoin valuti – izvornoj implementaciji *blockchaina*. Zatim se pojašnjava način sinkronizacije korisnika u decentraliziranim mrežama putem mehanizama za postizanje konsenzusa te način na koji se *blockchain* odnosi prema informacijskoj privatnosti i autentičnosti podataka. U konačnici se pažnja posvećuje primjenama *blockchaina* u kontekstima van financijskih transakcija s posebnom pažnjom posvećenom primjeni *blockchaina* u znanstvenoj zajednici te zaštiti i očuvanju digitalnih podataka. Iako je u pitanju vrlo mlada i neprovjerena tehnologija, njezin potencijal je neupitan. Zaključuje se kako je potrebno vrijeme za pronalazak odgovarajuće implementacije koja će biti sigurna i pouzdana.

KLJUČNE RIJEČI

Digitalni informacijski objekti, zaštita i očuvanje digitalnih podataka, autentičnost digitalnih podataka, informacijska privatnost, *blockchain*

1. UVOD

Zaštita i očuvanje informacijskih objekata predstavlja praksu pohrane informacijskih objekata na duljii vremenski rok pri čemu im je potrebno osigurati pristup i zadržati njihovu informacijsku vrijednost. Pri tome treba naglasiti kako zaštita i očuvanje informacijskih objekata istovremeno podrazumijeva i zaštitu podataka. Naime, svaki informacijski objekt čine podaci zapisani na nekom mediju, a pojam „informacijski“ predstavlja interpretiranu sadržajnu vrijednost tih podataka. Dakle, uspješnom zaštitom i očuvanjem podataka očuvat će se i informacijski objekti koje ti podaci tvore. Ovakvi postupci najčešće se vežu uz informacijske ustanove poput arhiva, knjižnica i muzeja. Međutim, činjenica je kako brojne organizacije imaju potrebu za strukturiranim i trajnim očuvanjem informacijskih objekata koji svjedoče o njihovim aktivnostima, te evidentiranjem svih eventualnih izmjena na njima kroz vrijeme. Konačni cilj je očuvanje podataka, odnosno informacijskih objekata koji su pouzdani i autentični, čiji je integritet očuvan te kojima se može pristupiti i upotrebljavati ih kroz razdoblje u kojem se čuvaju.

Prvi dio ovog rada bavi se pitanjima zaštite i očuvanja podataka u digitalnom dobu. Naime, dok se praksa zaštite i očuvanja analognih informacijskih objekata razvijala dugi niz godina prije nego je postala standardizirana i jasno definirana, dolazak digitalnog doba donio je nove oblike informacijskih objekata čije su značajke bile znatno drukčije od njihovih analognih ekvivalenata. Digitalni informacijski objekti sastoje se od nekoliko razina koje određuju njihove značajke te je njihove međusobne odnose potrebno očuvati. Međutim, i u digitalnom dobu temeljni je napor zaštite i očuvanja ostao isti – očuvati autentičnost i pouzdanost informacijskih objekata. Pitanje je koja su svojstva autentičnog informacijskog objekta, u kakvom se sustavu isti treba čuvati te koje su strategije dostupne za postizanje ovih ciljeva? Dodatno pitanje u digitalnom dobu veže se uz informacijsku privatnost. Očito je kako se podaci koje generira pojedinac mogu koristiti u nelegitimne svrhe. Uzimajući u obzir i težnju prelaska u digitalni oblak (eng. *cloud*), potencijalna meta nisu samo korisnički podaci već i podaci koji sačinjavaju informacijske objekte koji se trajno čuvaju. Postoji li rješenje ovog problema te kako zaštititi digitalne podatke od moguće zlouporabe?

Drugi dio rada bavi se pojašnjavanjem *blockchain* tehnologije. Ovaj se koncept pojavio u jeku svjetske financijske krize i implementacijom u Bitcoin sustav uspio je u kratkom roku preporoditi područje financija. Tehnologija iza Bitcoina pojašnjena je kroz razlaganje njezine arhitekture, gradivnih elemenata i osnovnih funkcija, a posebna se pažnja posvećuje načinu na koji se *blockchain* odnosi prema informacijskoj privatnosti i autentičnosti podataka. Postavlja se pitanje je li *blockchain* u sferi financija pronašao svoju najbolju primjenu ili postoje slučajevi u

kojima je primjena ove tehnologije prikladnija te može li *blockchain* unaprijediti praksu zaštite i očuvanja digitalnih podataka svojim inovativnim pristupom privatnosti i autentičnosti.

2. ZAŠTITA I OČUVANJE PODATAKA U DIGITALNOM DOBU

U studenom 1966., uslijed dugotrajnog kišnog perioda, Firenca biva pogođena prirodnom katastrofom kakva u povijesti grada nije zabilježena nekoliko stoljeća. Rijeka Arno izljeva se iz svog korita na ulice grada preplavljujući pritom podrume privatnih prostora, muzeja i knjižnica te utapajući stoljeća kulturne baštine u mulju i blatnoj vodi. Ovaj katastrofični događaj ostat će zapamćen ne samo među žiteljima grada, već i među stručnjacima u području zaštite i očuvanja kao katalizator globalnih promjena u zajednici.[1] Naime, kada su se u Firenci, zbog potreba sanacije štete nastale poplavom skupili stručnjaci iz cijelog svijeta, postalo je očito da su zaštita i očuvanje relativno nerazvijene u stručnom smislu – naučene samostalnim radom ili uz mentorstvo, s vrlo malim brojem materijala i tehnika poznatih svima u grupi.[2] Ovakav razvoj događaja naveo je zajednicu da zaštitu i očuvanje kulturne baštine krene promatrati kroz globalnu prizmu, prilikom čega se usredotočila na razvoj dijeljenih tehnika i smjernica kao i mogućih preventivnih mjera koje bi u budućnosti mogle u potpunosti ili barem djelomično spriječiti posljedice sličnih katastrofa.[3] U nadolazećim desetljećima struka zaštite i očuvanja materijalnih zapisa doživjela je transformaciju od stručne nerazvijenosti i samoukih odluka do prakse temeljene na uvriježenim standardima s posebnom pažnjom pridanom preventivnim mjerama. Može se pretpostaviti kako je dolazak digitalnog doba dodatno unaprijedio struku otvaranjem novih komunikacijskih kanala te olakšavanjem stvaranja i raspačavanja informacija. Međutim, pojava interneta i munjevit napredak tehnologije sa sobom su donijeli novi niz pitanja i problema – dok su materijalni zapisi imali relativno uvriježene prakse i pristupe očuvanju, došlo je do poplave digitalnim podacima i medijima za koje nisu vrijedila ista pravila.

Kako se digitalizirao svijet tako je i struka zaštite i očuvanja morala proći prilagodbe za suočavanje s nadolazećim izazovima. Stoga digitalna zaštita i očuvanje predstavlja dugoročnu pohranu digitalnih informacijskih objekata s mogućnošću pronalaženja i tumačenja podataka koji

[1] Usp. Conway, Paul. Preservation in the age of Google: digitization, digital preservation, and dilemmas. // Library Quarterly 80, 1(2010), str. 61. URL: https://deepblue.lib.umich.edu/bitstream/handle/2027.42/85223/J15%20Conway%20Preservation%20Age%20of%20Google%202010.pdf?sequence=1 (2018-07-21)
[2] Usp. Baker, Cathleen Ann. The Florence Flood, 1966: what we learned, 19. 12. 2016. URL: https://www.lib.umich.edu/blogs/beyond-reading-room/florence-flood-1966-what-we-learned (2018-07-20)
[3] Usp. Conway, Paul. Nav. dj, str 62.

čine te objekte kroz vremenski raspon u kojem su potrebni. Dugoročno u ovom slučaju označava razdoblje dovoljno dugo da se u njemu pojavljuju izazovi zastarijevanja tehnologije, podrške novih medija i formata te izmjena u korisničkim navikama.[4]

Masovna upotreba informacijskih tehnologija ubrzala je proces proizvodnje podataka, s gotovo eksponencijalnim rastom iz godine u godinu. Nije začuđujuća činjenica kako je 90 % podataka u svijetu stvoreno u zadnje dvije godine, odnosno kako se na dnevnoj razini proizvede 2,5 kvintilijuna bajtova podataka.[5] Stančić je na istom tragu kada se dotiče Mooreova zakona koji nalaže kako razvoj informacijske tehnologije udvostručuje računalnu snagu i gustoću zapisa na medije svake dvije godine.[6] Treba uzeti u obzir kako je dobar dio novoproizvedenih podataka nestrukturiran i nema pretjeranu arhivističku vrijednost, ali također treba naglasiti da količina podataka koju je potrebno očuvati na dulje razdoblje neizbježno raste. Sudbinu digitalnih podataka određuju brze promjene u načinima pohrane, formatima i tehnologijama koje prijete da njihov život u digitalnom dobu učine tegobnim, okrutnim i kratkim te se zaštiti i očuvanju digitalnih podataka moramo posvetiti u cjelosti – tehnički, legalno i organizacijski, kako bi ih bilo moguće prenijeti budućim generacijama.[7]

2.1. Karakteristike digitalnih podataka

Kako bi se bolje razumjele karakteristike i specifičnosti čuvanja digitalnih podataka potrebno je najprije definirati informacijske objekte. Bilo koje gradivo koje pruža određene informacije smatra se informacijskim objektom, pri čemu medij pohrane nije važan – informacijski objekt može biti i u digitalnom i u analognom obliku.[8] Dakle, informacijskim objektom može se smatrati znanstveni članak zapisan u PDF formatu, kao i bilješka na komadu papira.

[4] Usp. Reddy Kolle, Shankar et al. Strategies and techniques for preservation of digital resources. // PEARL: A Journal of Library and Information Science 8, 4(2014), str. 221. URL: https://www.researchgate.net/publication/273506866_Strategies_and_Techniques_for_Preservation_of_Digital_Resources (2018-07-25)

[5] Usp. Jacobson, Ralph. 2.5 quintillion bytes of data created every day. How does CPG & Retail manage it?, 24. 4. 2013. URL: https://www.ibm.com/blogs/insights-on-business/consumer-products/2-5-quintillion-bytes-of-data-created-every-day-how-does-cpg-retail-manage-it/ (2018-07-27)

[6] Usp. Stančić, Hrvoje. Arhivsko gradivo u elektroničkom obliku: mogućnosti zaštite i očuvanja na dulji vremenski rok. // Arhivski vjesnik 49, 1(2006), str. 110. URL: https://hrcak.srce.hr/index.php?show=clanak&id_clanak_jezik=9508 (2018-07-23)

[7] Usp. Marcum, Deanna. Introduction: the changing preservation landscape. // The state of digital preservation: an international perspective. Conference proceedings. Washington: Council on library and information resources, 2002. Str. 1-3. URL: https://www.clir.org/wp-content/uploads/sites/6/pub107.pdf (2018-07-27)

[8] Usp. Stančić, Hrvoje. Nav. dj. Str 109.

Nemoguće je pružiti jedinstvenu i jednoznačnu definiciju digitalnih informacijskih objekata – neki od njih u svojoj su suštini samo jednostavne transkripcije tradicionalnih informacijskih objekata poput knjiga, izvješća i listi, dok s druge strane postoji cijeli spektar informacijskih objekata koji ne mogu biti izraženi u tradicionalnim ili analognim medijima poput interaktivnih mrežnih stranica, virtualnih modela i računalnih igara.[9] Metode zaštite i očuvanja moraju se usmjeriti na promijenjivost i složenost digitalnih informacijskih objekata, no to ne mora nužno značiti da u svrhu zaštite i očuvanja mora biti sačuvano apsolutno svako svojstvo nekog objekta. Na primjeru periodnog sustava elemenata moguće je primjetiti kako neke osobine informacijskog objekta ipak imaju veći prioritet. Informacijska vrijednost periodnog sustava proizlazi iz tabličnog poretka kemijskih elemenata koji je odraz njihove atomske građe i svojstava, odnosno prostornog rasporeda elemenata. Taj bi se raspored mogao poremetiti ili u potpunosti uništiti ako bi se za tumačenje periodnog sustava koristio neprikladan program ili ako bi ga se pohranilo u neodgovarajućem formatu čime bi objekt u potpunosti izgubio svoju informacijsku vrijednost. S druge strane, ako bi se promijenila tipografija, odnosno font slova kojim su ispisana imena kemijskih elemenata u periodnom sustavu, a zadržao pravilan prostorni raspored elemenata, informacijska vrijednost objekta ne bi bila narušena budući da bi njegove temeljne značajke ostale očuvane.[10] Dakle, digitalni informacijski objekt predstavlja onaj informacijski objekt koji je nastao uz pomoć informacijske tehnologije, pri čemu njegov izvorni oblik može biti digitalan ili se može raditi o digitaliziranom objektu. Bez obzira na sadržaj i dodatne značajke, svaki se digitalni informacijski objekt može promatrati iz fizičke, logičke i konceptualne razine. Svaka od ovih razina ima određena svojstva čijom se analizom može prodrijeti u problematiku zaštite i očuvanja digitalnih informacijskih objekata, odnosno podataka koji zapisani na nekom mediju sačinjavaju takve objekte.[11]

Fizička razina predstavlja razinu zapisa digitalnog informacijskog objekta na neki medij. Dakle, svaki je objekt zabilježen jedinstvenim zapisom u binarnom sustavu, pri čemu će specifičnosti zapisa ovisiti o samom mediju. Fizička razina neovisna je o značenju, odnosno na njoj ne postoji razlika između teksta, slike, zvuka i slično – bitno je samo na koji način i na kojem mediju je objekt zapisan. Ovdje postaje očigledna razlika između analognih i digitalnih informacijskih objekata. Naime, pri očuvanju analognih informacijskih objekata bilo je dovoljno očuvati medij na kojem se nalazi zapis. Međutim, u slučaju digitalnih informacijskih objekata

[9] Usp. Thibodeau, Kenneth. Overview of technological approaches to digital preservation and challenges to coming years. // The state of digital preservation: an international perspective. Washington: Council on library and information resources, 2002. Str. 4. URL: https://www.clir.org/wp-content/uploads/sites/6/pub107.pdf (2018-07-27)
[10] Isto, str. 5.
[11] Usp. Stančić, Hrvoje. Nav. dj, str. 110.

sadržaj se može odvojiti od izvornog medija i prebaciti na jedan ili više drugih medija, ili promijeniti tehničko i programsko okruženje bez promjene medija na kojem se objekt nalazi.[12] Stoga su problemi očuvanja na fizičkoj razini uglavnom vezani uz trajnost, ali se u ovom kontekstu trajnost medija i trajnost zapisa na mediju mogu promatrati kao dvije odvojene cjeline.[13]

Nadalje, logička razina predstavlja način na koji će sadržaj biti fizički organiziran i zapisan. Jednom kada se podaci učitaju u memoriju, vrsta medija i način zapisa na medij potpuno gube važnost.[14] Na logičkoj razini moguće je razlikovati jednostavne i složene informacijske objekte. Na primjer, časopis u jednoj datoteci u PDF formatu predstavlja jednostavan objekt. S druge strane, časopis razdvojen u više datoteka u PDF formatu, prema člancima, predstavlja složeni objekt pri čemu mora postojati dodatni logički objekt koji će ukazati na pravilan redoslijed i služiti kao poveznica među člancima. Dakle, za očuvanje informacijskih objekata na logičkoj razini potrebno je očuvati podatke o njihovom prepoznavanju, redoslijedu i učitavanju.[15]

Treća razina digitalnog informacijskog objekta je konceptualna razina. Na ovoj razini se informacijski objekt prepoznaje kao smislena cjelina te tumači kao slika, tekst, zvuk itd. Sadržaj i struktura ove razine moraju biti sadržani u logičkoj razini gdje mogu biti različito organizirani što izavno utječe na njezino tumačenje. U suštini, ovisno o organizaciji na logičkoj razini, digitalni informacijski objekti će se na konceptualnoj razini tumačiti u različitim formatima.[16] Ovdje je moguće vidjeti još jedno bitno svojstvo digitalnih informacijskih objekata – na konceptualnoj razini mogu postojati različita digitalna enkodiranja istog objekta, odnosno, moguće je očuvati temeljne značajke objekta čak i promjenom njegova formata.[17]

Kako bi se digitalni informacijski objekt mogao očuvati potrebno je imati dostupne podatke o odnosima između fizičke, logičke i konceptualne razine. Recimo, ako bi se željelo pronaći izvješće razdvojeno na master dokument i nekoliko poddokumenata, moralo bi se znati da je informacijski objekt pohranjen na određen način te identitete svih njegovih logičkih komponenti. Dakle, da bi se digitalni informacijski objekt očuvao mora biti moguće identificirati i pronaći sve njegove digitalne komponente – sve logičke i fizičke objekte potrebne za rekonstrukciju konceptualnog objekta. U procesu zaštite i očuvanja digitalnih podataka mora biti očuvana

[12] Usp. Sannet, Shelby; Park, Eun. Authenticity as a requirement of preserving digital data and records. // IASSIST Quarterly 24 (2000), str. 15. URL: http://www.interpares.org/display_file.cfm?doc=ip1_dissemination_jar_sanett~park_iassist_quarterly_24_2000.pdf (2018-07-23)
[13] Usp. Stančić, Hrvoje. Nav. dj, str. 111.
[14] Usp. Thibodeau, Kenneth. Nav. dj, str. 7.
[15] Usp. Stančić, Hrvoje. Nav. dj, str. 112.
[16] Isto.
[17] Usp. Thibodeau, Kenneth. Nav. dj, str. 10.

mogućnost reprodukcije informacijskog objekta, to jest mogućnost pristupa objektu i njegova upotrebljivost ljudima i računalnim sustavima. Međutim, za uspješno očuvanje digitalnog informacijskog objekta nije uvijek nužno niti preporučljivo sačuvati nepromijenjene veze između fizičke i logičke razine. U nekim slučajevima postoji određena prednost u izmjenama na jednoj ili obje razine digitalnog informacijskog objekta, primjerice, pohranjivanju dokumenta iz MS Word formata u PDF format kako bi se spriječile neovlaštene izmjene na njemu. Također, prilikom zastarijevanja tehnologije i migracije na novi medij morat će doći do izmjena u načinu fizičkog bilježenja objekta. U slučaju analognih informacijskih objekata ovakve izmjene ne bi bile u skladu s principima očuvanja, međutim, u digitalnom svijetu ovi su koncepti znatno fleksibilniji i ponekad nužni za očuvanje na dulji rok.[18] U konačnici, ne postoji recept koji jasno definira koje izmjene na određenim razinama digitalnog informacijskog objekta treba provesti za njegovo očuvanje. Evidentno je kako sve izmjene moraju zadržati mogućnost pristupa sadržaju, međutim treba naglasiti kako je pristup višeslojan koncept te se ne odnosi samo na mogućnost fizičkog pregleda već i zadržavanje autentičnosti informacijskog objekta, odnosno podataka koji čine takve objekte.

