Blockchain - nova tehnologija zaštite podataka

Vlahović, Marko

SVEUČILIŠTE SJEVER

SVEUČILIŠNI CENTAR VARAŽDIN

DIPLOMSKI RAD br. 330/PE/220

BLOCKCHAIN – NOVA TEHNOLOGIJA ZAŠTITE PODATAKA

Marko Vlahović

Varaždin, srpanj 2020.

SVEUČILIŠTE SJEVER

SVEUČILIŠNI CENTAR VARAŽDIN

Studij Poslovna ekonomija, Međunarodna trgovina

DIPLOMSKI RAD br. 330/PE/2020

BLOCKCHAIN – NOVA TEHNOLOGIJA ZAŠTITE PODATAKA

Student:

Marko Vlahović, 0685/336D

Mentor:

doc. dr. sc. Petar Mišević

Varaždin, srpanj 2020.

Sveučilište Sjever
Sveučilišni centar Varaždin
104. brigade 3, HR-42000 Varaždin

Prijava diplomskog rada

Definiranje teme diplomskog rada i povjerenstva

ODJEL Odjel za ekonomiju

STUDIJ diplomski sveučilišni studij Poslovna ekonomija

PRISTUPNIK Marko Vlahović | MATIČNI BROJ 0685/336D

DATUM 12.03.2020. | KOLEGIJ Korporativna sigurnost

NASLOV RADA Blockchain - nova tehnologija zaštite podataka

NASLOV RADA NA ENGL. JEZIKU Blockchain - new data protection technology

MENTOR Petar Mišević | ZVANJE doc.dr.sc.

ČLANOVI POVJERENSTVA
1. izv.prof.dr.sc. Ante Rončević, predsjednik
2. izv.prof.dr.sc. Anica Hunjet, član
3. doc.dr.sc. Petar Mišević, mentor
4. doc.dr.sc. Darijo Čerepinko, zamj.član
5.

Zadatak diplomskog rada

BROJ 330/PE/2020

OPIS

Svakodnevan život i poslovanje u današnje doba nisu mogući bez interneta, mobitela i osobnog računala. Zbog toga je zaštita digitalne imovine i osobnih podataka od sve veće važnosti za pravne i fizičke osobe, s obzirom na sve veće rizike i ugroze od računalnog kriminaliteta. Ulaganje u informacijsku sigurnost ne predstavlja trošak već jamči konkurentsku prednost i opstanak organizacije na tržištu.
U diplomskom radu je potrebno:
- objasniti pojam Blockchain tehnologije i način na koji ista doprinosi očuvanju informacijske privatnosti i autentičnosti digitalnih podataka,
- načini funkcioniranja Blockchain tehnologije u digitalnom poslovanju,
- analizirati zakonske propise koji reguliraju obradu podataka u informacijskim sustavima,
- definirati područja informacijske sigurnosti i aktualne rizike i ugroze,
- obraditi strukturu, primjenu i budući razvoj blockchain tehnologije,
- provesti istraživanje u obliku ankete vezano uz implementaciju informacijske sigurnosti u zaštiti podataka te razine educiranosti korisnika od računalnih ugroza,
- obraditi rezultate istraživanja i definirati zaključak diplomskog rada.

ZADATAK URUČEN | POTPIS MENTORA

Predgovor

Od svog osnutka 2008. godine, blockchain je i dalje izvor revolucionarnih mogućnosti i rješenja. Blockchain se može opisati kao zapis svih provedenih transakcija koji je transparentan i dostupan svima, a istovremeno otporan na manipulacije treće strane.

Iako je prvenstveno razvijena za digitalne valute, blockchain tehnologija razvila se u mnogo više i probila je granice prvotne namjene. Sama ideja i koncept decentraliziranog sustava i uspješne implementacije digitalnog peer-to-peer sustava bio je prijeko potreban korak, pogotovo nakon desetljeća monopola i dominacije od strane velikih centraliziranih kompanija.

Blockchain tehnologija nudi brojne prednosti poput decentralizacije, anonimnosti i sigurnosti. Primjena ove tehnologije je vrlo široka te obuhvaća područja od kripto valuta, financijskih usluga pa sve do IoT i razne socijalne službe. Ovaj rad prikazuje razlog nastanka ove tehnologija, njenu arhitekturu, prednosti i mane te područja primjene.

Sažetak

Svakodnevni život i poslovanje u današnje doba nisu mogući bez interneta, mobitela i osobnog računala. Zbog toga je zaštita i očuvanje digitalne imovine od sve veće važnosti za pravne i fizičke osobe uzevši u obzir učestale rizike vezane uz područje cyber kriminala. Ulaganje u informacijsku sigurnost ne predstavlja trošak već jamči konkurentsku prednost i opstanak organizacije na tržištu.