2.2. Očuvanje autentičnosti digitalnih podataka

Autentičan informacijski objekt je objekt za koji se može dokazati da jest ono što tvrdi da jest, da ga je poslala ili stvorila osoba za koju tvrdi da ga je poslala ili stvorila te da je stvoren ili poslan kada tvrdi da jest. K tomu možemo dodati dimenzije pouzdanosti, integriteta i upotrebljivosti. Pri čemu je objekt pouzdan onda kada se njegovom sadržaju može vjerovati kao točnom prikazu transakcija, aktivnosti ili činjenica kojima je svjedočio i na koji se može osloniti u budućim transakcijama ili aktivnostima. Nadalje, integritet se odnosi na cjelovitost i nepromijenjenost informacijskog objekta pri čemu ga je potrebno zaštititi od neovlaštenih izmjena, odrediti koji mu se dodaci i bilješke mogu pridružiti nakon njegova stvaranja, pod kojim uvjetima i tko je ovlašten za njihovo dodavanje. U konačnici svi odobreni dodaci i izmjene moraju biti eksplicitno naznačeni i provjerljivi. Upotrebljiv informacijski objekt jest onaj koji se može pronaći, pročitati, prikazati i tumačiti pri čemu njegovo naknadno prikazivanje mora biti moguće kao povezano s aktivnosti u okviru koje je nastao. Kontekstualne veze objekata moraju nositi informacije koje su potrebne za razumijevanje aktivnosti prilikom kojih su stvoreni i korišteni. Dakle, upotrebljivost informacijskog objekta odnosi se na njegovu pravilnu indeksiranost, održavanje uspostavljenih odnosa između fizičke i logičke razine te mogućnost njihovog pravilnog tumačenja u

[18] Isto, str. 11-13.

konceptualnoj razini, kao i prisutnost svih dodatnih logičkih objekata koji upućuju na redoslijed u složenim informacijskim objektima.[19]

U povijesnom kontekstu autentičnost je proizlazila iz okolnosti u kojima je informacijski objekt stvoren – prisutnost autorova potpisa i potpisa svjedoka indicirala je autentičnost.[20] Međutim, autentičnost digitalnih informacijskih objekata razlikuje se od autentičnosti njihovih analognih ekvivalenata. Prema Thibodeau, idealan sustav za zaštitu i očuvanje bio bi neutralni komunikacijski kanal za prijenos informacija u budućnost, što znači da sustav ni u kom slučaju ne bi smio oštetiti informacijske objekte koji se u njemu čuvaju. Takav sustav možemo zamisliti kao crnu kutiju u koju ulaze nizovi bitova kojima možemo pristupiti u bilo kom trenutku. Ako je sustav pouzdan bilo koji informacijski objekt koji se u njemu čuvao i kojem se kasnije pristupilo bit će autentičan.[21] Dakle, fizičke i logičke razine informacijskog objekta u idealnom bi slučaju morale ostati nepromijenjene od trenutka kada je objekt pohranjen u sustav te kroz cijelo razdoblje u kojem ga se čuva. Međutim, jasno je kako je takvo što u kontekstu digitalnih informacijskih objekata nemoguće te da će se u nekom trenutku na nekoj od razina morati provesti radnje kojima će se osigurati pristup i pravilno tumačenje objekata kroz vrijeme. To znači da je iz perspektive kasnijeg pristupa znatno bitnije očuvati prohodnost od fizičke do konceptualne razine informacijskog objekta od trenutka njegova unosa u sustav do trenutka eventualnog pristupa.[22]

U obzir treba uzeti da će čak i na fizičkim informacijskim objektima vremenom doći do promjena, bile one željene ili ne – papir može izmijeniti svoja kemijska svojstva, tinta može izblijedjeti. U skladu s time, bez obzira je li okruženje digitalno ili analogno, uz autentičnost je potrebno vezati i dimenziju povjerenja. Ne postoji apsolutno jamstvo da informacijski objekt nije bio modificiran u razdoblju u kojem ga se čuva, stoga mora postojati određena razina povjerenja u osobu, organizaciju, sustav ili metodu da će informacijski objekt kojem se pristupa doista biti autentičan.[23] Također, kriteriji autentičnosti u konačnici će ovisiti o namjeni objekta. Ako bi se željelo znati je li neki dokument autentičan primjerak rukopisa nekog autora, moralo bi ga se usporediti s drugim poznatim rukopisima istog autora. U ovom bi slučaju kriterij bio vizualni izgled teksta. Međutim, u slučaju da bi se željelo provjeriti autentičnost autorovih misli, izgled rukopisa ne bi bio značajan već bi se pažnja preusmjerila na sadržaj i stil pisanja. Budući da

[19] Stančić, Hrvoje. Nav. dj, str. 113-114.
[20] Usp. Rogers, Corinne. Authenticity of digital records: a survey of professional practice. // Canadian journal of information and library science 39, 2(2015), str. 99. URL: https://muse.jhu.edu/article/590936/summary (2018-07-30)
[21] Usp. Thibodeau, Kenneth. Nav. dj, str. 13.
[22] Usp. Stančić, Hrvoje. Nav. dj, str. 113.
[23] Usp. Thibodeau, Kenneth. Nav. dj, str. 14.

informacijske ustanove poput arhiva i knjižnica ne mogu propisati niti predvidjeti sve moguće upotrebe informacijskih objekata koje čuvaju, one svoje zbirke održavaju za univerzalni pristup iz bilo kojeg razloga. Uzme li se u obzir priroda digitalnih informacijskih objekata i njihove značajke, potrebno je definirati model neovisan o pohranjenom objektu koji će služiti kao kriterij za potrđivanje autentičnosti infromacijskog objekta kojem se pristupa.[24] Objekt je autentičan onda kada se može dokazati da je potpuno isti kao i prvi put kada je pohranjen u sustav te ako je njegova pouzdanost ostala nepromijenjena od trenutka kada je dostavljen.[25] Treba naglasiti kako se „potpuno isti" prije svega odnosi na nepromijenjen sadržaj informacijskog objekta budući da su izmjene na fizičkoj i logičkoj razini neizbježne. U konačnici se postavlja pitanje na osnovu kojih načela se uspostavlja sustav za zaštitu i očuvanje digitalnih informacijskih objekata, odnosno podataka koji sačinjavaju takve objekte. Uz to je potrebno razlučiti i koje su metode dostupne kako bi se pravilno mogla očuvati autentičnost podataka pohranjenih u takvom sustavu?

2.3. Kriteriji i strategije očuvanja digitalnih podataka

Zaštita i očuvanje digitalnih podataka iziskuju temeljito planiranje, obrazovanje kadrova i pronalazak ravnoteže između težine implementacije metode, njezine trajnosti te troškova održavanja i eventualnih izmjena kroz vrijeme. Ako je cilj sustava očuvati autentičnost i mogućnost pristupa digitalnim informacijskim objektima, odnosno podacima koji ih sačinjavaju, potrebno je zadovoljiti četiri osnovna kriterija – izvodljivost, održivost, praktičnost i prikladnost.

Izvodljivost se odnosi na tehničko i programsko okruženje sposobno za podršku određene metode zaštite i očuvanja digitalnih podataka. Tehničko okruženje predstavlja materijalnu osnovu na kojoj će se sustav pokretati te ovisno o kontekstu mora zadovoljiti kriterije potrebne za primjerenu obradu podataka i uključiti sve ulazno-izlazne uređaje i periferiju potrebnu za pravilno funkcioniranje sustava. S druge strane, programsko okruženje predstavlja sve nematerijalne elemente poput operativnog sustava i aplikacija koji moraju podržavati sve definirane funkcionalnosti.[26]

Nadalje, održivost se odnosi na dugoročnost metode, odnosno odgovara na pitanje može li se specifična metoda primjenjivati na neodređeno ili je moguće argumentirano pretpostaviti da će

[24] Isto, str. 14-15.
[25] Usp. Stančić, Hrvoje. Nav. dj, str. 115.
[26] Usp. Thibodeau, Kenneth. Nav. dj, str. 15.

postojati njezin logičan nastavak.[27] Na ovaj se način pokušava izbjeći bezizlazna situacija do koje može doći zastarijevanjem tehnologije pri čemu bi se metoda morala ili potpuno napustiti, što bi značilo implementiranje sustava iz početka, ili bi zahtijevala dodatne troškove kako bi ju se učinilo održivom.

Zatim je potrebno zadovoljiti kriterij praktičnosti koji nalaže da metoda treba biti unutar razumnih ograničenja težine i troškova implementacije. Ovdje se radi o pronalaženju ravnoteže između idealne implementacijske metode, stvarnih mogućnosti te zahtjeva gradivnih elemenata poput tehničkog i programskog okruženja. U konačnici, kriterij prikladnosti ovisi o tipovima informacijskih objekata i specifičnim ciljevima njihove zaštite i očuvanja te će voditi donošenje odluke o najpogodnijim strategijama[28]. Niti jedna od niza dostupnih strategija nije savršena niti u potpunosti otporna na slabe točke zaštite i očuvanja digitalnih podataka, ali uz prikladnu implementaciju i metodičnost moguće je osigurati neometan pristup pohranjenim informacijskim objektima kroz vrijeme.

Bez obzira koju strategiju zaštite i očuvanja odabrali Williamson naglašava važnost dokumentacije procesa. Tako je moguće osigurati dugoročnu dostupnost informacija o tehničkim odlukama donesenim tijekom stvaranja, pohrane i održavanja sustava kao i kadrovskom znanju.[29] Ove dokumentacija bit će od posebne koristi u slučajevima kada dođe do pogrešaka i kvarova u sustavu, ali i prilikom edukacije novopridošlih kadrova. Čak i da se potreba za dokumentacijom ukaže vrlo rijetko ili nikad, šanse za neometan proces zaštite i očuvanja digitalnih podataka bit će znatno veće ako ga se ispravno dokumentira. Dakle, odabir primjerene strategije ovisit će o ispunjavanju prethodno navedenih kriterija i prirodi informacijskih objekata koji se čuvaju. Neke od najučestalijih strategija su: osvježavanje medija, migracija, replikacija, izrada sigurnosnih kopija, emulacija, enkapsulacija i očuvanje same tehnologije.

Osvježavanje medija odnosi se na periodičko prenošenje digitalnog sadržaja na nove medije za pohranu. Pri osvježavanju medija najčešće dolazi do promjena na fizičkoj razini informacijskog objekta, budući da različiti mediji imaju različite tehnike bilježenja bitova. Međutim, postoji koncept „modificiranog osvježavanja“ pri čemu se podaci prenose na medij koji je dovoljno sličan trenutnom kako bi se osigurala nepromijenjenost niza bitova koji tvori informacijski objekt.[30] Bez obzira dolazi li do izmjena na fizičkoj razini, osvježavanjem medija

[27] Isto.
[28] Isto.
[29] Usp. Williamson, Andrew. Strategies for managing digital content formats. // Library Review 54, 9(2005). URL: https://strathprints.strath.ac.uk/2295/1/strathprints002295.htm (2018-07-24)
[30] Usp. Reddy Kolle, Shankar et al. Nav. dj, str. 223.

adresiraju se fizičko propadanje i zastarijevanje tehnologije kako bi se nastavio neometan pristup informacijskim objektima kroz određeno razdoblje a ova strategija često se provodi u kombinaciji s migracijom.[31]

Migracija predstavlja prebacivanje digitalnog sadržaja u formate koji se mogu tumačiti pomoću suvremenih tehničkih i programskih rješenja čime se pokušava izbjeći gubitak mogućnosti pristupa podacima uzrokovan zastarijevanjem formata. Pored prenošenja iz formata u format migracija također može uključivati prijenos iz operativnog sustava u operativni sustav, ali i iz programskog jezika u programski jezik. Budući da je nemoguće napraviti točnu kopiju informacijskog objekta postoji rizik gubitka pojedinih funkcionalnosti jer dolazi do izmjena na logičkoj razini. Takvi se gubitci pokušavaju izbjeći pa se migracija usmjerava na očuvanje integriteta informacijskog objekta kako bi se njegove ključne značajke mogle pravilno tumačiti u novom okruženju.[32]

Nadalje, replikacija označava dupliciranje podataka na više sustava na različitim lokacijama. Dupliciranje se može odvijati sinkrono ili asinkrono, odnosno u stvarnom vremenu ili s odgodom, ali obje metode će proizvesti identičnu kopiju informacijskog objekta na udaljenoj lokaciji. Replikacija je vrlo slična izradi *backupa*, odnosno sigurnosne kopije, koja također predstavlja stvaranje digitalnih kopija, ali čini to tako da se nove kopije objekata stvaraju periodički kroz njihov životni vijek.[33] Dakle replikacija će uvijek proizvesti jedan duplikat objekta pri čemu će on sadržavati sve prethodne izmjene i dodatke na objektu. S druge strane, stvaranjem sigurnosne kopije će se kreirati više duplikata objekta u kronološkom slijedu pri čemu će svaki novi duplikat sadržavati sve izmjene iz prethodnih duplikata te posljednje izmjene na informacijskom objektu. Cilj replikacije i kreiranja sigurnosnih kopija je čuvanje duplikata podataka na udaljenim lokacijama u slučaju prirodnih katastrofa i kvarova na tehničkom i/ili programskom okruženju na kojima je sustav implementiran.

Zatim je dostupna strategija emulacije, odnosno oponašanja zastarjelih tehničkih okruženja, aplikacija i operativnih sustava izradom prilagođenog programskog rješenja. Emulacija se primjenjuje u slučajevima kada ne postoji mogućnost tumačenja objekta u okruženju temeljenom na suvremenoj arhitekturi jer bi se migracijom u drugi format izgubila mogućnost pristupa. Primjeri takvih objekata često su retro računalne igre koje zahtijevaju zastarjele arhitekture za pravilno pokretanje. Velik problem emulacije je dugoročnost – emulatori nisu

[31] Usp. Isto.
[32] Isto.
[33] Usp. Williamson, Andrew. Nav. dj.

otporni na zastarijevanje te, kao i informacijski objekti koji se na njima pokreću, zahtijevaju prilagodbe kako bi funkcionirali u različitim okruženjima što može iziskivati dodatne troškove i dovesti u pitanje održivost operacije.[34]

Enkapsulacija je ključni element emulacije. Ona predstavlja tehniku kojom se izbjegavaju ranjivosti digitalnih formata tako da se grupira informacijski objekt i podatke potrebne za njegovo tumačenje poput identifikatora, metapodataka i programskih specifikacija.[35] Dakle, prilikom enkapsulacije čuvaju se svi odnosi na logičkoj razini kako bi se prilikom kasnije dekapsulacije objekta isti mogao pravilno reproducirati u konceptualnoj razini.

U konačnici, očuvanje tehnologije predstavlja čuvanje digitalnog informacijskog objekta zajedno sa svim tehničkim i programskim rješenjima potrebnim za pristup objektu. Dakle, umjesto emuliranja na suvremenim tehničkim i programskim rješenjima, institucije moraju izdvojiti znatna sredstva za nabavljanje dijelova te održavanje licenci. Očito je da ova strategija nije dugoročno održiva jer se rezervni dijelovi više ne proizvode, a njihova postojeća zaliha iščezava. U skladu s time, pitanje je vremena kada se pristup digitalnom informacijskom objektu može zauvijek izgubiti.[36]

U posljednjem se desetljeću kao dodatna strategija pojavila mogućnost zakupljivanja infrastrukture potrebne za zaštitu i očuvanje digitalnih podataka od vanjskih pružatelja usluga kroz korištenje *cloud* servisa. Neovisno o tome jesu li u pitanju pojedinci ili institucije, vidljiv je trend u porastu korištenja ovakvih usluga. Tome svjedoče predviđanja poput onog da je 2013. manje od 20 % digitalnih podataka bilo pohranjeno u *cloudu*, te da se do 2020. očekuje da će ta brojka biti dvostruko veća.[37] Slične prognoze 2012. dala je i agencija Gartner, jedna od vodećih istraživačkih i savjetodavnih tvrtki, navodeći da će korisnici više od trećine svojih podataka pohranjivati u *cloudu* do 2016.[38] Ovakvi servisi donekle uklanjaju jednu od dimenzija kriterija praktičnosti, a to je težina implementacije budući da infrastruktura već postoji. Međutim, postavlja se pitanje jesu li *cloud* servisi konačno rješenje svih problema zaštite i očuvanja digitalnih podataka ili ispod površine postoje mogući problemi koji bi te napore mogli otežati.