U diplomskom radu objašnjen je pojam blockchain tehnologije i način na koji ista doprinosi jačanju sigurnosti, informacijske privatnosti i autentičnosti digitalnih podataka u digitalnom poslovanju. Prikazani su načini funkcioniranja blockchain tehnologije u digitalnom poslovanju te su analizirani zakonski propisi koji reguliraju obradu podataka u informacijskim sustavima. Također, prikazana je organizacija i upravljanje informacijskom sigurnosti i aktualni rizici i ugroze. Obrađena je struktura, primjena i budući razvoj blockchain tehnologije.

Na kraju rada provedeno je istraživanje u obliku ankete vezano uz implementaciju informacijske sigurnosti u zaštiti podataka te razine educiranosti korisnika od računalnih ugroza. Obrađeni su rezultati istraživanja i definiran je zaključak diplomskog rada.

Ključne riječi:

blockchain, zaštita podataka, informacijska sigurnost, decentralizacija, kriptovalute

Summary

Everyday life and business nowadays are not possible without the internet, cell phones and personal computers. Therefore, the protection of digital property and personal data is of increasing importance for legal and natural persons, given the growing risks and threats of cybercrime. Investing in information security does not represent a cost burden but guarantees the competitive advantage and survival of the organization in the market.

The thesis explains the concept of Blockchain technology and the way in which it contributes to the preservation of information privacy and authenticity of digital data. Presented are the ways in which Blockchain technology works in digital business with analysis of legal regulations governing the data processing in information systems. The paper also defines the areas of information security and current risks and threats. The structure, application and future development of Blockchain technology are elaborated.

At the end of the paper, a survey was carried out in the form of a poll related to the implementation of information security in data protection and the level of education of users about computer threats. The results of the research are processed and the conclusion of the diploma thesis is defined.

Keywords

Blockchain, dana protection, information security, decentralization, cryptocurrenci

Sadržaj

1. UVOD

Najvažnije sredstvo za razmjenu i prijenos informacija i podataka je jezik koji je primarno sredstvo za komuniciranje, razmjenu informacija, iskustava i znanja. Međutim, jezična komunikacija ograničena je prostorom i vremenom. Za razmjenu informacija između dvije ili više osoba, nužno je da te osobe budu u isto vrijeme na istom mjestu. Ovakav način prenošenja informacija ovisi ponajviše o komunikacijskim vještinama osobe koja informacije daje ali i sposobnosti razumijevanja osobe koja te informacije prima. Pogrešna interpretacija i daljnje prenošenje tih pogrešnih podataka dodatna je opasnost. Društvo je bilo organizirano na način da je samo nekolicina pojedinaca (poglavice, vračevi, svećenici…) posjedovalo znanje i to se znanje prenosilo usmenim putem s koljena na koljeno. Smrću, odbijanjem da se prenese znanje na nekog drugog ili zbog nekog drugog razloga, dolazilo je do trajnog gubitka znanja potrebnih za razvoj društva. Zbog svega navedenog, nužan je bio sljedeći korak u razvoju čovječanstva - stvaranje pisma.

Najraniji oblik pisma je piktografsko (slikovno pismo) koje se sastoji od niza pojednostavljenih sličica koje asociraju na određenu stvar. Kombinacijom tih sličica moguće je prikazati neki događaj ili misao. Najpoznatiji primjer ovog pisma su egipatski hijeroglifi. Daljnjim razvojem pisma omogućeno je trajno pohranjivanje podataka, informacija i znanja. Razvojem pisma, razvija se i pismenost i pisani zapisi postaju dostupni većini. Međutim, time se stvara problem zaštite zapisa koji nisu namijenjeni svima.

Jedan od prvih načina zaštite bilo je je fizičko prikrivanje poruka. Skrivanje poruka u tajne pretince, korištenje posebnih materijala te tome slične tehnike. Nedostatak ovakve zaštite sastoji se u tome što se prilikom pronalaska takve poruke, otkriva cijeli njen sadržaj. Zbog toga je osmišljen novi način zaštite - kriptografija.

„Kriptografija (kripto- + -grafija), prevođenje (kriptiranje ili šifriranje) razgovijetnoga teksta (jasan, otvoreni tekst), ili kakva drugoga skupa podataka, u nerazgovijetan tekst (kriptirani tekst, kriptogram ili šifrat), kako bi ga jedino onaj koji posjeduje unaprijed utvrđen ključ za odgonetanje (dekriptiranje, dešifriranje) mogao prevesti u izvorni, razgovijetni tekst. Zadaća je kriptografije da omogući dvjema osobama (pošiljatelj i primatelj) očuvanje tajnosti poruka, čak i u komunikaciji nesigurnim komunikacijskim kanalom (računalna mreža, telefonska linija), koji je dostupan trećim osobama.“[1]

[1] kriptografija. *Hrvatska enciklopedija, mrežno izdanje,* Leksikografski zavod Miroslav Krleža, 2020., raspoloživo na: http://www.enciklopedija.hr/Natuknica.aspx?ID=33988, datum pristupa: 31. 5. 2020.

Kriptiranje se u počecima svodilo na različite kombinacije dislokacije znakova poruke ili supstitucijom. Jedna od najpoznatijih takvih šifri je Cezarova šifra u kojoj je svako slovo poruke zamijenjeno trećim slovom u abecednom redoslijedu iza njega. Modernija i također poznata verzija ove vrste šifriranja je *„Enigma“* - mehanički stroj koji služi za šifriranje i dešifriranje, a koristila ga je Njemačka u Drugom svjetskom ratu. Metode koje Enigma koristi su aritmetička supstitucija i mapirajuća supstitucija.

Smatra se da suvremena kriptografija počinje 1949. godine djelom C.E.Shannon *Communication Theory of Secrecy Systems* (Komunikacijska teorija tajnih sustava). U suvremeno doba, najveći protok podataka je u digitalnom obliku pa se i suvremena kriptografija oslanja uglavnom na procesorsku snagu računala. Postupci kriptiranja i dekriptiranja temelje se na matematičkim algoritmima i provode se pomoću računala.

Zaštita digitalne imovine i osobnih podataka svakim danom sve više dobiva na važnosti. Svakodnevan život i poslovanje u današnje doba nisu mogući bez interneta, mobitela i osobnog računala. Korištenjem bilo kojeg od tih i sličnih uređaja, ostavljamo digitalni trag, informacije o sebi i svojim navikama koje netko može zlorabiti. Zbog toga je zaštita digitalne imovine i osobnih podataka od sve veće važnosti za pravne i fizičke osobe s obzirom na sve veće rizike i ugroze od računalnog kriminaliteta.

Ulaganje u informacijsku sigurnost ne predstavlja trošak već jamči konkurentsku prednost i opstanak organizacije na tržištu. Krađa identiteta, gubitak i krađa podataka samo su neke od opasnosti koje mogu dovesti do neželjenih posljedica. Za privatne osobe to može biti od gubitka podataka sentimentalne važnosti poput fotografija pa sve do financijskih prevara.

Gubitak i krađa podataka organizaciji mogu nanijeti nesagledivu štetu u financijskom ali i u reputacijskom pogledu. Naime, razvojem novih metoda zaštite digitalnih podataka paralelno se razvijaju i tehnologije za probijanje tih zaštita.

Na koji će se način provoditi zaštita digitalne imovine odlučuje sam korisnik - privatni ili poslovni. Postoji više načina i tehnologija, a jedna od tih tehnologija u zaštiti podataka je i blockchain.

Blockchain je digitalni zapis provedenih transakcija. Naziv dolazi iz strukture ove tehnologije, a sastoji se od blokova informacija (block) koji su povezani u lanac (chain). [2] Od svog osnutka 2008. godine, blockchain je i dalje izvor revolucionarnih mogućnosti i rješenja. Iako je blockchain tehnologija većim dijelom pozornost privukla zbog bitcoina, ista se razvija kao ključna tehnologija i u drugim industrijama.

Iako je prvenstveno razvijena za digitalne valute, blockchain tehnologija razvila se u mnogo više te je probila granice prvotne namjene. Sama ideja i koncept decentraliziranog sustava i uspješne implementacije digitalnog peer-to-peer sustava bio je prijeko potreban korak, pogotovo nakon desetljeća monopola i dominacije od strane velikih centraliziranih kompanija.

Cilj ovog rada je naglasiti važnost zaštite i sigurnosti digitalne imovine, prikazati neke od metoda zaštite, omogućiti uvid sa zakonskog stajališta i upoznati blockchain kao novu tehnologiju zaštite podataka na primjerima kripto valuta te primjenu blockchain tehnologije u području korporativno – informacijske sigurnosti. Blockchain tehnologija nudi brojne prednosti poput decentralizacije, anonimnosti i sigurnosti.

Struktura blockchain tehnologije u zaštiti digitalnih podataka korisniku osigurava povjerljivost, integritet i raspoloživost. Kroz povjerljivost sustav onemogućava neautorizirane osobe da pristupaju podacima, kroz integritet im onemogućava mijenjanje sadržaja podataka, dok se kroz dostupnost korisnicima omogućava siguran i stalan pristup podacima.

Također, važno je naglasiti kako blockchain tehnologija osigurava neporecivost i autentičnost u smislu dokazivanja svake aktivnosti pojedinca u digitalnom poslovanju bilo da se podaci dijele na privatnoj ili javnoj mreži. Primjena blockchain tehnologije je vrlo široka te obuhvaća područja od kripto valuta, financijskih usluga pa sve do IoT i razne socijalne službe. Ovaj rad prikazuje razlog nastanka blockchain tehnologije, njenu arhitekturu, prednosti i mane te područja primjene.

2. PODATAK I INFORMACIJA

[2] *What is Blockchain Technology? A Step-by-Step Guide For Beginners* (2015), raspoloživo na: https://blockgeeks.com/guides/what-is-blockchain-technology/, datum pristupa sadržaju: 02.03.2020.