[34] Usp. Reddy Kolle, Shankar et al. Nav. dj, str. 223.
[35] Isto, str. 224.
[36] Isto.
[37] Usp. Rogers, Corinne. Nav. dj, str. 99.
[38] Usp. Verma, Shalini. Forecast: consumer digital storage needs, 2010-2016, 2012. URL: http://www.gartner.com/newsroom/id/2060215 (2018-09-05)

2.4. Čuvanje digitalnih podataka u oblaku

Računalni *cloud* ili oblak predstavlja skup dijeljenih računalnih resursa koji uključuje i prostor za pohranu. Većina ovakvih servisa javnosti je dostupna na mreži a u vlasništvu je tehnoloških divova poput Amazona, Googlea i sl. *Cloud* usluge dostupne su na zahtjev putem javnih mreža, bez potreba za nabavkom opreme i procesom konfiguracije. Uz to mogu ponuditi dodatne kapacitete ako se za to ukaže potreba pri čemu naplaćuju samo prostor za pohranu koji se koristi.[39] Osnovna funkcija *cloud* servisa je replikacija digitalnih podataka s jednog ili više medija te pohrana njihovih duplikata na udaljene lokacije. Dok će standardnom korisniku najčešće biti dovoljne osnovne funkcionalnosti jednog takvog servisa, oni koji pružaju usluge zaštite i očuvanja digitalnih podataka institucijama moraju omogućiti ne samo pristup, nego i upravljanje informacijskim objektima koji su u aktivnoj pohrani.[40]

Iz institucionalne perspektive ovakvi servisi mogu ponuditi brojne prednosti, posebice u slučajevima manjih arhiva s ograničenim proračunima. Prije svega, korisnici *clouda* mogu očekivati da će se njihov sustav temeljiti na suvremenoj infrastrukturi o čijim nadogradnjama i održavanju neće morati voditi računa niti izdvajati sredstva, što je velika prednost naspram institucionalnog rasta koji je često ograničen, spor i reaktivan. Također je moguće osloniti se na iskustvo pružatelja usluga u upravljanju velikim skupovima podataka što bi, uzmu li se u obzir potrebe za obrazovanjem kadrova i periodičkih nadogradnji na lokalnom sustavu, potencijalno moglo biti jeftinije.[41] U konačnici, replikacija koja se odvija u *cloudu* u potpunosti je automatizirana te je uz osnovnu uslugu moguće dodati pristup dodatnim alatima i procedurama implementiranim za specifične potrebe institucije.[42]

S druge strane, ovakav pristup zaštiti i očuvanju digitalnih podataka sa sobom nosi i brojne izazove. Prije svega, postavlja se pitanje životnog vijeka tehnologije na kojoj je *cloud* zasnovan, ali, još bitnije, pružatelja usluge. Budući da se radi o informacijskim objektima koji se čuvaju dugoročno, pitanje je što bi se dogodilo s podacima u slučaju propasti pružatelja? Pored toga, iako neizgledno, kako bi se podaci pohranjeni u *cloudu* mogli povratiti u slučaju kvara u njegovoj cjelokupnoj infrastrukturi? K tomu treba dodati i pitanja autorskih prava – potrebe za dodatnim

[39] Usp. Cloud services. // Digital preservation handbook. URL: https://www.dpconline.org/handbook/technical-solutions-and-tools/cloud-services (2018-07-25)
[40] Usp. Oliver, Gillian; Knight, Steve. Storage is a strategic issue: digital preservation in the cloud. // D-Lib Magazine 21, 3/4(2015). URL: http://www.dlib.org/dlib/march15/oliver/03oliver.html (2018-07-25)
[41] Isto.
[42] Usp. Cloud services. // Digital preservation handbook. URL: https://www.dpconline.org/handbook/technical-solutions-and-tools/cloud-services (2018-07-25)

licencama, pravo pružatelja usluge da podatke koristi za svoje potrebe te pitanje vlasništva nad podacima nastalim u novom okruženju.[43] Ovo su, naravno, problemi koji se rješavaju ovisno o zasebnom slučaju, a na tražiteljima usluga je da jasno definiraju svoje potrebe i osiguraju primjerenu zaštitu i očuvanje digitalnih podataka.

Međutim, na jedno od pitanja nije toliko jednostavno odgovoriti, a to je pitanje privatnosti podataka i zaštite sadržaja informacijskih objekata u ovakvim servisima. Pritom se ne radi samo o korisničkim podacima poput imena i lozinki, već osjetljivim podacima koji sačinjavaju informacijske objekte koji se čuvaju kao i podacima koji se mogu povezati s pojedincima i ugroziti njihovu dobrobit. Nesumnjivo je da u svakom sustavu postoje mehanizmi namijenjeni rješavanju ovakvih problema, no možemo li u potpunosti vjerovati da ti mehanizmi mogu pružiti potpunu privatnost podataka i zaštitu kako od vanjskih napada tako i od unutarnjih sudionika? Ovdje se ponovno dolazi do dimenzije povjerenja budući da, kao i u slučaju autentičnosti podataka, ne postoji apsolutno jamstvo da je privatnost u nekom sustavu očuvana. Dakle, potrebno je imati dozu povjerenja u sustav, osobu ili organizaciju da će svoj posao obavljati savjesno. Međutim, živimo u dobu kada nas vlastiti uređaji snimaju, prisluškuju i prate, kada smo svakodnevno okruženi ciljanim reklamama, a državne institucije putem nadzornih kamera na ulicama skeniraju i prepoznaju lica građana. Može li se doista vjerovati nekom tko jamči informacijsku privatnost, kako ju zaštititi i što koncept informacijske privatnosti uopće predstavlja?

3. INFORMACIJSKA PRIVATNOST

Neumoljiv napredak tehnologije pružio je mnoge prednosti koje čovječanstvo svakodnevno uživa. Pojavom interneta otvorila su se vrata u svijet, informacije nikada nisu bile dostupnije, a kontakt s najudaljenijim lokacijama nikada nije bio lakši. Kroz samo nekoliko godina *Web* 2.0 pružio je nove dimenzije interakcije s mrežom, društveni mediji su omogućili stotine novih „prijateljstava“ a koncept velikih podataka (eng. *big data*) bio je relativno nov. Tehnologija je uznapredovala toliko da je čovječanstvu svijet stavila u dlanove putem pametnih telefona, internet stvari (eng. *Internet of Things*) je otvorio komunikacijske kanale između svih uređaja, a e-Vlada je pružila biometrijske putovnice i administraciju preselila na mrežu. Danas se podaci pohranjuju i obrađuju na razini eksabajta (10^6 GB) – ilustracije radi, kada bi se pokušalo pohraniti 100 eksabajta na CD-

[43] Isto.

e kapaciteta 720 megabajta slažući ih jedan na drugi, izgradio bi se toranj koji bi dosegao Mjesec.[44] Facebook je u manje od dva desetljeća skupio 300 petabajta (3 x 10^9 GB) podataka što je 100 puta više od količine podataka koju je Kongresna knjižnica uspjela akumulirati u 200 godina.[45] Pojedinci danas svoje privatne podatke svojevoljno dijele za mrežne usluge, profilira ih se pomoću aktivnosti na mreži i gotovo je u svakom trenutku moguće znati gdje su. Čini se kako je privatnost zamijenjena za apsolutnu povezanost ali treba naglasiti kako takav slijed događaja nije bio stoljetni plan neke orvelijanske organizacije – *World Wide Web* današnjice nije se mogao predvidjeti, a u trenutku kada je otvoren široj javnosti njegov je rast izmakao kontroli te se pitanja poput privatnosti više nisu mogla rješavati kroz dizajn već naknadno i reaktivno.[46] Međutim, znači li to da je manjak privatnosti inherentan tehnološkom napretku ili postoje načini da se neke prošle greške isprave?

Privatnost se najčešće razdvaja na dvije dimenzije – konstitutivnu, odnosno ustavnu te informacijsku. Ustavna privatnost odnosi se na slobodu pojedinca u donošenju odluka o intimnim i osobnim situacijama bez uplitanja drugih.[47] Dakle, u slučaju ustavne privatnosti u pitanju nije privatnost podataka nekog pojedinca već pravo na emocionalni spokoj i pravo da se ga se „ostavi na miru“[48]. S druge strane nalazi se koncept informacijske privatnosti, odnosno legitimnog interesa pojedinaca za kontroliranjem pristupa osobnim podacima, koji je u tehnološkom kontekstu znatno bitniji. U normativnom smislu informacijska privatnost se odnosi na moralno pravo osobe da izravno kontrolira pristup svojim privatnim podacima, situacije u kojima bi drugi mogli doći do tih podataka te tehnologiju koja se može koristiti za generiranje, obradu i raspačavanje takvih podataka. Pojam osobnih podataka ovdje se odnosi na sve podatke čijom se analizom može identificirati pojedinca – bilo da se radi o kupovnim navikama, religijskoj opredijeljenosti, medicinskim nalazima i sl. Iako se u literaturi informacijska privatnost konceptualizira na nekoliko različitih načina, u kontekstu tehnologije najkorisniji je koncept zaštite podataka budući da, kao i s njihovom zaštitom i očuvanjem, postoji jasna slika objekta koji se želi zaštititi.[49]

---

[44] Usp. Privacy and information technology. // Stanford encyclopedia of philosophy, 20. 11. 2014. URL: https://plato.stanford.edu/entries/it-privacy/ (2018-07-30)
[45] Usp. Zyskind, Guy; Nathan, Oz; Pentland, Alex. Decentralizing privacy: using Blockchain to protect personal data. // 2015 IEEE Security and Privacy Workshops. San Jose: IEEE, 2015. Str. 180. URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7163223 (2018-08-02)
[46] Usp. Privacy and information Technology. Stanford encyclopedia of philosophy, 20. 11. 2014. URL: https://plato.stanford.edu/entries/it-privacy/ (2018-07-30)
[47] Isto.
[48] Usp. Rights of privacy. // Encyclopaedia Britannica Online. Encyclopedia Britannica. URL. https://www.britannica.com/topic/rights-of-privacy (2018-08-02)
[49] Usp. Privacy and information Technology. // Stanford encyclopedia of philosophy, 20. 11. 2014. URL: https://plato.stanford.edu/entries/it-privacy/ (2018-07-30)

Neupitno je da se istu tehnologiju koja nam je oduzela privatnost može koristiti kako bi se ista poboljšala, ali težnja tehnološkog napretka je upravo suprotna. Divovi poput Googlea i Facebooka ulažu nezamisliva sredstva u infrastrukturu za prikupljanje, čuvanje i analizu podataka koje korisnici svakodnevno generiraju služeći se njihovim servisima. Ovdje se ipak ne radi o klasičnoj zaštiti i očuvanju podataka jer je arhivistička vrijednost osobnih podataka milijuna korisnika upitna. S druge strane, novčana vrijednost tih podataka je nesporna – osobni podaci postali su valuta digitalnog doba.[50] Postoje dvije klasične reakcije na ovakav razvoj događaja. Jedan tabor, uglavnom sačinjen od IT-jevaca tvrdi da u digitalnom dobu ne postoji koncept privatnosti te da se društvo na to može samo navići. S druge strane, često se može čuti kako se nalazimo u dobu kada je privatnost pojedinca bitnija no ikad te da se nešto mora poduzeti kako ne bi potpuno nestala.[51]

Ironično je što se pitanjima privatnosti bavilo prije nego što je digitalni svijet današnjice uopće bio zamisliv. Tako je pravo na privatnost definirano još 1948. u UN-ovoj Univerzalnoj deklaraciji ljudskih prava, i dvije godine kasnije, 1950., u Europskoj konvenciji o ljudskim pravima. Međutim ovi se problemi ne mogu riješiti zakonodavstvom, jer ono napreduje na razini godina, a tehnologija na razini mjeseci.[52] Treba dodati i kako se većina istraživanja informacijske privatnosti odnosi na pojašnjavanje i predviđanje teorijskih doprinosa s malim brojem studija usredotočenih na dizajn.[53] Očito je kako zakoni i teoretiziranje nisu dovoljni za zaštitu privatnosti podataka u digitalnom dobu – u 21. stoljeću izazov je osigurati da se tehnologija dizajnira tako da se zahtjeve privatnosti uključi u programska rješenja, arhitekturu, infrastrukturu i poslovne procese.[54] Ovakav pristup rješavanju problema privatnosti naziva se privatnost kroz dizajn a zasnovan je na proaktivnim mjerama i preventivnim radnjama pri čemu je jamstvo privatnosti zadana postavka bilo kog sustava. Privatnost je sastavnica od samog početka te je ugrađena u dizajn u kojem je potpuno funkcionalna te omogućuje nedvosmislenu i potpunu sigurnost.[55]

---

[50] Usp. Dorraji, Seyed Ebrahim; Barcys, Mantas. Privacy in digital age: dead or alive?!: regarding the new EU data protection regulations. // Social technologies 4, 2(2014), str. 309. URL: https://www3.mruni.eu/ojs/social-technologies/article/view/2047/3805 (2018-08-02)

[51] Usp. Privacy and information Technology. // Stanford encyclopedia of philosophy, 20. 11. 2014. URL: https://plato.stanford.edu/entries/it-privacy/ (2018-07-30)

[52] Usp. Isto, str. 308-313.

[53] Usp. Belanger, France; Crossler, Robert E. Privacy in the digital age: a review of information privacy research in information systems. // MIS Quarterly 35(2011), str. 1019. URL: https://www.researchgate.net/publication/220259962_Privacy_in_the_Digital_Age_A_Review_of_Information_Privacy_Research_in_Information_Systems (2018-08-02)

[54] Usp. Privacy and information Technology. // Stanford encyclopedia of philosophy, 20. 11. 2014. URL: https://plato.stanford.edu/entries/it-privacy/ (2018-07-30)

[55] Usp. Dorraji, Seyed Ebrahim; Barcys, Mantas. Nav. dj. Str. 314.

Međutim, čak i u sustavu iz temelja dizajniranom s privatnošću na umu, i dalje postoji neizbježna dimenzija povjerenja. Korisnik mora imati određenu dozu povjerenja da će se njegova privatnost poštivati od strane sustava, odnosno ljudi koji rade unutar tog sustava. Dakle, kao i u slučaju očuvanja autentičnosti, između krajnjeg korisnika i njegova cilja na mreži mora postojati neki posrednik. Problematika posredovanja ne proizlazi iz samog čina, već ljudskog čimbenika – ljudi su nepredvidivi, s potencijalnim skrivenim namjerama koje je nemoguće provjeriti niti dokazati, a koje se mogu negativno odraziti na krajnjeg korisnika. Posredovanje je kao paradigma postojalo prije pojave interneta i u svom se nepromijenjenom obliku preselilo na mrežu. Napori da se ova paradigma izmijeni postojali su i ranije, ali do prave promjene koja će se pretvoriti u globalnu opčinjenot doći će u jeku svjetske financijske krize 2008. godine.

4. BITCOIN REVOLUCIJA

2008. godinu će uz standardna geopolitička previranja i prijetnje globalnog terorizma obilježiti ekonomska kriza kakvu SAD i svijet nisu osjetili još od Velike depresije. Ono što je započelo kao nestabilnost na američkoj burzi brzo se širi na ostatak svijeta zahvaljujući globalizaciji financijskih ekonomskih sustava. Nepravilnosti u financijskom sustavu vrlo brzo postaju očite te započinje potraga za krivcima. Kako je došlo do smanjene proizvodnje dobara i usluga, smanjenja potrošnje energije te štednje i ulaganja, javnost odgovorne pronalazi u financijskim institucijama i vladama te njihovom manjku regulative financijskog sustava.[56] S druge strane, mnogi smatraju kako akademska zajednica treba snositi odgovornost jer nije bila sposobna razumjeti niti voditi modernu ekonomiju.[57] Ovakvo međusobno okrivljavanje i potraga za odgovornima nikada nisu urodili plodom. Iste se godine, gotovo kao reakcija na nedostatan financijski sustav, na mreži pojavljuje manifest „*Bitcoin: A Peer-to-Peer Electronic Cash System*“ objavljen od strane nepoznatog autora ili grupe autora pod pseudonimom Satoshi Nakamoto. Nakamotov rad, objavljen u stilu znanstvenog članka, okrenuo je poimanja tradicionalnog financijskog sustava naglavce nudeći rješenje za radikalne ideje poput potpune eliminacije trećih strana – posrednika, u novčanim transakcijama na mreži. Naime, dok u fizičkom okruženju nisu postojali problemi ireverzibilnih transakcija, troškova posredovanja i nemogućnosti manjih transakcija, do tada nije postojao

[56] Usp. Zych, Izabela...[et al.]. Causes and solutions for the economic crisis according to the International Scientific Community. // Universitas Psychologica 14, 1(2015), str. 368. URL: http://revistas.javeriana.edu.co/index.php/revPsycho/article/view/6105/10622 (2018-08-05)

[57] Usp. Toarna, Alina; Cojanu, Valentin. The 2008 Crisis: causes and future direction for the academic research. // Procedia Economics and Finance 27(2015), str. 386. URL: https://www.sciencedirect.com/science/article/pii/S2212567115010102 (2018-08-05)

elektronički financijski sustav bez nekog oblika posredovanja. Dakle, bilo koja transakcija na mreži zahtijevala je tri strane – osobu A koja je slala novac, osobu B koja je novac primala, i osobu ili instituciju C koja je bila zadužena za osiguranje transakcije između osoba A i B, pri čemu je osoba C uzimala određenu proviziju od transakcije u svrhu osiguravanja iste te održavanja sustava. Nakamoto je predložio, konceptualizirao i implementirao sustav zasnovan na kriptografskim dokazima umjesto povjerenju koji je omogućavao izravne transakcije između subjekata bez potrebe za trećom stranom.[58] Taj sustav danas je poznat kao Bitcoin – kriptovaluta koja je od svog začeća 2009. izašla iz mračnih uglova mreže i ušla u javnu sferu s porastom vrijednosti od 5000 % do 2016. godine.[59] Međutim, ispostavilo se kako je algoritamska mreža iza Bitcoin valute samo jedna od mnoštva mogućih primjena Nakamotovih ideja koje su vremenom proširene izvan prvotno definirane primjene te su danas, desetljeće kasnije, poznate svijetu kao *blockchain*.

4.1. Gradivni elementi *blockchaina*

U svojoj suštini *blockchain* je distribuirana baza podataka, zasnovana na *peer-to-peer* arhitekturi (vezi ravnopravnih računala), koja sadrži rastuću listu, odnosno lanac, zapisa ili blokova zaštićenih od neovlaštenog izmjenjivanja.[60] Dizajniran je na dva matematička principa – enkripciji javnog ključa te *hash* ključevima. Enkripcija javnog ključa je koncept moderne kriptografije poznat još i kao asimetrična enkripcija a zasniva se na paru ključeva, javnom i privatnom, povezanim s određenim korisnikom koji mora potvrditi svoj identitet na mreži ili enkriptirati podatke.[61] Korisnik svoj javni ključ može podijeliti s bilo kim dok privatni ključ treba držati u tajnosti. Svi drugi korisnici koji posjeduju njegov javni ključ mogu mu poslati enkriptiranu poruku, ili transakciju u slučaju Bitcoina, pri čemu će istu moći dekriptirati samo onaj korisnik koji je u posjedu privatnog ključa koji odgovara javnom ključu korištenom za enkripciju.[62]

Nadalje, *hash* ključ je rezultat funkcije koja uzima ulaz u obliku alfanumeričkog niza proizvoljne duljine i smanjuje ga na izlaz definirane duljine. U kontekstu *blockchaina*, ili još specifičnije, kriptovaluta, svaka transakcija tretira se kao ulaz koji prolazi kroz *hashing* algoritam

[58] Usp. Nakamoto, Satoshi. Bitcoin: a Peer-to-Peer electronic cash system. Str. 1. URL: https://bitcoin.org/bitcoin.pdf (2018-08-07)
[59] Usp. Uruqhart, Andrew. The inefficiency of bitcoin. 2016. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2828745 (2018-08-07)
[60] Usp. Witte, J. H. The Blockchain: a gentle four page introduction. 2016., str. 1. URL: https://arxiv.org/pdf/1612.06244.pdf (2018-08-07)
[61] Usp. Public key cryptography. URL: https://www.ibm.com/support/knowledgecenter/en/SSB23S_1.1.0.13/gtps7/s7pkey.html (2018-08-07)
[62] Usp. Witte, J. H. Nav. dj, str 2.

pri čemu joj se dodjeljuje izlaz fiksne duljine.[63] U svojoj suštini, *hashing* algoritam uzima potencijalno beskonačan ulaz bitova i pretvara ga u izlaz koji je dovoljan za identifikaciju ulaza. Bitna značajka *hash* ključeva je njihova ireverzibilnost. Recimo da neki internet poslužitelj pohranjuje samo *hash* ključeve lozinki svojih korisnika. On tako može provjeriti svaku korisničku prijavu bez znanja specifičnih korisničkih lozinki.[64] Ovakav pristup posebno je koristan u slučaju obrade velikog broja podataka ili transakcija budući da ne zahtijeva pamćenje potencijalno ogromne količine podataka u ulazu, već samo *hash* ključa kao izlaza tih podataka.[65]

Zapis je bilo koji oblik dokaza o prošlosti koji olakšava očuvanje točnosti informacija kroz vrijeme. Takav specifičan i redovito ažuriran dokument naziva se *ledger* odnosno glavna knjiga transakcija. Održavanje takvog zapisa između dvije ili više strana tradicionalno je predstavljalo rizik budući da je zahtijevalo ili središnji autoritet, odnosno posrednika, na čije su se zapise sve strane u nekom odnosu mogle oslanjati, ili oslanjanje na zapise jedne od strana u korespondenciji.[66] *Blockchain* uklanja rizik ovakve interakcije distribuiranjem jednog zapisa s vremenskom oznakom kao dokaza o kronološkom slijedu transakcija među svim članovima u mreži. Svi članovi u mreži zajedničkim naporima ažuriraju taj zapis i koriste ga kao jedini izvor istinitosti transakcija.[67]

Distribucija se u ovom slučaju odnosi na bazu podataka koja je fragmentirana i pohranjena na više fizičkih lokacija, a njezina se obrada raspodjeljuje među više članova u mreži. Takva baza podataka krajnjem će korisniku i dalje izgledati kao homogena cjelina, ali činjenica je kako se radi o nizu baza koje su pohranjene na većem broju računala. Podacima na tim računalima može se pristupati istovremeno s više lokacija i mijenjati ih preko mreže pri čemu sva računala koja poslužuju bazu surađuju kako bi održala konzistentnost globalne baze podataka.[68] Specifičnost *blockchaina* je ta što se distribuirana baza, odnosno zapis, ne može modificirati unatrag već joj je jedino moguće pridruživati nove transakcije na osnovu konsenzusa članova u mreži.

Nadalje, *peer-to-peer* označava arhitekturu u kojoj svi članovi unutar neke mreže imaju jednak autoritet i odgovornosti, odnosno svaki član je ujedno i klijent i poslužitelj.[69] U slučaju

[63] Usp. What is hashing: under the hood of Blockchain. URL: https://blockgeeks.com/guides/what-is-hashing/ (2018-08-10)
[64] Usp. Witte, J. H. Nav. dj, str 2.
[65] Usp. What is hashing: under the hood of Blockchain. URL: https://blockgeeks.com/guides/what-is-hashing/ (2018-08-10)
[66] Usp. Witte, J. H. Nav. dj, str 2.
[67] Usp. Nakamoto, Satoshi. Nav. dj, str 1.
[68] Usp. Distributed databases. URL: https://docs.oracle.com/cd/A57673_01/DOC/server/doc/SCN73/ch21.htm (2018-08-10)
[69] Usp. Wararkar, Pravin...[et al.]. Resolving problems based on Peer to Peer network security issue's. // Procedia Computer Science 78(2016), str. 652. URL:

blockchaina peer-to-peer je odgovoran za distribuciju zapisa među članovima mreže. Ovakav je pristup oprečan tradicionalnoj klijent-server arhitekturi koja, iako dolazi u različitim oblicima, uvijek uključuje namjenskog centralnog poslužitelja na kojem su pohranjeni podaci kojima klijenti mogu pristupati, ali oni sami ne mogu posluživati datoteke drugim korisnicima. Budući da klijent-server zahtijeva centraliziranu strukturu, poslužitelj mora neprestano biti spojen na mrežu kako bi mogao posluživati datoteke klijentima. S druge strane, u slučaju *peer-to-peer*-a dovoljno je da je jedan član na mreži kako bi sustav mogao djelovati budući da su svi članovi u mreži svojevrsni poslužitelji.[70] Ovakav pristup organizaciji omogućuje jeftino dijeljenje podataka među članovima budući da ne zahtijeva uspostavu centralnog poslužitelja a postao je izrazito popularan kroz servise poput Napstera i Torrenta koji su omogućavali korisnicima istovremeno preuzimanje i dijeljenje datoteka s drugim članovima u mreži. Dakle, preuzimanjem neke datoteke na osobno računalo započinje proces njezine lokalne pohrane kroz spremanje fragmenata koji će kroz vrijeme, odnosno po završetku preuzimanja tvoriti cjelinu. U *peer-to-peer* mreži preuzete fragmente moguće je dijeliti s drugim članovima koji preuzimaju istu datoteku pri čemu onaj koji datoteku dijelu igra ulogu poslužitelja. Dokle god je barem jedno računalo na koje se ista datoteka preuzima ili je već preuzeta na mreži, mreža će moći neometano raditi, odnosno ta specifična datoteka ostat će dostupna svim članovima.

Primjenom kriptografskih principa u svom dizajnu *blockchain* je eliminirao potrebu za posredovanjem financijskih institucija te anonimizirao transakcije, a distribuiranjem zapisa kroz *peer-to-peer* arhitekturu pružio decentraliziran, demokratičan pristup njihovom potvrđivanju.[71] Za razumijevanje implikacija ovakve uništavajuće tehnologije potrebno je najprije razumjeti interakciju prethodno navedenih gradivnih elemenata na primjeru Bitcoin transakcije.

4.2. Arhitektura *blockchaina*

Izvorna implementacija *blockchaina*, Bitcoin, sastoji se od mreže agenata koji lokalno pohranjuju kopiju distribuiranog *ledgera*, odnosno zapisa svih transakcija od začeća lanca do sadašnjeg trenutka. Budući da je u pitanju okruženje bez posrednika sve transakcije su javne kako bi se

https://www.researchgate.net/publication/301234162_Resolving_Problems_Based_on_Peer_to_Peer_Network_Security_Issue's (2018-08-10)

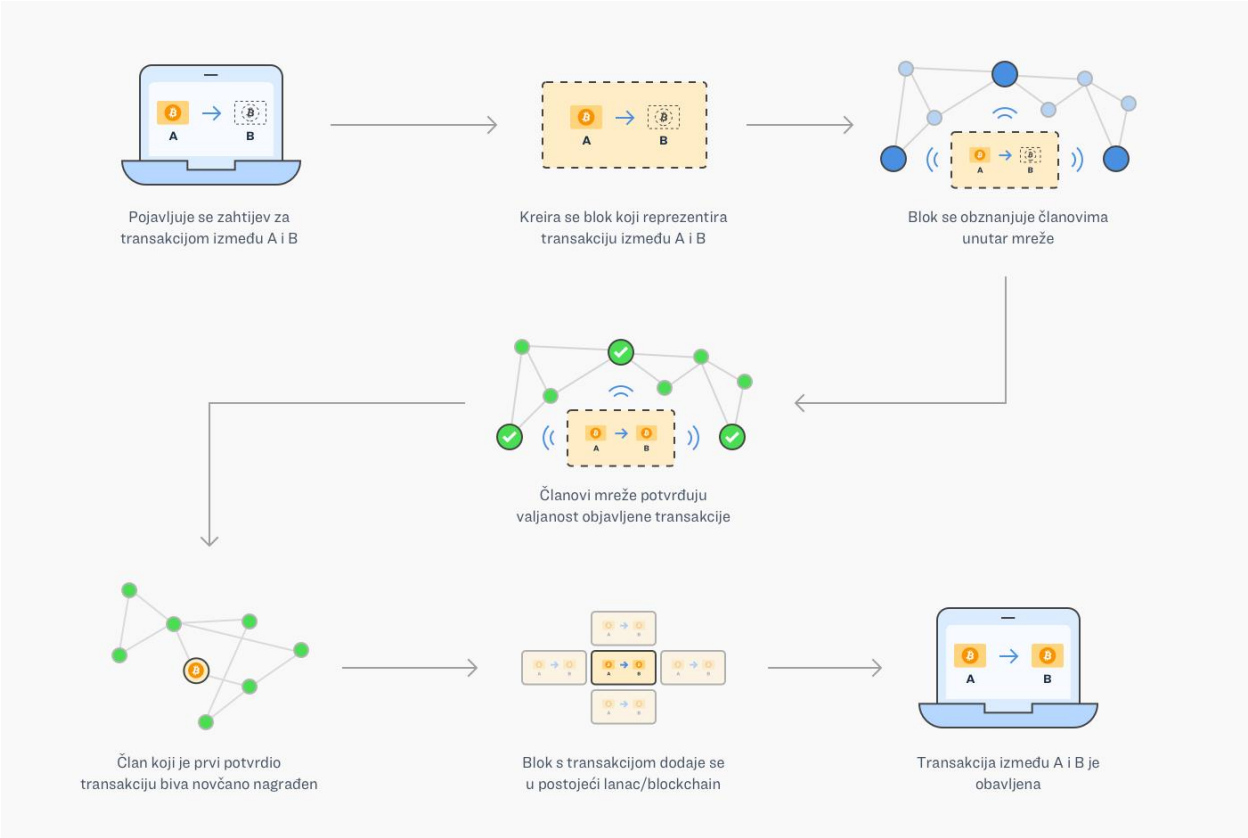
[70] Usp. Posey, Brien. Understanding the differences between client/server and peer-to-peer networks, 26. 5. 2000. URL: https://www.techrepublic.com/article/understanding-the-differences-between-client-server-and-peer-to-peer-networks/ (2018-08-10)

[71] Usp. Witte, J. H. Nav. dj, str 2.

mogao postići konsenzus sudionika o njihovoj autentičnosti.[72] Svaki agent posjeduje elektronički novčanik kao reprezentaciju vlasništva svih plaćanja u Bitcoinu. Ovdje u igru dolaze javni i privatni ključ agenta – svaka transakcija u *blockchainu* reprezentirana je javnim ključem dok je privatni ključ pohranjen u novčanik. Javni ključ može koristiti svatko s *blockchainom* u svrhu slanja enkriptiranih poruka, odnosno transakcija, koje samo vlasnik privatnog ključa može dekriptirati.[73]

Prilikom transakcije korisnik A zahtijeva javni ključ od korisnika B tijekom čega se njihova namjera za transakciju objavljuje svima u mreži. Ovdje u igru dolaze *mineri*, odnosno rudari, posebni agenti koji posjeduju kopiju *legdera*, te imaju dovoljno računalne moći za obavljanje zadatka potvrđivanja novoobjavljene transakcije. Ovaj zadatak sastoji se iz dva dijela – rudar najprije mora potvrditi da korisnik A posjeduje sredstva koja namjerava prebaciti korisniku B, te mora riješiti izračunski zadatak kako bi transakciju mogao dodati u lanac. Prvi dio zadatka relativno je jednostavan – budući da se radi o javnom zapisu svih transakcija rudar vrlo lako može izračunati posjeduje li korisnik A dovoljno sredstava za obavljanje transakcije. Teži dio dolazi nakon provjere valjanosti sredstava – u ovom trenutku rudar mora prvi stvoriti novi *hash* ključ enkodirajući pritom posljednji poznati *hash* ključ i podatke o novoj transakciji nakon čega će biti novčano nagrađen.[74] Ovaj proces naziva se *proof-of-work* i predstavlja jedan od mogućih načina postizanja konsenzusa u mreži. U slučaju *proof-of-work*-a radi se o dokazu da je rudar uložio računalnu snagu u provjeru valjanosti transakcije.[75] Kako bi uspjeh rudara bio nasumičan, odnosno kako bi se osigurala demokratičnost mreže, novogenerirani ključ mora imati unaprijed određenu strukturu koju agenti pokušavaju nasumično pogoditi. Ovaj proces naziva se rudarenje, a od rudara iziskuje ulaganje računalne snage kako bi se pronašao nasumičan niz brojeva – *nonce (number used only once)*, koji će prolaskom kroz *hashing* algoritam proizvesti *hash* ključ odgovarajućeg formata čime će potvrda transakcije biti prihvaćena. Ta se potvrda odmah obznanjuje unutar mreže prilikom čega se *blockchain* ažurira.[76] Grafički prikaz transkacije u Bitcoin sustavu te osnovnih funkcionalnsti *blockchaina* moguće je vidjeti na Slici 1.

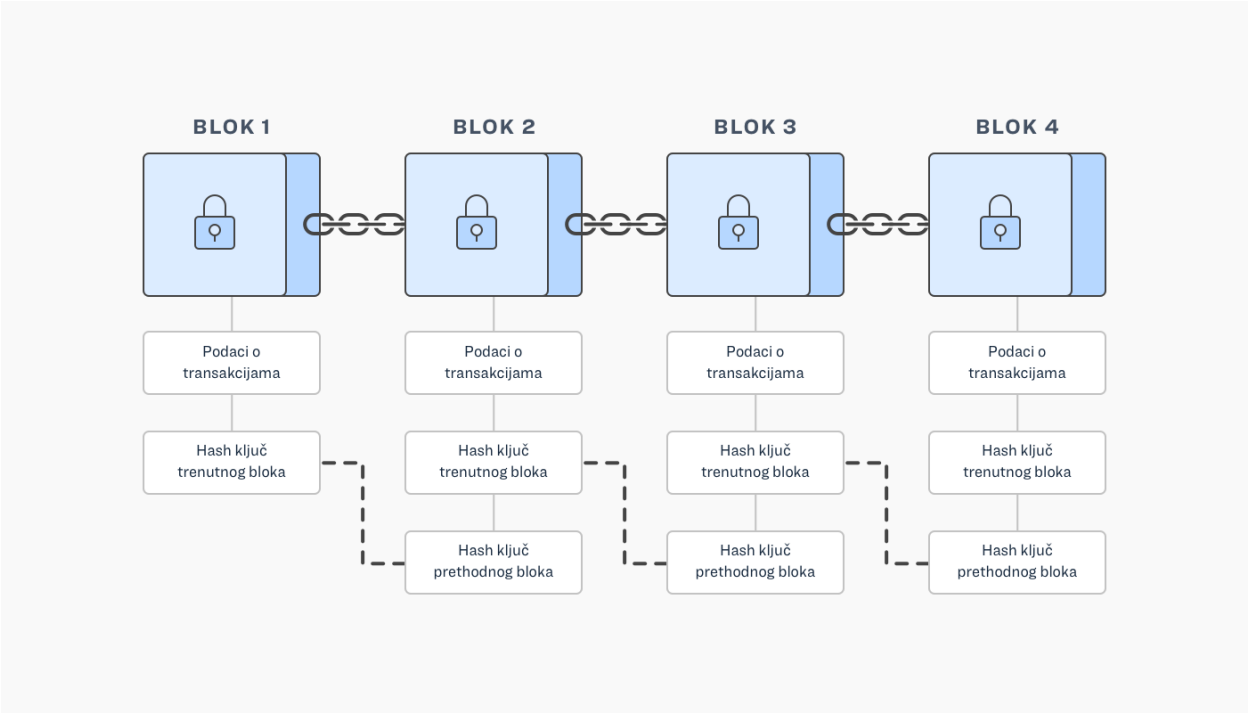
[72] Usp. Nakamoto, Satoshi. Nav. dj, str 2.
[73] Usp. Witte, J. H. Nav. dj, str 2-3.
[74] Isto, str 3.
[75] Usp. Nakamoto, Satoshi. Nav. dj, str 3.
[76] Usp. Witte, J. H. Nav. dj, str 2-3.