Podaci su zapisane i memorirane činjenice. Kada se podatak ili grupa podataka pročita i protumači, dobije se informacija, odnosno obavijest. Kada se na informacije primjeni vještina ili iskustvo, stekne se znanje.

Zakon o tajnosti podataka definira podatak kao „*...dokument, odnosno svaki napisani, umnoženi, nacrtani, slikovni, tiskani, snimljeni, fotografirani, magnetni, optički, elektronički ili bilo koji drugi zapis podatka, saznanje, mjera, postupak, predmet, usmeno priopćenje ili informacija, koja s obzirom na svoj sadržaj ima važnost povjerljivosti i cjelovitosti za svoga vlasnika*“.[3]

Nadalje, definiciju informacije možemo pronaći i u stručnoj literaturi - “*Informacija, lat. (informare – dati oblik, oblikovati, predočiti), uputa, obavijest, obavještenje, saopćenje o toku radova ili o nečijoj djelatnosti; podatak o nečem.*”[4]

Noviji pokušaju definiranja pojma informacije navode da je ona “*saznanje dobiveno istraživanjem, učenjem ili instrukcijom.*”[5] No, isto tako, navedeni izvor navodi da je „*podatak činjenica (poput nečeg izmjerenog ili statistike), korišten kao baza za rasuđivanje, diskusiju ili izračun*.“[6]

Za razliku od teoretskih pristupa, zakonodavac u Zakonu o tajnosti podataka (NN br. 79/07, 86/12), u članku 2., st.1., podatak definira kao „*...dokument, odnosno svaki napisani, umnoženi, nacrtani, slikovni, tiskani, snimljeni, fotografirani, magnetni, optički, elektronički ili bilo koji drugi zapis podatka, saznanje, mjera, postupak, predmet, usmeno priopćenje ili informacija, koja s obzirom na svoj sadržaj ima važnost povjerljivosti i cjelovitosti za svoga vlasnika*.“

U članku 2., st. 2., spomenutog zakona, klasificirani podatak definira se kao “*...onaj koji je nadležno tijelo, u propisanom postupku, takvim označilo i za koji je utvrđen stupanj tajnosti,*

---

[3] *Zakon o tajnosti podataka*, I. Osnovne odredbe, članak 2, NN79/07, 86/12, https://www.zakon.hr/z/217/Zakon-o-tajnosti-podataka, datum pristupa 28.05.2020.

[4] Klaić B., *Rječnik stranih riječi*, Nakladni zavod MH Zagreb, 1988. god.

[5] Merriam-Webster dictionary (2020), Dictionary, raspoloživo na: www.merriam-webster.com/dictionary/information, datum pristupa sadržaju: 11.02.2020.

[6] Merriam-Webster dictionary (2020), Dictionary, raspoloživo na: www.merriam-webster.com/dictionary/information, datum pristupa sadržaju: 11.02.2020.

kao i podatak kojeg je Republici Hrvatskoj tako označenog predala druga država, međunarodna organizacija ili institucija s kojom Republika Hrvatska surađuje."

U članku 2., st. 3., istog zakona neklasificirani podatak definira se kao „*...podatak bez utvrđenog stupnja tajnosti, koji se koristi u službene svrhe, kao i podatak koji je Republici Hrvatskoj tako označenog predala druga država, međunarodna organizacija ili institucija s kojom Republika Hrvatska surađuje.*"

U članku 2., st. 4., klasifikacija podataka definira se kao „*...postupak utvrđivanja jednog od stupnjeva tajnosti podatka s obzirom na stupanj ugroze i područje ovim Zakonom zaštićenih vrijednosti.*"

U članku 2., st. 5., istog zakona deklasifikacija podataka uređena je kao „*...postupak kojim se utvrđuje prestanak postojanja razloga zbog kojih je određeni podatak klasificiran odgovarajućim stupnjem tajnosti, nakon čega podatak postaje neklasificirani s ograničenom uporabom samo u službene svrhe.*"

U članku 4., st. 1., već spomenutog zakona navodi se da stupnjevi klasifikacije podataka mogu biti vrlo tajno, tajno, povjerljivo, ograničeno.

Postoje više kriterija prema kojima se informacija može podijeliti. Tako Javorović, Bilandžić[7], definiraju vrste informacija prema različitim kriterijima:

- prema nastanku (izvorne, izvedene)
- prema učinku (korisne, nekorisne)
- prema izvoru (unutarnje, vanjske)
- prema podrijetlu (vlastite, tuđe)
- prema pojavnom obliku (glasovne, pisane, zvučne, slikovne, zvukovne, znakovne)
- prema vjerodostojnosti (istinite, neistinite)
- prema otvorenosti (javne, tajne)
- prema sadržaju (osobne, opće, poslovne/funkcionalne)
- prema području djelovanja
- prema dospijeću (pravovremene, zastarjele).