Slika 1. Grafički prikaz transakcije u Bitcoin mreži

Jednom kada je *proof-of-work* zadovoljen i novi blok dodan u lanac on se više ne može izmijeniti, odnosno takvo što je gotovo nemoguće, a svaki novi blok dodatno će ga ojačati čime je osigurana autentičnost povijesti transakcija u *blockchainu*. Zlonamjeran agent u mreži bi za izmjenu specifičnog bloka morao izmijeniti i sve blokove koji su u lanac dodani nakon njega te imati dovoljno računalne snage da prestigne rast lanca i u konačnici u lanac doda posljednji blok. Uzme li se u obzir da se nove transakcije potvrđuju otprilike svakih 10 minuta, mogućnost da sporiji napadač sustigne brzinu lanca eksponencijalno pada s njegovim rastom.[77] Pojednostavljeni prikaz funkcije *hashiranja* i rasta lanca moguće je vidjeti na Slici 2.

[77] Usp. Nakamoto, Satoshi. Nav. dj, str 3.



Slika 2. Grafički prikaz funkcije *hashiranja* u *blockchainu*

Iz primjera transakcije Bitcoina je moguće razlučiti tri značajke *blockchaina* koje su ujedno izvor njegovog potencijala ali i njegovih problema. Prije svega, *blockchain* je ovisan o veličini mreže agenata. Poželjno je imati što veću distribuiranu mrežu kako bi se smanjile šanse zlonamjernih napada ili centralizacije kontrole nad lancem. U kriptovalutnim sustavima poput Bitcoina inicijativa za uključivanje u mrežu je rudarenje, odnosno novčana nagrada koja proizlazi iz uspješne potvrde transakcije i dodavanja bloka u lanac.[78] Međutim, pitanje je kakva bi inicijativa bila potrebna za širenje distribuirane mreže agenata u sustavu koji svojim članovima ne nudi materijalnu korist. Nadalje, *blockchain* karakterizira dubina lanca. Svi agenti u mreži svoj *ledger* uvijek ažuriraju na najdulju verziju lanca koja predstavlja konsenzus članova o valjanosti povijesti transakcija.[79] Dakle, što je lanac dulji to je trajnost i nepromjenjivost blokova dublje u lancu veća zahvaljujući kontinuiranom *hashiranju*. Naravno, u teoriji je moguće dodati nepotvrđen blok u lanac, međutim takvo što predstavlja iznimno težak zadatak koji se može otpisati kao nemoguć pothvat. U konačnici, posljednja značajka *blockchaina* proizlazi upravo iz inicijative za uključivanje u jednu takvu mrežu. Radi se o mogućnosti većinske kontrole nad mrežom poznate pod nazivom napad 51 %. U pitanju je rizik da unutar *blockchain* sustava postoji agent ili grupa agenata koji dominiraju na području računalne snage što im omogućava brže rudarenje, a samim time i manipulaciju nad dodavanjem novih blokova u lanac. U velikoj distribuiranoj mreži šanse

[78] Usp. Witte, J. H. Nav. dj, str 4.
[79] Usp. Nakamoto, Satoshi. Nav. dj, str 3.

za zlonamjernom kontrolom lanca opadaju, međutim treba uzeti u obzir da je novčana dobit često dobar poticaj za postizanje nemogućeg. Također ne treba pretpostavljati da rizik zlonamjerne kontrole lanca u sustavima koji ne koriste novac kao inicijativu ne postoji. Uzme li se u obzir da određene skupine mogu imati legitimne interese u cenzuriranju ili neovlaštenom manipuliranju podacima u nekom sustavu, napad 51 % nije nešto što bi se trebalo olako otpisati u bilo kom kontekstu.[80]

Dakle, primjenom principa kriptografije za anonimiziranje članova mreže, njezinom distribucijom i demokratiziranjem, *blockchain* je u vrlo kratkom roku ponovno oživio financijski sustav. Međutim, očito je da ni *blockchain* nije otporan na zlouporabu ni probleme – u krajnjem slučaju, savršen sustav ne postoji. Ono što se iskristaliziralo u desetljeću od začeća Bitcoina je primjenjivost *blockchaina* na različite slučajeve – u svojoj suštini on omogućuje stvaranje sigurne distribuirane baze za bilo koji tip podataka. Promjenom načina i resursa potrebnih za potvrđivanje blokova u lancu *blockchain* može zadržati svoju srž i služiti svrhama izvan konteksta financija, stoga su mehanizmi za postizanje konsenzusa poput *proof-of-work*-a vrlo bitna odrednica u definiranju njegove primjene.[81]

4.3. Mehanizmi za postizanje konsenzusa u *blockchainu*

Decentraliziranost *blockchaina* znači da unutar sustava ne postoji centralno tijelo koje će se baviti potvrđivanjem transakcija već je taj zadatak distribuiran među članovima u mreži i temelji se na konsenzusu koji predstavlja dinamičan način postizanja sporazuma u grupi. Za razliku od glasanja gdje se poštuje odluka većine bez uzimanja u obzir potreba manjine, konsenzus označava usuglašavanje koje će potencijalno biti od koristi cijeloj grupi. Metode kojima se konsenzus postiže u *blockchainu* nazivaju se mehanizmi za postizanje konsenzusa. Bitne značajke tih mehanizama su:

- suglasnost,
- suradnja
- jednakost,
- uključivost i
- sudjelovanje.

[80] Usp. Witte, J. H. Nav. dj, str 4.
[81] Isto.

Dakle, mehanizam za postizanje konsenzusa je zasnovan na suglasnosti budući da pokušava dobiti što veću moguću razinu dogovora među članovima grupe. Nadalje, suradnički je tako da od svih sudionika zahtijeva zajednički rad na postizanju rezultata koji će koristiti cijeloj grupi. Mehanizam temeljen na jednakosti ne pravi razliku među glasovima unutar grupe – svaki član ima jedan glas, a svaki glas ima jednaku težinu. U konačnici je poželjno aktivno sudjelovanje svih članova u procesu postizanja konsenzusa, odnosno proces ne treba biti nalik glasanju gdje ljudi odlučuju da ne žele glasati jer ne vjeruju da će svojim uključenjem postići ikakvu promjenu.[82] Ranije spomenuti *proof-of-work* predstavlja najpoznatiji mehanizam za postizanje konsenzusa. Međutim njegova potreba za konstantnom nadogradnjom i akumuliranjem računalne moći kao i potrošnja resursa kao svrha sama sebi doveli su do razvoja alternativnih mehanizama kojima se pokušalo adresirati neke od njegovih problema. Dakle, uz *proof-of-work* neki od poznatijih mehanizama za postizanje konsenzusa su:

- *proof-of-stake*,
- *proof-of-activity* te
- *proof-of-capacity*.

Proof-of-work je mehanizam za postizanje konsenzusa u Bitcoin mreži. Temeljen je na korištenju računalne moći za potvrđivanje blokova kroz rješavanje kriptografske zagonetke. *Nonce* koji rudari pokušavaju pronaći ne može se predvidjeti, pa se samim time ni rudar koji će ga otkriti ne može odrediti prije nego ga otkrije. Dakle, pronalazak *nonce*-a u svojoj je suštini nasumično pogađanje koje je izrazito zahtjevno za računalo i samim time iziskuje potrošnju ogromne količine energije.[83] Upravo iz tog aspekta proizlaze problemi *proof-of-work*-a. Prije svega, neograničeno velik broj rudara u isto vrijeme ulaže energiju i računalne resurse u provjeru jedne transakcije koju će u konačnici potvrditi samo jedan član. To znači da će energija koju su utrošili svi ostali rudari biti potrošena bez razloga, odnosno kao svrha samoj sebi. Stoga je sasvim legitimno propitivati utjecaj ovakvog sustava na okoliš budući da je energetski trošak jedne Bitcoin transakcije dovoljan za održavanje oko jednog i pol američkog kućanstva na jedan dan, a u Bitcoin mreži se potvrdi otprilike 110.000 transakcija dnevno.[84] Drugi problem proizlazi iz potrebe za akumulacijom

[82] Usp. Boaventura, Andre. Demystifying blockchain and concesus mechanisms – everything you wanted to know but were never told, 12.4. URL: https://medium.com/oracledevs/demystifying-blockchain-and-consensus-mechanisms-everything-you-wanted-to-know-but-were-never-aabe62145128 (2018-08-11)
[83] Isto.
[84] Usp. Malmo, Christopher. Bitcoin is unsustainable, 29. 6. 2015. URL: https://motherboard.vice.com/en_us/article/ae3p7e/bitcoin-is-unsustainable (2018-08-11)

računalne moći jer će brže računalo moći brže isprobavati moguće kombinacije *nonce*-a i samim time imati prednost pri potvrđivanju transakcija. Upravo su ove dvije značajke *proof-of-work* mehanizma dovele u pitanje decentraliziranost Bitcoina budući da je vremenom došlo do centralizacije rudarenja u dijelovima svijeta s jeftinom električnom energijom, a kontinuirana nadogradnja računala postala je problem zbog porasta u cijenama računalnih komponenti.[85] Kako bi se izbjegla centralizacija mreže koja promovira upravo suprotno razvijena je alternativa *proof-of-work*-u u vidu *proof-of-stake* mehanizma.

Proof-of-stake prije svega eliminira koncept rudarenja i dokazivanja rada kroz rješavanje složenih kriptografskih zagonetki. Ovaj mehanizam temelji se na udjelu koji pojedini članovi imaju unutar sustava – pojedinac ulaže u valutu na kojoj je sustav temeljen čime postaje validator, odnosno svojevrsna ekvivalenta rudaru. Potvrđivanje blokova u ovom se slučaju ne temelji na nasumičnom pogađanju *nonce*-a, već na nasumičnom odabiru validatora prema njihovom udjelu u mreži.[86] Inicijativa proizlazi upravo iz činjenice da će članovi s visokim udjelima željeti održati mrežu na životu i učiniti ju što sigurnijom. Ovaj pristup postizanju konsenzusa predstavlja znatno „jeftiniju“ alternativu budući da ne zahtijeva stalne tehničke nadogradnje i potrošnju ogromnih količina električne energije. O značajnim ekonomskim razlikama u održavanju *proof-of-work* nasuprot *proof-of-stake* sustava svjedoči i Czarnekovo istraživanje iz 2014. godine u kojem je izračunao prosječne troškove električne energije i računalnih komponenti u dva sustava jednake veličine temeljena na ova dva mehanizma. Došao je do zaključka kako je za održavanje *proof-of-work* sustava na godišnjoj razini potrebno izdvojiti oko 62 milijuna dolara za električnu energiju te oko 69 milijuna dolara za računalne komponente. S druge strane, godišnji trošak održavanja *proof-of-stake* sustava iznosio bi oko 8 tisuća dolara za električnu energiju te oko 50 tisuća dolara za računalne komponente.[87] Međutim, ni *proof-of-stake* ne predstavlja idealno rješenje. Prije svega, s obzirom na to da je rad na potvrđivanju transakcija računalno nezahtjevan, validatorima je omogućeno glasanje za oprečne transakcije budući da nemaju što izgubiti. Uz to, kako šanse validatora za odabir od strane sustava rastu proporcionalno njihovom udjelu u mreži, sustav nagrađuje one koji posjeduju najviše čime se ponovno javlja rizik od centralizacije moći u rukama nekolicine.[88]

[85] Usp. Boaventura, Andre. Nav. dj.
[86] Isto.
[87] Usp. Czarnek, Matthew; Secondleo. Nxt network: energy and cost efficiency analysis. 2014. URL: https://www.scribd.com/document/254930279/Nxt-Network-Energy-and-Cost-Efficiency-Analysis (2018-09-06)
[88] Usp. Boaventura, Andre. Nav. dj.

Proof-of-activity je pokušaj rješavanja problema *proof-of-stake* i *proof-of-work* mehanizama kombinacijom značajki oba mehanizma. Dakle, u ovom su slučaju prisutni i koncept rudara i koncept validatora. Rudarenje predstavlja prvi korak u kojem se umjesto punog bloka koji nosi podatke o transakcijama kreira njegov prazan predložak nakon čega se odabire grupa validatora prema principima *proof-of-stake* mehanizma. Jednom kada svi validatori potvrde predložak bloka on postaje punopravan i dodaje se u lanac. Međutim, kritike ovog mehanizma usmjerene su na iste probleme koje imaju *proof-of-work* i *proof-of-stake* mehanizmi te on za sad ne predstavlja dobru alternativu niti jednom od njih.[89]

U konačnici, *proof-of-capacity*, odnosno *proof-of-space* predstavlja noviju alternativu rješavanju problema popularnih mehanizama za postizanje konsenzusa. Umjesto računalne snage ili udjela u mreži, *proof-of-capacity* mehanizam se oslanja na korištenje slobodnog prostora za pohranu na računalima članova mreže. Dakle, svaki član može namijeniti slobodan prostor na svom tvrdom disku koji će se koristiti za pohranjivanje mogućih rješenja kriptografske zagonetke. Umjesto nasumičnog pogađanja u stvarnom vremenu, rješenja se pohranjuju prije nego proces rudarenja uopće započne, a sustav u konačnici odabire najbrže rješenje i nagrađuje njegovog vlasnika. Prilika za uspješnim rješavanjem zadatka raste s prostorom namijenjenim za pohranu mogućih rješenja što ovaj mehanizam čini energetski učinkovitijim i znatno pristupačnijim od njegovih popularnijih alternativa.[90] Uz to, budući da se umjesto sirove snage računala koristi njegov prostor za pohranu, moguće je pretpostaviti kako će ovaj mehanizam svojim razvojem biti najpogodniji za sustave u kojima je potrebno trajno čuvati i dijeliti podatke. Međutim, budući da se radi o relativno novoj tehnologiji koja nije rigorozno testirana niti implementirana u širokom spektru slučajeva razumljivo je zašto *proof-of-capacity* još nije pronašao svoje mjesto među punokrvnim mehanizmima za postizanje konsenzusa u *blockchainu*.

Dakle, bilo je potrebno razviti mehanizme koji će automatski razrješavati suglasnost u zajednici budući da u *blockchainu* ne postoji centralna struktura zadužena za koordinaciju interakcije među članovima mreže. Na taj je način otklonjena mogućnost manipulacije mrežom od strane nadređenog tijela. Međutim, očito je kako u *blockchain* sustavima i dalje postoji sklonost prema centralizaciji kojoj se još uvijek ne pridaje dovoljno pažnje. Budući da je upravo decentraliziranost jedna od glavnih značajki ove tehnologije, nimalo ne začuđuju napori da se ista očuva. No pitanje je koje su točno značajke decentralizirane arhitekture, koliko je ona bitna u

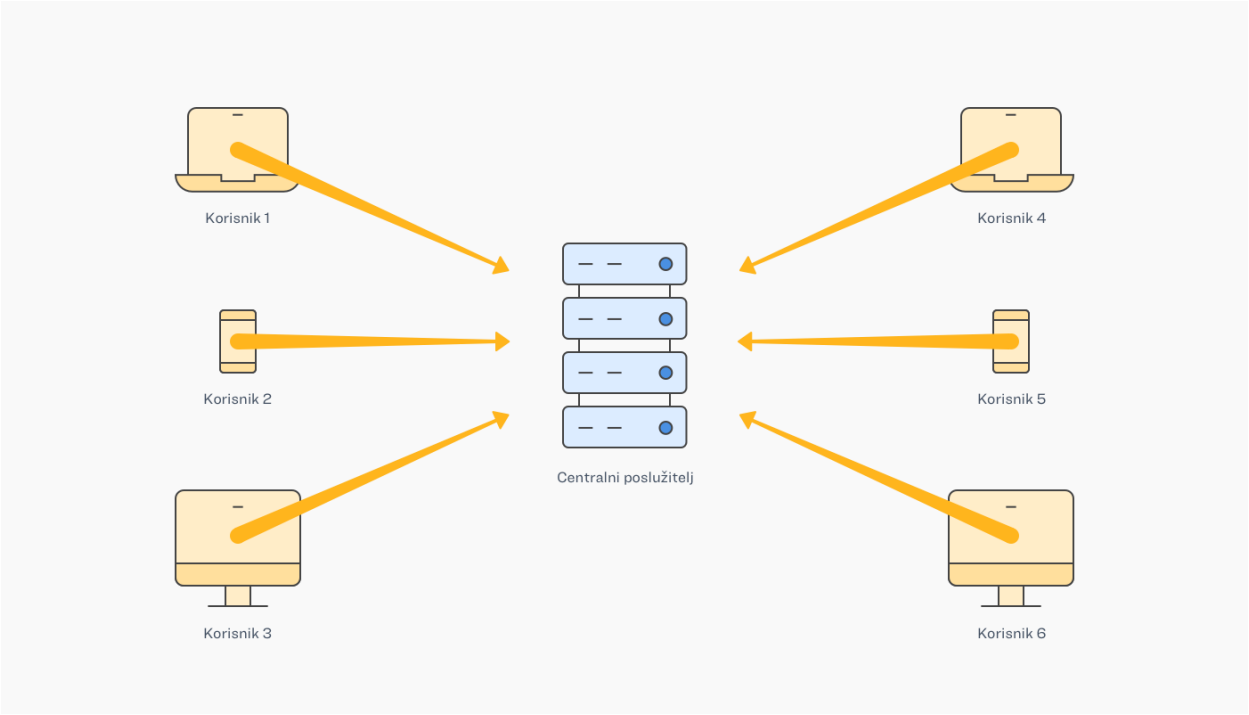
[89] Isto.
[90] Usp. Proof of capacity (Cryptocurrency). URL: https://www.investopedia.com/terms/p/proof-capacity-cryptocurrency.asp (2018-08-11)

očuvanju ekosustava poput *blockchaina*, i kako ona utječe na interakcije i privatnost korisnika u jednom takvom okruženju?