[7] Javorović B., Bilandžić M. (2007), *Poslovne informacije i business intelligence*, Zagreb: Golden marketing – Tehnička knjiga, str. 32-33

Podaci i informacije važan su resurs u svakodnevnom poslovanju organizacije. Važno je da je informacija kvalitetna, odnosno da je točna i ispravna. Vrijednost informacije teško je procijeniti budući da ona ovisi o korisniku koji ju koristi i svrsi za koju se koristi.

Nemoguće je zamisliti poslovanje bez podataka. Financijski izvještaji, popis zaposlenika, stanje robe na skladištu i evidencija radnog vremena samo su neki od podataka koji se koriste u svakodnevnom poslovanju. Osim podataka koji su nužni za poslovanje, neki podaci moraju se evidentirati i čuvati kao rezultat zakonom predviđene obveze.

U Zakonu o arhivskom gradivu i arhivima (NN br. 61/18, 98/19) navedeno je da se „*ovim Zakonom uređuju zaštita i obrada javnog dokumentiranog i arhivskog gradiva, dostupnost i korištenje gradiva u arhivima, zaštita privatnog arhivskog gradiva, javna arhivska služba te nadležnosti i djelatnost arhiva.*“ [8]U Zakonu se ističe da je arhivsko gradivo od interesa i pod zaštitom Republike Hrvatske.

Čuvanje i zapisivanje podataka nekada je bilo ograničeno na fizički zapis na papiru, kamenu, glinenim pločama i sl. U današnje vrijeme većina podataka čuva se u digitalnom obliku, što olakšava i ubrzava obradu i korištenje. Podaci se koriste za izgradnju podatkovnog i informacijskog sustava koji podupire poslovanje.

Zbog važnosti u poslovanju, informacije i podaci su važan resurs te se u modernom poslovanju nazivaju - digitalna ili informacijska imovina.

Podatak se može prenositi i zapisivati na razne načine. Podatak je niz prepoznatljivih simbola, odnosno znakova, koji su zapisani na nekom mediju. Znakovi mogu biti različiti a zajednička im je karakteristika da imaju određeno značenje. Znakovi abecede (A,a,B,b,D,f,M,N) služe nam za zapisivanje govora. Znakovi kao +, -, / koriste se u matematici i govore nam koje matematičke funkcije primijeniti. [9]

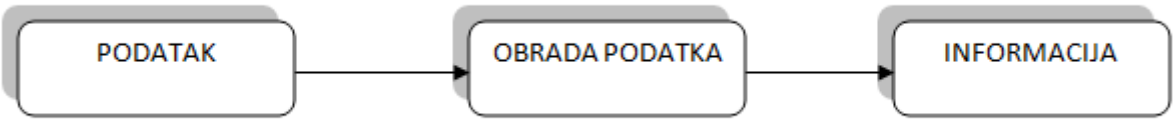
Računala obrađuju i zapisuju podatke na drugačiji način nego što ih mi doživljavamo. Računalu treba zapis koji je moguće obrađivati i prenositi primjerice s USB memorije na memoriju računala, iz memorije računala u procesor, iz procesora na memoriju i iz memorije

[8] *Zakon o arhivskom gradivu i arhivima*, I. Opće odredbe, članak 1., NN 61/18, 98/19, https://www.zakon.hr/z/373/Zakon-o-arhivskom-gradivu-i-arhivima, datum pristupa 04.04.2020.

[9] Varga M. (2014), *Upravljanje podacima*, Zagreb: Element d.o.o., str. 2

na ekran. Svaki podatak i informacija mogu se "razbiti" na manje dijelove koje nazivamo "bit". Bit je kratica od "*Binary DigIT*" (dolazi od engleske riječi „*Binary digit*" a znači binarna znamenka, jer se koriste „0" i „1" - znamenke binarnog sustava), a označava najmanju jedinicu podatka ili informacije. Bit može imati vrijednost „1" ili „0". Ove vrijednosti mogu se tumačiti kao "da" ili "ne", "točno" ili "netočno", "pozitivno" ili "negativno". Svaki se podatak može kodirati, odnosno "pretvoriti" u niz jedinica i nula. Takav oblik podataka računalo razumije i može obrađivati.[10]

Informacija i obavijest nastaju interpretacijom i obradom podataka, odnosno stavljanjem u neki kontekst značenja. Protumačeni podatak daje informaciju.



Slika 1 - Proces nastanka informacije

Izvor : izradio autor

Informacije je činjenica određenog značenja. Informacija mora biti točna, potpuna i provjerena.

Slijedom navedenog, moguće je izdvojiti određene karakteristike kvalitetne informacije.

- **Točnost informacije**

Informacija je točna ako objektivno opisuje pravo stanje stvari. Kako bi bio učinkovit i poslovno funkcionalan, informacijski sustav nužno mora biti ispunjen točnim informacijama. Zbog toga je važno provjeriti izvor informacija prije nego uđu u informacijski sustav. Netočne informacije mogu naštetiti cijelom poslovnom sustavu i sveukupnom poslovanju.