4.4. Informacijska privatnost u *blockchainu*

Većina prometa na mreži prolazi kroz nekoliko centraliziranih platformi i servisa koji svojim korisnicima jamče privatnost i autonomiju. Bilo da se radi o upitima na Googleu čija je prevlast postala jasna pojavom termina „guglati“, kupovini na Amazonu ili uspomenama na Facebooku, neupitno je da je pojedinčev svakodnevni boravak na mreži u rukama nekoliko korporativnih divova koji periodički šire svoj spektar usluga i čine očitim rastući trend centralizacije.[91] Stoga je jasna i pomutnja koju je uzrokovala pojava i brzo širenje decentralizirane strukture kakvu ima *blockchain*. Pozadina munjevitog rasta kriptovalutnih sustava poput Bitcoina dobro je poznata – glavni pokretač njihovog širenja bila je njihova vrijednost. Kao tehnologija iza tih sustava, *blockchain* je u manje od desetljeća doživio svojevrsnu renesansu pronalazeći primjenjivost u mnogim drugim kontekstima u kojima se decentralizacija pokazala kao primjerena alternativa. Međutim, za razumijevanje decentralizirane arhitekture i njezinih potencijalnih koristi za korisnike, potrebno je najprije razumjeti centraliziranu arhitekturu čija je pojednostavljena struktura vidljiva na Slici 3.

[91] Usp. De Filippi, Primavera. The interplay between decentralization and privacy: the case of blockchain technologies. // Journal of Peer Production 7(2016), str. 2. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2852689 (2018-08-11)



Slika 3. Grafički prikaz centralizirane mreže

Jednostavan primjer centraliziranog sustava bio bi sustav izdavanja digitalnih certifikata, odnosno interakcija korisnika s takvim sustavom. Dakle, prednost digitalnih certifikata nasuprot njihovih analognih ekvivalenata je manjak potrebe za fizičkom prisutnošću prilikom njihovog podizanja. U suštini, digitalni certifikat moguće je dobiti u bilo kom trenutku, s bilo koje lokacije bez obzira na udaljenost od institucije koja ga izdaje, uz preduvjet povezanosti s mrežom. Međutim, iako se krajnjem korisniku može činiti kako sustav na neki način dolazi k njemu putem sučelja prikazanog na ekranu njegova uređaja, činjenica je kako apsolutno svi udaljeni korisnici dolaze na centralnu arhitekturu poslužitelja koja pohranjuje njihove podatke i preko koje se digitalni certifikati izdaju. Ovakva struktura ima određene prednosti – prije svega, centralizirani sustavi su znatno bolje usklađeni te zahtijevaju manji broj transakcija podataka za koordinaciju grupe pojedinaca pri čemu se smanjuje i količina nepotrebnog razotkrivanja podataka. Pri tome se misli na razotkrivanje ostalim korisnicima u nekoj mreži, budući da su podaci potrebni za korištenje neke usluge ili servisa uvijek poznati pružatelju pod jamstvom njihove zaštite i poštivanja prava. Nadalje, centralizacija znatno olakšava reguliranje interakcije korisnika s platformom te u konačnici omogućuje održavanje evidencije svih aktivnosti u nekom sustavu.[92] Dok se krajnjem korisniku zaista može činiti kako su njegove namjere i kretanje mrežom tajne, što one drugim korisnicima najčešće i jesu, činjenica je kako sustav i ljudi koji ga održavaju mogu pratiti i bilježiti svaki korisnički korak od početka do kraja sesije. Uz to, ogromna prednost

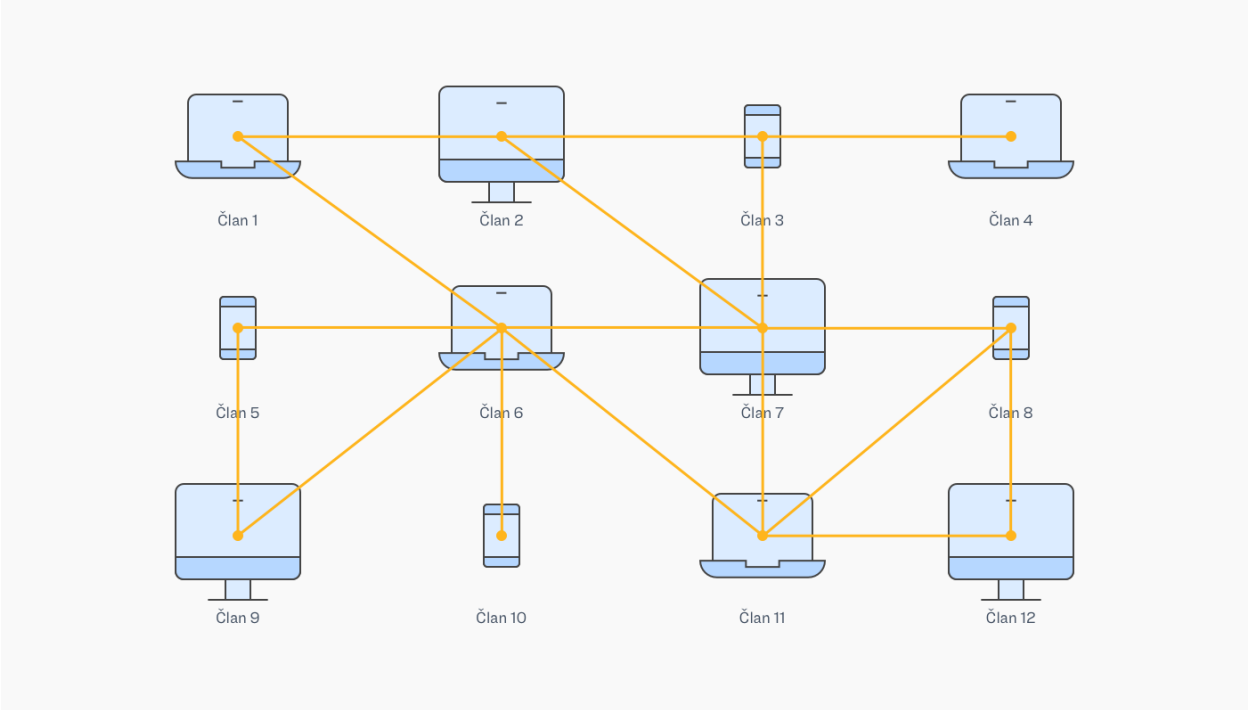
[92] Isto.

centralizacije je što korisnici ne moraju samostalno osiguravati komunikacijske kanale, što naravno dolazi uz potrebu povjeravanja podataka operatorima u nadi da će ih oni koristiti u legitimne svrhe. S obzirom na to da prosječan korisnik najčešće ne posjeduje tehničko znanje niti volju potrebnu za enkripciju podataka, centraliziran sustav koji sve to obavlja automatski u zamjenu za njegove podatke predstavlja olakšicu i prednost. Međutim, ovakav odnos implicira prijetnju nadgledanja budući da su korisnički podaci u digitalnom dobu postali vrijedan izvor informacija hakerima i vladama a centralizacija i personalizacija uglavnom su samo opravdanje za kontrolu tijeka informacija na mreži. Ipak, očito je kako je ugodnost korištenja centraliziranih usluga bitnija te je cijena koju za to plaćamo povjerenje u sustav da će naši podaci ostati sigurni.[93]

S druge strane, decentralizirani sustavi poput *blockchaina* predstavljaju stav oprečan centralizaciji. Primjer strukture jednog takvog sustava vidljiv je na Slici 4. Činjenica je kako su znatno teži za implementirati i koristiti budući da zahtijevaju veću uključenost i znanje korisnika, ali predstavljaju znatno bolje rješenje za podršku individualnih prava i sloboda. Potrebno je naglasiti kako utjecaj ovakvih sustava na informacijsku privatnost nije toliko izravan koliko bi se dalo pretpostaviti na prvu – dok je cijena centralizacije povjerenje u sustav, cijena decentralizacije je transparentnost, odnosno javnost podataka o svim interakcijama na mreži svim članovima.[94] Međutim, transparentnost ne znači nužno da privatnost u sustavu poput *blockchaina* ne postoji – upravo je eliminacija centralnog tijela, odnosno posrednika, korak unaprijed budući da korisnici više nisu primorani razmjenjivati svoje podatke za usluge. Dakle, decentralizacija pruža višu razinu suverenosti podataka ostavljajući kontrolu nad njihovim dijeljenjem samo i jedino njihovim vlasnicima što je u konačnici temeljna ideja koncepta informacijske privatnosti.[95] S druge strane, upravo zbog nedostatka posrednika u decentraliziranim mrežama znatno je teže postići koordinaciju među članovima, ali je time znatno otežana i mogućnost praćenja i reguliranja članova te kontroliranja tijeka informacija. Koordinacija se postiže distribuiranjem određenih podataka svim članovima u mreži, odnosno korištenjem ranije spomenutih mehanizama za postizanje konsenzusa. Težnja decentralizacije je potpuna anonimizacija korisnika, međutim, većina implementacija *blockchaina* još uvijek ne podržava anonimnost već pseudonimnost. Anonimnost bi značila da je nemoguće povezati bilo koji identifikator sa specifičnim profilom. S druge strane, pseudonimnost znači upravo korištenje određenih identifikatora kako bi se pravi identitet osobe sakrio. Dakle, komunikacija u *blockchainu* može biti enkriptirana, ali metapodaci

[93] Isto, str 1-3.
[94] Isto str 1.
[95] Usp. Privacy and information Technology. // Stanford encyclopedia of philosophy, 20. 11. 2014. URL: https://plato.stanford.edu/entries/it-privacy/ (2018-07-30)

o tome tko s kim komunicira, koliko dugo, itd. moraju biti vidljivi svima u mreži kako bi se osigurala transparentnost i napredak cijele grupe. Upravo to je nedostatak većine trenutnih implementacija *blockchaina* – mreže nisu dovoljno zaštićene od analize javnih metapodataka od strane vanjskih tijela čime je moguće ugroziti njihove članove. Međutim, budući da se radi o relativno mladoj tehnologiji, šanse su kako će buduće implementacije biti usmjerene na rješavanje ovih problema i krčenje puta prema apsolutnoj anonimnosti i privatnosti u mreži. Ipak, postavlja se pitanje hoće li okruženja u kojima su sve interakcije javne biti nešto na što će se društvo moći prilagoditi ili će pristupačnost centralizacije ostati odlučujuća odrednica i izvor bezbrižnosti u interakciji s mrežom.[96]



Slika 4. Grafički prikaz decentralizirane distribuirane mreže

4.5. Autentičnost u *blockchainu*

Findlay u svojoj raspravi o *blockchainu* kao potencijalnom rješenju nepovredivosti zapisa navodi rastuću potrebu za kreiranjem decentraliziranog arhiva u kojem će se čuvati pouzdani, autentični i ispravno indeksirani informacijski objekti, a koji će postojati iznad korporativnih i vladinih tijela. Pojam nepovredivosti proizlazi iz arhivističke terminologije, a odnosi se na postupanje sa zapisima kao dokazima ako su isti rezultat rutinskih i konzistentnih procesa vođenja evidencije; ako se

[96] Usp. De Fillipi, Primavera. Nav. dj, str. 1-12.

čuvaju u sustavima s kontroliranim izmjenama; te ako posjeduju kvalitetne metapodatke o kontekstu u kojem su stvoreni, odnosno o vlastitom podrijetlu.[97] U skladu s time, pouzdanost, autentičnost, integritet i upotrebljivost zapisa pružat će povjerenje u taj zapis kao legitiman dokaz neke aktivnosti a upravo koncepti autentičnosti i integriteta čine srž *blockchaina*.[98]

Odvojimo li *blockchain* od njegove implementacije u Bitcoin mreži, možemo razlučiti kako se radi o bazi zapisa, odnosno sustavu za vođenje evidencije zasnovanom na kriptografiji i distribuciji unutar neke mreže. Dakle, *blockchain* služi za periodičko bilježenje i čuvanje dokaza o interakcijama u nekom sustavu – povezivanje podataka s kontekstom i stvaranje međusobnih odnosa pomoću metapodataka. U svojoj suštini može se koristiti za bilo koji tip podataka i aktivnosti budući da nije vezan uz njih, već uz evidentiranje njihovih identifikatora i pohranjivanje u neraskidiv lanac.[99]

Ovdje do izražaja dolaze značajke *blockchaina* u pogledu digitalnih potpisa i *hash* ključeva te upravo iz tih kriptografskih principa proizlazi autentičnost *blockchaina* kao povijesnog dokaza transakcija unutar nekog sustava. Prije svega, svaki je blok unutar lanca potpisan čime je zabilježen njegov autor. Time se pruža konkretan dokaz o tome da je zapis stvoren od strane onog za kog tvrdi da jest, da njegov autor ne može poreći stvaranje tog zapisa, te da zapis nije izmijenjen na svom putu do primatelja.[100] Potom se zapis s pridruženim identifikatorima vremenski označuje i *hashira* čime se pridružuje stalno rastućem lancu povijesti aktivnosti. *Hashiranje* predstavlja ireverzibilan proces, a budući da se svaki blok u lancu *hashira* zajedno s podacima svih prethodnih blokova, bilo kakve kasnije izmjene gotovo su nemoguće čime je osiguran integritet zapisa. U konačnici, budući da je decentraliziran, dodavanje zapisa u *blockchain* bit će moguće samo postizanjem konsenzusa većine članova u mreži kako bi se onemogućilo zlonamjerno rukovanje lancem.

U svojoj srži arhiv predstavlja sustav za vođenje evidencije, međutim i mnoge druge institucije imaju stalnu potrebu za periodičkim, kontroliranim i strukturiranim vođenjem zapisa o svojim aktivnostima. Cilj takvog procesa je kreiranje dokaza, bilo da se radi o novčanim transakcijama, poslovnim procesima ili izmjenama na informacijskim objektima u svrhu njihove

[97] Usp. Findlay, Cassie. Decentralised and inviolate: the blockchain and its uses for digital archives, 23. 01. 2015. URL: https://rkroundtable.org/2015/01/23/decentralised-and-inviolate-the-blockchain-and-its-uses-for-digital-archives/ (2018-08-12)
[98] Usp. Lemeiux, Victoria Louise. Trusting records: is Blockchain technology the answer?. // Records Management Journal 26, 2 (2016), str. 112. URL: http://www.emeraldinsight.com/doi/pdfplus/10.1108/RMJ-12-2015-0042 (2018-08-12)
[99] Usp. Findlay, Cassie. Nav. dj.
[100] Usp. Lemeiux, Victoria Louise. Nav. dj. Str 116-117.

dugotrajne zaštite i očuvanja. Pravilno vođenje evidencije kroz godine je standardizirano u dokumentima poput funkcionalnih zahtjeva za čuvanje zapisa, ili sustavima poput OAIS-a (*Open Archival Information System*) ali je sam proces iziskivao prilagodbe od slučaja do slučaja te određenu razinu povjerenja u instituciju da će svoje dužnosti obavljati savjesno. *Blockchain* je vođenje evidencije doveo na novu razinu stvaranjem nepovredivog zapisa čija se autentičnost i integritet ne temelje na povjerenju već predstavljaju gradivne elemente ove tehnologije.[101] U konačnici ostaje vidjeti na koji se način *blockchain* može primjenjivati izvan konteksta financija te je li moguće na ovoj tehnologiji zasnovati sustav za zaštitu i očuvanje digitalnih podataka.

5. PRIMJENE *BLOCKCHAINA* IZVAN KONTEKSTA FINANCIJA

U desetljeću od nastanka i širenja Bitcoin mreže *blockchain* je pronašao primjenjivost u mnogim drugim područjima izvan slanja novčanih transakcija. Potencijal ove tehnologije za stvaranje distribuiranih mreža zasnovanih na transparentnosti umjesto povjerenju te vođenje autentičnog zapisa o povijesti aktivnosti doveo je do razvoja koncepata i implementacija *blockchaina* u područjima u kojima se njegova primjenjivost nije činila mogućom na prvi pogled. Neke od perspektivnijih primjena *blockchaina* su u području distribucije dobara, upravljanja organizacijama, medicine, vođenja države te znanstvenih istraživanja.