- **Potpunost informacije**

[10] Gregurić V., Hajdinjak N., Jakšić M., Počuča B., Rakić D., Svetličić S., Šokac D., Vlajinić D. (2019), *Informatika 5 – udžbenik u petom razredu osnovne škole*, Zagreb: Profil Klett d.o.o., modul: Informacije i digitalna tehnologija, jedinica: Kako radi računalo, odlomak: Binarni sustav

Informacija je potpuna ako opisuje pravo stanje stvari, bez potrebe za dodatnim opisom ili pojašnjenjem. Informacija ne smije izostaviti ili skrivati bilo kakve činjenice, povoljne ili nepovoljne. Potpunost informacije utvrđuje se provjerom činjenica iz više relevantnih izvora.

KARAKTERISTIKE KVALITETNE INFORMACIJE	INFORMACIJA MORA BITI:
- dostupnost	- dostupna
- dostatna	- količinski odgovarajuća
- uvjerljivost	- istinita i kredibilna
- potpunost	- potpuna
- jezgrovitost	- jezgrovita, kompaktna, koncizna
- konzistentnost	- konzistentno prezentirana
- jednostavnost	- jednostavna za korištenje
- točnost	- točna i pouzdana
- interpretabilnost	- odgovarajuće prikazana
- objektivnost	- nepristrana i objektivna
- relevantnost	- relevantna, primjerena, odgovarajuća
- reputacija	- iz provjerenih izvora
- sigurnost	- zaštićena od neovlaštenih pristupa
- pravovremenost	- pravovremena i ažurna
- razumljivost	- razumljiva
- dodana vrijednost	- korisna, daje na vrijednosti

Tablica 1 – Karakteristika kvalitetne informacije

Kreirana na temelju izvora: Kahn, Strong, Wang: „Information Quality Benchmarks: Product and Service Performance. Comm. of ACM“, vol 45, no 4, 2002.

Pipino, Lee, Wang: „Data Quality Assessment . Comm. of ACM“, vol 45, no 4, 2002. - “Gartner: Drive Data Quality Improvements From a Foundation of Metrics“, 2007.

- **Primjerenost informacije**

Informacija je primjerena ako odgovara zahtjevima osobe koja je informaciju tražila. Primjerice, ako korisnik traži informaciju o cijeni nekog proizvoda, a dobije informaciju o količini tog proizvoda na skladištu, informacija nije primjerena i samim time je u tom trenutku beskorisna za korisnika.

- **Pravovremenost informacije**

Informacija je pravovremena ako se dobije na vrijeme. Ako koristimo prije navedeni primjer, korisnik informaciju o cijeni proizvoda mora dobiti što je prije moguće. Ako informacija kasni, moguće je da je u međuvremenu došlo do promjene cijene i da dobivena informacija više nije točna.

3. ORGANIZACIJA I UPRAVLJANJE INFORMACIJSKOM SIGURNOSTI

Proboji u informacijske sustave i podatkovne mreže danas su jedan od najefikasnijih načina neovlaštenog prikupljanja podataka koji napadačima osigurava smanjeni rizik budući da se obavlja uglavnom s velike udaljenosti, prikriven brojnim slojevima zaštite prave lokacije, identiteta i ciljeva.

Cyber napade karakterizira skup hakerskih procesa, koji nužno trebaju određenu razinu prikrivenosti na duže vrijeme uz korištenje naprednih napadačkih alata koje se teško mogu identificirati tradicionalnim antivirusnim softverima.

Brzi razvoj tehnologija i njihove primjene u digitalnom poslovanju uvjetuje kako svaka organizacija ukoliko želi opstati na tržištu mora imati suvremen i razvijen informacijski sustav.

Informacijska sigurnost u digitalnom poslovanju još uvijek nije dovoljno ozbiljno shvaćena. Niska razina znanja zaposlenika iz područja informacijske sigurnosti predstavlja ozbiljan rizik po informacijsku imovinu organizacije. Zbog toga je važno u planiranju i razvoju sustava upravljanja informacijskom sigurnosti voditi brigu o educiranosti zaposlenika te odgovornostima i dužnostima svakog pojedinca u organizaciji.

Također, značajan rizik informacijske sigurnosti je i neorganizirano implementiranje sigurnosnih kontrola zbog čega je svaku sigurnosnu kontrolu ugrađenu u sustav nužno dokumentirati, a sigurnost informacijskih sustava graditi prema unaprijed definiranim pravilima koji se vežu uz dokument Sigurnosna politika organizacije.

Uloga sigurnosne politike u području informacijske sigurnosti je određivanje prihvatljivog i neprihvatljivog načina ponašanja kako bi zaštitili informacijsku imovinu; opremu (eng. hardware), programsku podršku (eng. *software*) i podatke.