Prema Leeju i Pilkingtonu *blockchain* bi mogao imati pozitivan utjecaj na lanac opskrbe potrošačkom elektronikom. Radi se o industriji proizvođača telefona, računala, kamera, televizora i sl. za koju se očekuje da će do 2023. prijeći vrijednost od 1,8 trilijuna dolara. Problematika lanca opskrbe proizlazi iz manjka uvida potrošača u putovanje proizvoda kroz ljude, mjesta i materijale te nemogućnosti utvrđivanja stvarnih cijena proizvoda i usluga koje konzumiraju.[102] Međutim, ni kompanije najčešće ne mogu znati što se sve događa s proizvodima na putu od proizvođača do distributera što je posebice problematično u industriji hrane. Stoga nije začuđujuća činjenica kako kineski ogranak Walmarta već koristi *blockchain* za praćenje pošiljki svinjskog mesa.[103] Stvaranjem svojevrsnih digitalnih putovnica u *blockchainu* bila bi osigurana autentičnost i

[101] Usp. Findlay, Cassie. Nav. dj.
[102] Usp. Lee, Jong-Hyouk; Pilkington, Marc. How the blockchain revolution will reshape the consumer electronics industry. // IEEE Consumer Electronics Magazine 4(2017), str. 20. URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7948864 (2018-08-12)
[103] Usp. Beal, George. Industries with heavy supply chains face major problems. Blockchain tech might be the answer, 31. 10. 2017. URL: https://thenextweb.com/contributors/2017/10/31/supply-chains-blockchain-tech/ (2018-08-12)

podrijetlo proizvoda.[104] Uz to, korištenjem senzora i pridruživanjem potrebnih metapodataka osigurala bi se transparentnost, uračunljivost i društvena odgovornost svih strana uključenih u distribuciju nekog proizvoda.[105]

Nadalje, *blockchain* bi mogao izmijeniti organizacije i njihove procese zapošljavanja stvaranjem distribuirane mreže poslodavaca i zaposlenika u kojima bi se bilježile sve interakcije u organizaciji. Na taj bi se način otklonila mogućnost kandidata za posao da lažiraju svoje reference, ali i organizacija da skrivaju neetične prakse.[106] Zaposlenici i poslodavci posjedovali bi nepromjenjiv digitalni trag u obliku bodova koji bi se akumulirali i u teoriji olakšavali pronalaženje posla, ali i zaposlenika.[107] Uz to, *blockchain* ima velik potencijal otvaranja financijskih i računovodstvenih praksi organizacija prema van kako bi se izbjegle pronevjere.[108]

Još jedna potencijalna primjena tehnologije bila bi za utvrđivanje metodologije istraživanja u medicini. Naime, u posljednjim je godinama došlo do krize reproducibilnosti istraživanja u znanstvenim publikacijama. Prema Ioannidis preko 80 % studija nemoguće je reproducirati.[109] Benchoufi predlaže praćenje kronološkog slijeda događaja u istraživanju kroz *blockchain* što bi onemogućilo naknadne prilagodbe i izmjene podataka. Pri tom bi se podaci poput rasporeda ispitivanja, dokumentacije, pristanka ispitanika, plana statističke analize vremenski označili i pohranili kao prvi blok čime bi se izbjeglo odstupanje te nepotpuno ili pristrano iznošenje podataka u istraživanjima.[110]

Posljednja i vjerojatno najviše utopistička primjena *blockchaina* bila bi decentralizirana vlast. Naime, pobornici tehnologije tvrde kako bi se civilno društvo moglo organizirati i štititi vlastite interese bolje i učinkovitije zamjenom tradicionalnih funkcija države s uslugama zasnovanim na *blockchainu* i decentraliziranim platformama u otvorenom pristupu. Neki autori smatraju tradicionalnu vladu opterećenjem navodeći kako je suviše spora, nedovoljno inovativna

[104] Usp. O'Connor, Chris. What blockchain means for you, and the Internet of Things, 10. 02. 2017. URL: https://www.ibm.com/blogs/internet-of-things/watson-iot-blockchain/ (2018-08-13)
[105] Usp. Lee, Jong-Hyouk; Pilkington, Marc. Nav. dj. Str 21.
[106] Usp. Tapscott, Don; Tapscott, Alex. How the blockchain will change organizations. // MIT Sloan: management review 58, 2(2017), str. 11. URL: http://sloanreview.mit.edu/article/how-blockchain-will-change-organizations/ (https://docs.m0m0g33k.net/python/mitsmr2017winter-dl.pdf) (2018-08-13)
[107] Usp. Mamoria, Mohit. Every company will use blockchain by 2027, 20. 10. 2017. URL: https://hackernoon.com/your-company-will-use-blockchain-in-less-than-10-years-heres-how-6d9da452fa8d (2018-08-13)
[108] Usp. Tapscott, Don; Tapscott, Alex. Nav. dj. Str 11-12.
[109] Usp. Ioannidis JPA. Why most published research findings are false. // PloS Medicine 2, 8(2005), 124. URL: http://journals.plos.org/plosmedicine/article/file?id=10.1371/journal.pmed.0020124&type=printable (2018-08-13)
[110] Usp. Benchoufi, Mehdi; Ravaud, Philippe. Blockchain technology for improving clinical research quality. // Trials 18 (2017), 335. URL: https://trialsjournal.biomedcentral.com/articles/10.1186/s13063-017-2035-z (2018-08-13)

te pogoduje malim skupinama u društvu. Uz to dolazi do oblikovanja struja koje smatraju kako smo u razdoblju povijesti u kojem pojedinci mogu zamijeniti bilo koju centraliziranu političku instituciju putem distribuiranog konsenzusa i stvoriti uvjete za idealno društvo jednakosti zasnovano na plošnim strukturama. *Blockchain* bi se pritom mogao koristiti za stvaranje slojevitijih i personaliziranijih usluga vlade pri čemu bi izvor legitimnosti bili pojedinci bez upotrebe prisile. Na ovaj način bi se stvorio sustav izravne demokracije u kojem bi građani bili uključeni u proces donošenja političkih odluka. *Blockchain* bi predstavljao trajni repozitorij javnih zapisa vođen algoritmima i pravilima slobodnog tržišta u kojem bi vlada bila predstavljena svim članovima u mreži umjesto odabranim pojedincima. Nažalost, jasno je da su ovakve ideje zasnovane na pretjeranoj idealizaciji *blockchaina* kao rješenja svih problema modernog tržišta i društva. Prije svega, u pitanju je mlada i ranjiva tehnologija čije se primjene još uvijek razvijaju i testiraju, i iako je tehnološki napredak donio brojne prednosti svakodnevnom životu, naivno je ulogu vlade spuštati na mrežu trenutnih mikro-interakcija koje su u potpunosti automatizirane. Politika i vladanje ipak su više od agregiranja glasova, sinkronizacije baza i prisilnog provođenja transakcija – algoritmi nisu namijenjeni za zakonodavstvo.[111]

Ipak, neovisno o ishodu nekih ranije navedenih primjena *blockchaina*, ohrabrujuće je vidjeti da se primjenjivost tehnologije promišlja u različitim dimenzijama. Stoga posebno zanimanje bude napori da se problemi znanstvene zajednice poput lažnog čimbenika odjeka (eng. *impact factor*) i krize reproducibilnosti istraživanja riješe kroz *blockchain*.

5.1. *Blockchain* za znanost

Ključna značajka znanstvenih istraživanja je reproducibilnost. Budući da je cilj znanosti unaprijediti društvo, ona nikada ne bi trebala biti svrha sama sebi. Istraživanja bi se trebala provoditi s ciljem pomicanja granica i reproducibilnošću rezultata kao temeljnim konstruktom. Stoga je kriza reproducibilnosti i lažnog čimbenika odjeka koja se pojavila u znanstvenoj zajednici ozbiljna prijetnja da znanost svede na razinu samopromocije i ugleda umjesto ključnog elementa ljudskog napretka.[112]

[111] Usp. Atzori, Marcella. Blockchain technology and decentralized governance: is the state still necessary?, 01. 12. 2015, str. 4. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2709713 (2018-08-13)
[112] Usp. Furlanello, Cezare et al. Towards a scientific blockchain framework for reproducible data analysis, 20. 07. 2017. URL: https://arxiv.org/pdf/1707.06552.pdf (2018-08-13)

Ioannidis je u ranije spomenutom istraživanju otkrio izrazito nisku stopu reproducibilnosti objavljenih istraživanja koju smatra posljedicom izvlačenja zaključaka na osnovi malog broja studija sa statističkim značajem. Pri tome navodi nekoliko čimbenika koji mogu utjecati na ishod istraživanja. Prije svega, jedan od uzroka je pristranost koja predstavlja kombinaciju dizajna, prikupljanja podataka i njihove analize te prezentacije koji mogu uzrokovati produkciju rezultata onda kada ih ne bi trebalo biti. Pri tome do manipulacije rezultatima najčešće dolazi u fazi analize podataka ili selektivnoj prezentaciji. Nadalje, u slučajevima provjeravanja istih hipoteza u izoliranim timovima često dolazi i do izoliranih i oprečnih otkrića što je dovoljna inicijativa da se ista prilagode kako bi se dobili željeni rezultati. Otkriveno je kako istraživanja s manjim uzorcima često imaju manju vjerodostojnost, a istinitost rezultata ovisna je i o fleksibilnosti definicija pri čemu će veća fleksibilnost polučivati manje vjerodostojne rezultate. Autor u konačnici ne isključuje ni financijske interese kao ni predrasude unutar znanstvenog područja navodeći da iako predrasude ne moraju imati financijsku podlogu, istraživanja temeljena na financijskom interesu i predrasudama najčešće nisu vjerodostojna. Spoj navedenih čimbenika doveo je do rastućeg tijela nereproducibilnih istraživanja te Ioanndisovog zaključka kako je čak 85 % objavljenih istraživanja nereproducibilno.[113]

K tomu treba dodati i rastući broj lažnih tvrtki koje tvrde da izračunavaju čimbenik odjeka za znanstvene publikacije i koje su neprimijećene uspjele ući i u recenzirane dobrostojeće publikacije. Jalalian je 2013. godine otkrio i prijavio pet takvih tvrtki, najčešće smještenih u Aziji, čije su neetične poslovne prakse između ostalog uključivale pisanje završnih radova i disertacija te korištenje identiteta uglednih izdavačkih kuća. Iako se ne može reći kako su napori autora bili uzaludni, činjenica je kako nije uspio zaustaviti širenje ove prakse te je već 2015. godine otkrio ukupno tridesetak lažnih tvrtki za izračunavanje čimbenika odjeka.[114]

Ova kriza u zajednici nagnala je nekolicinu autora da se okrenu alternativnim rješenjima problema. Neki od njih smatraju kako bi migracija znanstvene zajednice na *blockchain* mogla na istraživanja staviti spregu i ponovno ih podići na razinu kvalitete koja je vremenom izgubljena. Imajući na umu navedenu problematiku Furlanello tvrdi kako trenutni znanstveni sustav neprimjereno nagrađuje članove zajednice koji ulažu napore u provođenje rigoroznih i reproducibilnih istraživanja te predlaže mrežu PROBO zasnovanu na *blockchainu* koja bi kroz sustav ugleda nagrađivala istraživače sredstvima za financiranje daljnjih istraživanja i kupnju

[113] Usp. Ioannidis, J.P.A. Nav. dj.
[114] Usp. Jalalian, Mehrdad. The story of fake impact factor companies and how we detected them. // Electron Physician 7, 2(2015), str. 1069-1072. URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4477767/ (2018-08-13)

opreme.[115] Na istom tragu je Rossum koji navodi kako su znanstvena istraživanja u svojoj biti veliko dinamično tijelo podataka koje se zajedničkim naporima stvara, mijenja, koristi i dijeli te kako su kao takva savršena za migraciju na *blockchain*. U svom radu se dotiče inicijative *Blockchain for Research*, koju predvodi Soenke Bartling, usmjerene na uspostavu distribuirane mreže za stvaranje i održavanje rastućeg tijela znanstvenih istraživanja. Naravno, uspješno prihvaćanje *blockchaina* u ovom kontekstu zahtijeva široku usvojenost od strane institucija, izdavača i samih znanstvenika, ali su potencijalne prednosti nemoguće za ignorirati. Prije svega, stvaranje ujedinjene decentralizirane platforme za znanstveni rad zasnovane na *blockchain* tehnologiji otvorilo bi nove dimenzije akademske komunikacije – budući da se vlasništvo nad sadržajem automatski uspostavlja kroz *blockchain* uklonila bi se potreba za patentnim uredima i izdavačima. Nadalje, sve interakcije unutar mreže bile bi pohranjene čime bi se unaprijedili koncepti povjerenja, čestitosti, zasluga i univerzalnog pristupa informacijama. Registracijom istraživanja u *blockchain* izbjegla bi se eventualna cenzura te proizvodnja nereproducibilnih rezultata budući da bi naknadna izmjena i prilagodba podataka bila nemoguća. U konačnici, takav bi pristup znatno olakšao prikupljanje pouzdanih i kompletnih podataka o izvedbi znanstvenika čime bi se omogućilo stvaranje sofisticiranijih i pouzdanijih metrika. Uključivanjem nekog oblika kriptovalute omogućilo bi se stvaranje sustava koji znatno pravednije raspodjeljuje sredstva čime bi se istraživačima olakšala nabava opreme i financiranje budućih istraživanja.[116]

Činjenica je kako je *blockchain* za znanost ideja do čije će konačne implementacije proći dugi niz godina, ali ona predstavlja dobar prvi korak za poticanje rasprave o korisnosti ove tehnologije u akademskoj zajednici. Međutim, ostaje još odgovoriti na temeljno pitanje ovog rada – je li *blockchain*, i u kojoj mjeri, primjenjiv na problematiku zaštite i očuvanja digitalnih podataka?

5.2. *Blockchain* kao odgovor na probleme digitalne zaštite

Nekolicina radova dostupnih na temu uglavnom je zasnovana na konceptualnim modelima i pretpostavkama te je potrebno naglasiti kako neki autori nisu otporni na blagonaklonost prema *blockchainu* koja najvjerojatnije proizlazi iz njegove razvikanosti. Međutim, Miller i njegov tim ozbiljnije su se pozabavili problematikom zaštite i očuvanja digitalnih podataka u distribuiranoj

[115] Usp. Furlanello, Cezare et al. Nav. dj.
[116] Usp. Rossum, Van Joris. Blockchain for research: perspectives on a new paradigm for scholarly communication. London: Digital Science, 2017. Str. 8-15. URL: https://figshare.com/articles/Blockchain_for_Research/5607778/1

blockchain mreži te dokazali kako je moguće prilagoditi arhitekturu Bitcoina za potrebe pohrane velikog skupa podataka. Ovaj model naziva se Permacoin a temeljen je na korištenju rudarenja koje ovisi o lokalnom prostoru pohrane, a ne računalnoj snazi. Radi se o prilagodbi *proof-of-work* mehanizma koju autor naziva *proof-of-retrievabilty*. Dakle, u sustavu koji je zadužen za zaštitu i očuvanje digitalnih podataka članovi trebaju dokazati namjenu prostora za pohranu kako bi uspješno spremili objekt ili njegov fragment, a ključna značajka sustava je mogućnost povrata i pristupa informacijskim objektima spremljenim u mreži. Razvojem konceptualnog modela Miller i njegov tim uspješno su dokazali neospornost primjene *blockchaina* za zaštitu i očuvanje digitalnih podataka navodeći kako bi mreža veličine Bitcoina mogla pohraniti skup podataka sličan onom koji se čuva u Kongresnoj knjižnici.[117] Međutim, Millerov rad nije se bavio pitanjima autentičnosti i pouzdanosti, niti je u obzir uzeo zadovoljavanje kriterija izvodljivosti, održivosti, praktičnosti i prikladnosti potrebnih za uspostavu takvog sustava. Permacoin jest dokaz potencijala *blockchaina* za dugotrajnu zaštitu i očuvanje digitalnih podataka, ali nije nužno razlog za slavlje. *Blockchain* u svom trenutnom stanju posjeduje određene probleme čijim se raščlanjivanjem može dobiti potpuniji odgovor na praktičnost primjene ove tehnologije za zaštitu i očuvanje digitalnih podataka.

Već je zaključeno kako su autentičnost i integritet podataka u srži *blockchaina*, a značajka tehnologije da stvori trajni zapis aktivnosti i izmjena ide ruku pod ruku s idejom L. Duranti o mogućnosti sustava da evidentira sve izmjene na svim digitalnim informacijskim objektima čime bi se očuvao njihov integritet. U suštini se radi o sustavu za verzioniranje s važnom prednošću *blockchaina* da evidenciju vodi automatski te svaki novi zapis enkriptira i učini nepromjenjivim. Dakle, svaka izmjena na informacijskim objektima u sustavu uz sebe bi mogla imati pridružene metapodatke o samom objektu kao i osobi koja ga je izmijenila te podacima o tome koje su razine objekta izmijenjene i na koji način. Mogućnost pridruživanja samog informacijskog objekta uz zapis značila bi stvaranje sigurnosne kopije objekta s posljednjim izmjenama koja bi se također čuvala u *blockchainu*. Nadalje, upotrebljivost objekta bila bi osigurana kroz njegovu distribuciju u mreži. Budući da bi se *blockchain* istovremeno pohranjivao na velik broj računala, rizik od kvara centralne infrastrukture ili gubitka podataka uslijed prirodnih katastrofa bio bi znatno manji te bi se podacima moglo pristupiti dok bi u mreži postojali aktivni članovi. To, naravno, ne isključuje

[117] Usp. Miller, Andrew et al. Permacoin: repurposing bitcoin work for data preservation. // 2014 IEEE Symposium on Security and Privacy. IEEE: 2014. Str 475-477. URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6956582 (2018-08-13)

mogućnost pohranjivanja cijelog niza podataka na udaljenoj lokaciji koja bi u mrežu bila uključena samo kako bi povukla posljednju verziju baze.[118]

Ipak, problemi se javljaju pri zadovoljavanju kriterija uspostave *blockchain* sustava za zaštitu i očuvanje digitalnih podataka. Prije svega, može se zaključiti kako bi kriteriji izvodljivosti i održivosti bili dobrim dijelom zadovoljeni. Naime, *blockchain* ne iziskuje nikakva posebna tehnička rješenja, a uzme li se u obzir da sustav za zaštitu i očuvanje digitalnih podataka ne bi zahtijevao konstantne nadogradnje za utrku u računalnoj moći šanse su da bi tehničko okruženje za implementaciju *blockchaina* već postojalo. S druge strane, budući da se radi o novoj tehnologiji, pitanje je je li moguće pronaći dovoljno stručan kadar za uspostavu *blockchaina*? Nadalje, upravo iz razloga što se radi o izrazito popularnoj i novoj tehnologiji, pretpostavka da bi postojala njezina logična nadogradnja je utemeljena. Međutim, praktičnost izvedbe dovodi u pitanje cijelu operaciju. Naime, u svom istraživanju primjenjivosti *blockchaina* na zaštitu i očuvanje digitalnih podataka Lemeiux je došla do zaključka da iako tehnologija podržava autentičnost i integritet, stvaranje distribuiranog decentraliziranog sustava u pitanje bi dovela pouzdanost. Budući da sustav ne bi posjedovao centralno tijelo za provjeru autentičnosti podataka koji u njega ulaze, šanse su da bi informacijski objekti prilikom ulaska u sustav bili neautentični i nepouzdani. Dakle, sustav za zaštitu i očuvanje digitalnih podataka temeljen na *blockchainu* morao bi imati neki oblik sprege pri unošenju informacijskih objekata u mrežu. Međutim, uzme li se u obzir da članovi unutar mreže ne bi nužno morali biti stručnjaci u području zaštite i očuvanja podataka, moralo bi postojati centralno tijelo za provjeru autentičnosti objekata čime bi se jedna od glavnih značajki tehnologije morala u potpunosti zaobići. Nadalje, pitanje je koja bi inicijativa postojala iza uključenja i održavanja jednog ovakvog sustava? U sustavima kriptovaluta poput Bitcoina inicijativa je vrlo jasna – vrijednost valute održavat će mrežu na životu, a novčana nagrada iza uspješnog rudarenja osigurat će njezin rast. Ali što bi nagnalo pojedince za uključenje u sustav u kojem potencijalno ne postoji nikakva nagrada za obavljanje dužnosti? Činjenica jest da građanska svijest raste po pitanju informacijske privatnosti i cenzure, ali postoji šansa da opće dobro nije dovoljno dobar razlog da se ovakav sustav održi na životu. Kako bi se osigurao od propasti, sustav bi prilikom svoje uspostave najvjerojatnije morao uključiti određeni broj članova koji bi ga održavali na životu čak i ako mreža ne bi uspjela rasti. Međutim, time se ponovno u pitanje dovodi decentraliziranost, budući da bi iza takve organizacije moralo postojati centralno tijelo. U konačnici, iako takav ishod