Na temelju pravila definiranih u dokumentu Sigurnosna politika organizacije osiguravaju se tri temeljna svojstva informacije:

- povjerljivost (tajnost),
- integritet,
- dostupnost.[11]

Stalno ulaganje u informacijski sustav i zaštitu informacijskog kapitala obveza je za svaku organizaciju te se traži sustavan pristup u području upravljanja informacijskom sigurnošću. Za poslovanje organizacije od velike je važnosti da informacijski sustav osigura povjerljivost, cjelovitost i dostupnost podataka. Prijetnja od digitalnog kriminala raste sve više i sve brže. Iako se organizacije odlučuju zaštititi svoju digitalnu imovinu raznim dostupnim alatima (softverskim i hardverskim), mnoge organizacije još nisu dovoljno svjesne ozbiljnosti od krađe i gubitka podataka zbog nedovoljnog ulaganja u sustav upravljanja informacijskom sigurnošću. Prema istraživanjima koje je proveo "McAfee", jedan od većih pružatelja softverske zaštite, štete prouzročene cyber kriminalom premašuju 400 milijardi USD i svake godine taj iznos raste.

Nekoliko je glavnih razloga zašto je potrebno ulagati u zaštitu digitalne imovine.

- **Rast troškova sigurnosnih proboja**

Činjenica je da cyber napadi mogu nanijeti veliku štetu svakoj organizaciji. Troškovi oporavka informacijskih proboja te vraćanja i spašavanja podataka mogu biti vrlo visoki. Šteta nanesena reputaciji također može biti vrlo visoka. Neuspješna obrana od cyber napada, gubitak ili krađa podataka mogu uzrokovati gubitak povjerenja postojećih i budućih poslovnih suradnika, što dovodi do gubitka klijenata, a samim time i pada profita.

- **Sofisticirani i usklađeni hakerski napadi**

Sve su češći sofisticirani i usklađeni hakerski napadi koje je sve teže zaustaviti. Takvi su napadi ciljani, a mete su najčešće visoko profitne organizacije. Cilj napada je krađa vrijednih

[11] *Sigurnosna politika* (2009), CARNet – Hrvatska akademska istraživačka mreža, CCERT-PUBDOC-2009-05-265

podataka koji se prodaju trećoj strani (konkurenciji i sl.) ili se vraćaju oštećenim organizacijama za određeni financijski iznos.

- **Lako dostupni alati za hakiranje**

Najveća opasnost krije se u visoko kvalificiranim i stručnim hakerima. Međutim, sve veća digitalizacija poslovanja i nužnost pristupa internetu za svaku organizaciju, dovela je do komercijalizacije cyber kriminala. Osobe koje nisu dovoljno stručne u hakiranju ili uopće ne znaju hakirati, mogu vrlo jednostavno unajmiti hakera koji će izvršiti napad na željeni cilj. Vrlo je lako na internetu pronaći i preuzeti razne programske alate koji pokreću napad jedim klikom miša.

- **Širenje IoT uređaja**

IoT ili "*Internet of Things*" čine različiti pametni uređaji povezani na internet. Takvi su uređaji sve češći u poslovnim uredima, kućama, stanovima pa i u automobilima. Služe pojednostavljanju i ubrzanju provođenja određenih zadataka. Međutim, iako olakšavaju svakodnevan život predstavljaju i sigurnosnu prijetnju. Korištenjem IoT uređaja povećava se rizik od hakerskih napada, gubitka i krađe podataka ili povrede privatnosti. IT tvrtka "Cisco" predviđa da će do 2021. godine čak 27,1 milijardi uređaja biti povezano na internet. Zbog raznih sigurnosnih nedostataka, sve je veća potreba za provođenjem procjena ranjivosti i rješavanju rizika koji ti uređaji predstavljaju.

- **Stroži propisi**

Cyber kriminal nije jedini uzrok potrebe za jačanjem sustava informacijske sigurnosti. Uvođenje propisa kao što je Opća uredba o zaštiti podataka (GDPR), obvezuje sve organizacije na provođenje odgovarajućih organizacijskih i tehničkih mjera u cilju zaštite privatnosti na internetu i zaštite osobnih podataka građana Europske unije (dalje u tekstu: EU).

3.1. Informacijska sigurnost

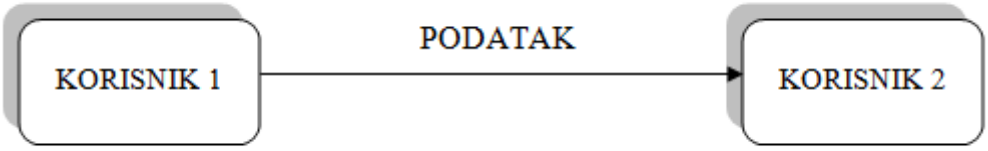
Sukladno Zakonu o informacijskoj sigurnosti (NN br. 79/07), u članku 2., st. 1., informacijska sigurnost definira se kao *"...stanje povjerljivosti, cjelovitosti i raspoloživosti podatka, koje se postiže primjenom propisanih mjera i standarda informacijske sigurnosti te organizacijskom potporom za poslove planiranja, provedbe, provjere i dorade mjera i standarda."*

Članak 37. Ustava Republike Hrvatske (NN br. 56/90, 135/97, 08/98, 113/00, 124/00, 28/01, 41/01, 55/01, 76/10, 85/10, 05/14) navodi da je „*zaštita osobnih podataka u RH ustavna kategorija te je osigurana svakoj fizičkoj osobi u RH bez obzira na državljanstvo i prebivalište, neovisno o rasi, boji kože, spolu, jeziku, vjeri, političkom ili drugom uvjerenju, nacionalnom ili socijalnom podrijetlu, imovini, rođenju, naobrazbi, društvenom položaju ili osobinama. Svakom se jamči sigurnost i tajnost osobnih podataka. Bez privole ispitanika, osobni se podaci mogu prikupljati, obrađivati i koristiti samo uz uvjete određene zakonom*."