[118] Usp. Duranti, Luciana. The long-term preservation of accurate and authentic digital data: the InterPARES Project. // Data Science Journal 4(2005), str. 107. URL: https://www.researchgate.net/publication/228846879_The_Long-Term_Preservation_of_Accurate_and_Authentic_Digital_Data_The_InterPARES_Project (2018-07-25)

nije poželjan, može se zaključiti kako bi prikladnost implementacije sustava za zaštitu i očuvanje digitalnih podataka na *blockchain* bila tek djelomično zadovoljena te je stoga razumljiv nedostatak konkretnih institucionalnih projekata u ovom području.[119]

Potencijal *blockchaina* je neupitan, međutim tehnologija je nova i nedovoljno testirana da bi u kratkom razdoblju u kojem postoji mogla polučiti punokrvnu primjenu u mnoštvu različitih sustava. Dizajniran s autentičnošću i integritetom podataka na umu, *blockchain* je primjenjiv u brojnim drugim slučajevima izvan područja financija. Međutim, njegova implementacija, posebice u slučaju zaštite i očuvanja digitalnih podataka sa sobom donosi više pitanja nego odgovora te je razumljivo da se njezinoj konkretizaciji još uvijek nije posvetilo previše vremena. Ipak, činjenica je kako će *blockchain* vremenom naći svoju primjenu – Bitcoin vode ljudi, ljudi definiraju njegovu upotrebu, ali će tehnologija biti ta koja će na kraju odlučiti koje su njezine primjene moguće i pouzdane.[120]

6. ZAKLJUČAK

Iako je praksa zaštite i očuvanja podataka evoluirala kako bi uz analogne informacijske objekte obuhvatila i digitalne, pouzdanost i autentičnost ostali su ključni čimbenici napora očuvanja. Problematika ovog područja proizlazi iz raznolikosti informacijskih objekata i broja metoda potrebnih za njihovo održavanje te zaštitu i očuvanje podataka koji sačinjavaju takve objekte. K tomu treba dodati i konstantu utrku s tehnološkim napretkom gubitak koje bi onemogućio pristup ogromnom skupu podataka koji se najčešće čuva za opće dobro. Digitalno doba je sa sobom donijelo i problematiku informacijske privatnosti te ideju da je pored korisničkih podataka potrebno zaštititi i podatke koji se čuvaju u repozitorijima, a koji su sve češće dani na provedbu vanjskom izvoditelju i pohranjeni na infrastrukturi nekog od nekolicine centraliziranih tehnoloških divova.

Blockchain tehnologija nudi rješenje problemu rastuće centraliziranosti kroz distribuirani zapis povijesti aktivnosti u decentraliziranoj mreži. Inovativan pristup razrješavanju problema informacijske privatnosti te autentičnost i integritet podataka kao temeljni čimbenici ove tehnologije omogućili su *blockchainu* da u manje od desetljeća pronađe primjene izvan svoje prvotne implementacije u kriptovalutnim sustavima. Posebno zanimljiv koncept je primjena

[119] Usp. Lemeiux, Victoria Louise. Nav. dj. Str 125.
[120] Usp. Lazarovich, Amir. Invisible ink: blockchain for data privacy: master's degree. Massachusetts: Massachusetts Institute of Technology, 2015. Str. 25. URL: https://dspace.mit.edu/handle/1721.1/98626 (2018-08-15)

blockchaina za stvaranje distribuirane baze znanstvenih istraživanja koja bi znanstvenicima omogućila izravniji i otvoreniji pristup radu njihovih kolega. Uspostavom ovakvog sustava uklonila bi se potreba za posrednicima u obliku izdavačkih kuća i patentnih ureda čime bi se olakšala proizvodnja reproducibilnih istraživanja neopterećenih vanjskim interesima. Nesumnjivo je kako bi u ovakvom okruženju pojam otvorenog pristupa poprimio svoje pravo značenje jer bi bazu znanstvenih istraživanja održavala samo i jedino znanstvena zajednica bez uplitanja i kontrole interesnih skupina. Ipak, na umu treba imati kako se radi o idealnim prognozama koje još nisu provjerene u stvarnom okruženju i za čiju potpunu implementaciju treba proći dugi niz godina obilježen pravnim bitkama i procesom šireg usvajanja tehnologije.

Veliki i stalno rastući broj autora koji se bave ovom problematikom često ignorira probleme ove tehnologije te idealizira *blockchain* kao konačno rješenje svih problema modernog društva. Ovaj rad je tehnologiju pojasnio te sagledao na koji način ona doprinosi očuvanju informacijske privatnosti i autentičnosti digitalnih podataka. Odgovor na pitanje o primjeni *blockchaina* na zaštitu i očuvanje digitalnih podataka nažalost nije pozitivan. Dok *blockchain* izrazito dobro rješava problem autentičnosti, pouzdanost informacijskih objekata predstavlja problem koji ova tehnologija ne može razriješiti bez poništavanja nekih njezinih osnovnih značajki. U konačnici, sustav za zaštitu i očuvanje digitalnih podataka zasnovan na *blockchainu* trenutno predstavlja enigmu koja se vjerojatno neće razriješiti u kratkom roku. *Blockchain* je izrazito moćna tehnologija s ogromnim potencijalom, ali umjesto njezina idealiziranja potrebno je napraviti korak unatrag i dozvoliti joj da sazre prije nego se počne upotrebljavati u širokom spektru slučajeva.

LITERATURA

Atzori, Marcella. Blockchain technology and decentralized governance: is the state still necessary?, 01. 12. 2015. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2709713 (2018-08-13)

Baker, Cathleen Ann. The Florence Flood, 1966: what we learned, 19. 12. 2016. URL: https://www.lib.umich.edu/blogs/beyond-reading-room/florence-flood-1966-what-we-learned (2018-07-20)

Beal, George. Industries with heavy supply chains face major problems. Blockchain tech might be the answer, 31. 10. 2017. URL: https://thenextweb.com/contributors/2017/10/31/supply-chains-blockchain-tech/ (2018-08-12)

Belanger, France; Crossler, Robert E. Privacy in the digital age: a review of information privacy research in information systems. // MIS Quarterly 35(2011), str. 1017-1041. URL: https://www.researchgate.net/publication/220259962_Privacy_in_the_Digital_Age_A_Review_of_Information_Privacy_Research_in_Information_Systems (2018-08-02)

Benchoufi, Mehdi; Ravaud, Philippe. Blockchain technology for improving clinical research quality. // Trials 18 (2017), 335. URL: https://trialsjournal.biomedcentral.com/articles/10.1186/s13063-017-2035-z (2018-08-13)

Boaventura, Andre. Demystifying blockchain and concesus mechanisms – everything you wanted to know but were never told, 12.4. URL: https://medium.com/oracledevs/demystifying-blockchain-and-consensus-mechanisms-everything-you-wanted-to-know-but-were-never-aabe62145128 (2018-08-11)

Cloud services. // Digital preservation handbook: URL: https://www.dpconline.org/handbook/technical-solutions-and-tools/cloud-services (2018-07-25)

Conway, Paul. Preservation in the age of Google: digitization, digital preservation, and dilemmas. // Library Quarterly 80, 1(2010), str. 61-79. URL: https://deepblue.lib.umich.edu/bitstream/handle/2027.42/85223/J15%20Conway%20Preservation%20Age%20of%20Google%202010.pdf?sequence=1 (2018-07-21)

Czarnek, Matthew; Secondleo. Nxt network: energy and cost efficiency analysis. 2014. URL: https://www.scribd.com/document/254930279/Nxt-Network-Energy-and-Cost-Efficiency-Analysis (2018-09-06)

De Filippi, Primavera. The interplay between decentralization and privacy: the case of blockchain technologies. // Journal of Peer Production 7(2016), str. 1-19. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2852689 (2018-08-11)

Distributed databases. URL: https://docs.oracle.com/cd/A57673_01/DOC/server/doc/SCN73/ch21.htm (2018-08-10)

Dorraji, Seyed Ebrahim; Barcys, Mantas. Privacy in digital age: dead or alive?!: regarding the new EU data protection regulations. // Social technologies 4, 2(2014), str. 306-317. URL: https://www3.mruni.eu/ojs/social-technologies/article/view/2047/3805 (2018-08-02)

Duranti, Luciana. The long-term preservation of accurate and authentic digital data: the InterPARES Project. // Data Science Journal 4(2005), str. 106-118. URL: https://www.researchgate.net/publication/228846879_The_Long-Term_Preservation_of_Accurate_and_Authentic_Digital_Data_The_InterPARES_Project (2018-07-25)

Encapsulation. 23. 5. 2011. URL: https://digitalpreservationpg.wordpress.com/tag/encapsulation/ (2018-07-27)

Findlay, Cassie. Decentralised and inviolate: the blockchain and its uses for digital archives, 23. 01. 2015. URL: https://rkroundtable.org/2015/01/23/decentralised-and-inviolate-the-blockchain-and-its-uses-for-digital-archives/ (2018-08-12)

Furlanello, Cezare et al. Towards a scientific blockchain framework for reproducible data analysis, 20. 07. 2017, str 1-8. URL: https://arxiv.org/pdf/1707.06552.pdf (2018-08-13)

Ioannidis JPA. Why most published research findings are false. // PloS Medicine 2, 8(2005), 124. URL: http://journals.plos.org/plosmedicine/article/file?id=10.1371/journal.pmed.0020124&type=printable (2018-08-13)

Jacobson, Ralph. 2.5 quintillion bytes of data created every day. How does CPG & Retail manage it?, 24. 4. 2013. URL: https://www.ibm.com/blogs/insights-on-business/consumer-products/2-5-quintillion-bytes-of-data-created-every-day-how-does-cpg-retail-manage-it/ (2018-07-27)

Jalalian, Mehrdad. The story of fake impact factor companies and how we detected them. // Electron Physician 7, 2(2015), str. 1069-1072. URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4477767/ (2018-08-13)

Lazarovich, Amir. Invisible ink: blockchain for data privacy: master's degree. Massachusetts: Massachusetts Institute of Technology, 2015, str 3-85. URL: https://dspace.mit.edu/handle/1721.1/98626 (2018-08-15)

Lee, Jong-Hyouk; Pilkington, Marc. How the blockchain revolution will reshape the consumer electronics industry. // IEEE Consumer Electronics Magazine 4(2017), str. 19-23. URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7948864 (2018-08-12)

Lemeiux, Victoria Louise. Trusting records: is Blockchain technology the answer?. // Records Management Journal 26, 2 (2016), str. 110-139. URL: http://www.emeraldinsight.com/doi/pdfplus/10.1108/RMJ-12-2015-0042 (2018-08-12)

Malmo, Christopher. Bitcoin is unsustainable, 29. 6. 2015. URL: https://motherboard.vice.com/en_us/article/ae3p7e/bitcoin-is-unsustainable (2018-08-11)

Mamoria, Mohit. Every company will use blockchain by 2027, 20. 10. 2017. URL: https://hackernoon.com/your-company-will-use-blockchain-in-less-than-10-years-heres-how-6d9da452fa8d (2018-08-13)

Marcum, Deanna. Introduction: the changing preservation landscape. // The state of digital preservation: an international perspective. Conference proceedings. Washington: Council on library and information resources, 2002. Str. 1-3. URL: https://www.clir.org/wp-content/uploads/sites/6/pub107.pdf (2018-07-27)

Miller, Andrew...[et al.]. Permacoin: repurposing bitcoin work for data preservation. // 2014 IEEE Symposium on Security and Privacy. IEEE: 2014, str 475-490. URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6956582 (2018-08-13)

Nakamoto, Satoshi. Bitcoin: a Peer-to-Peer electronic cash system. Str. 1-9. URL: https://bitcoin.org/bitcoin.pdf (2018-08-07)

O'Connor, Chris. What blockchain means for you, and the Internet of Things, 10. 02. 2017. URL: https://www.ibm.com/blogs/internet-of-things/watson-iot-blockchain/ (2018-08-13)

Oliver, Gillian; Knight, Steve. Storage is a strategic issue: digital preservation in the cloud. // D-Lib Magazine 21, 3/4(2015). URL: http://www.dlib.org/dlib/march15/oliver/03oliver.html (2018-07-25)

Posey, Brien. Understanding the differences between client/server and peer-to-peer networks, 26. 5. 2000. URL: https://www.techrepublic.com/article/understanding-the-differences-between-client-server-and-peer-to-peer-networks/ (2018-08-10)

Privacy and information technology. // Stanford encyclopedia of philosophy, 20. 11. 2014. URL: https://plato.stanford.edu/entries/it-privacy/ (2018-07-30)

Proof of capacity (Cryptocurrency). URL: https://www.investopedia.com/terms/p/proof-capacity-cryptocurrency.asp (2018-08-11)

Public key cryptography. URL: https://www.ibm.com/support/knowledgecenter/en/SSB23S_1.1.0.13/gtps7/s7pkey.html (2018-08-07)

Reddy Kolle, Shankar et al. Strategies and techniques for preservation of digital resources. // PEARL: A Journal of Library and Information Science 8, 4(2014), str. 221-225. URL: https://www.researchgate.net/publication/273506866_Strategies_and_Techniques_for_Preservation_of_Digital_Resources (2018-07-25)

Rights of privacy. // Encyclopaedia Britannica Online. Encyclopedia Britannica. URL: https://www.britannica.com/topic/rights-of-privacy (2018-08-02)

Rogers, Corinne. Authenticity of digital records: a survey of professional practice. // Canadian journal of information and library science 39, 2(2015), str. 97-113. URL: https://muse.jhu.edu/article/590936/summary (2018-07-30)

Rossum, Van Joris. Blockchain for research: perspectives on a new paradigm for scholarly communication. London: Digital Science, 2017. URL: https://figshare.com/articles/Blockchain_for_Research/5607778/1 (2018-08-13)

Sannet, Shelby; Park, Eun. Authenticity as a requirement of preserving digital data and records. // IASSIST Quarterly 24 (2000), str. 15-18. URL: http://www.interpares.org/display_file.cfm?doc=ip1_dissemination_jar_sanett~park_iassist_quarterly_24_2000.pdf (2018-07-23)

Stančić, Hrvoje. Arhivsko gradivo u elektroničkom obliku: mogućnosti zaštite i očuvanja na dulji vremenski rok. // Arhivski vjesnik 49, 1(2006), str. 107-121. URL: https://hrcak.srce.hr/index.php?show=clanak&id_clanak_jezik=9508 (2018-07-23)

Tapscott, Don; Tapscott, Alex. How the blockchain will change organizations. // MIT Sloan: management review 58, 2(2017), str. 10-13. URL: http://sloanreview.mit.edu/article/how-blockchain-will-change-organizations/ (https://docs.m0m0g33k.net/python/mitsmr2017winter-dl.pdf) (2018-08-13)

Toarna, Alina; Cojanu, Valentin. The 2008 crisis: causes and future direction for the academic research. // Procedia Economics and Finance 27(2015), str. 385-393. URL: https://www.sciencedirect.com/science/article/pii/S2212567115010102 (2018-08-05)

Thibodeau, Kenneth. Overview of technological approaches to digital preservation and challenges to coming years. Conference proceedings. Washington: Council on library and

information resources, 2002. Str. 4-31. URL: https://www.clir.org/wp-content/uploads/sites/6/pub107.pdf (2018-07-27)

Uruqhart, Andrew. The inefficiency of bitcoin. 2016, str 1-7. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2828745 (2018-08-07)

Verma, Shalini. Forecast: consumer digital storage needs, 2010-2016, 2012. URL: http://www.gartner.com/newsroom/id/2060215 (2018-09-05)

Wararkar, Pravin...[et al.]. Resolving problems based on Peer to Peer network security issue's. // Procedia Computer Science 78(2016), str. 652-659. URL: https://www.researchgate.net/publication/301234162_Resolving_Problems_Based_on_Peer_to_Peer_Network_Security_Issue's (2018-08-10)

What is hashing: under the hood of Blockchain. URL: https://blockgeeks.com/guides/what-is-hashing/ (2018-08-10)

Williamson, Andrew. Strategies for managing digital content formats. // Library Review 54, 9 (2005), str. 508-513. URL: https://strathprints.strath.ac.uk/2295/1/strathprints002295.htm (2018-07-24)

Witte, J. H. The Blockchain: a gentle four page introduction. 2016., str. 1-5. URL: https://arxiv.org/pdf/1612.06244.pdf (2018-08-07)

Zych, Izabela...[et al.]. Causes and solutions for the economic crisis according to the International Scientific Community. // Universitas Psychologica 14, 1(2015), str. 367-380. URL: http://revistas.javeriana.edu.co/index.php/revPsycho/article/view/6105/10622 (2018-08-05)

Zyskind, Guy; Nathan, Oz; Pentland, Alex. Decentralizing privacy: using Blockchain to protect personal data. // 2015 IEEE Security and Privacy Workshops. San Jose: IEEE, 2015. URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7163223 (2018-08-02)