Zaštita digitalnih sustava podrazumijeva poduzimanje određenih mjera i akcija, sve u svrhu zaštite digitalne imovine od nepredviđenih događaja i neželjenih posljedica. Složeni procesi koji se odvijaju unutar računalnih sustava moraju se zaštititi od brojnih prijetnji. Prijetnje mogu posredno ili neposredno, kontinuirano ili povremeno narušavati rad sustava i time se ugrožava sigurnost podataka i poslovnih procesa. Zbog toga je potrebno da se onemogući bilo kakvo slučajno i/ili namjerno narušavanje rada sustava, odnosno krađa, uništenja, oštećenje, izmjena ili neovlašteno korištenje digitalne imovine. Potrebno je poduzeti sve da se stvore uvjeti za neometan rad svih funkcija sustava, kako bi se podaci i informacije obrađivali i koristili na planiran i unaprijed određen način.

Za postavljanje uspješne zaštite potrebno je utvrditi:

- tko ili što se štiti – definiranje objekta zaštite (podaci, dokumenti, software, komunikacijska oprema...)
- od koga ili čega je potrebna zaštita – definiranje mogućih prijetnji i opasnosti (neovlašteni pristup, hakerski napadi, krađa, kvarovi, elementarne nepogode...)
- zašto štititi – analizirati moguće posljedice neprovođenja zaštite (gubitak ili krađa podataka, prekid rada sustava, financijski gubici...)
- na koji način štititi – odabir mjera i vrste zaštite (potrebna analiza i procjena rizika za utvrđivanje najefikasnije mjere zaštite).



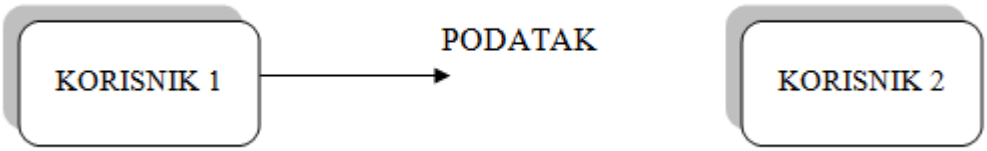
Slika 2 – Neometan protok podataka

Izvor : Izradio autor

Prijetnje koje ugrožavaju i utječu na sigurnost digitalnih podataka u informacijskim mrežama i sustavima, mogu se podijeliti u nekoliko glavnih kategorija.

- **Prekid protoka podataka**

Radi se o aktivnom napadu. Prekida se normalan tok podataka i na taj se način onemogućava normalan rad nekog sustava ili pružanje neke usluge. Ovakav napad direktno utječe na raspoloživost podataka.

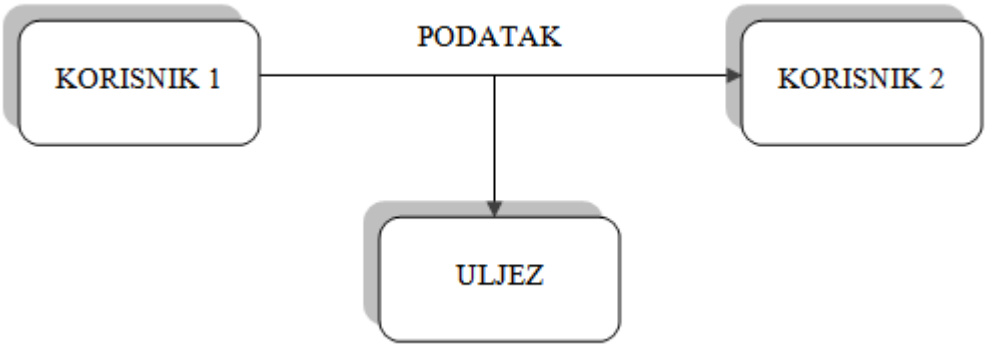


Slika 3 – Prekid protoka podataka

Izvor : Izradio autor

- **Presretanje podataka**

Presretanje je pasivan napad i teško se otkriva. Najčešće se radi o prisluškivanju, nadziranju rada sustava, praćenje protoka podataka i neovlaštenom pristupu informacijama, odnosno predstavlja napad na povjerljivost. Ovakav napad ne utječe na podatke i rad sustava, ali je najčešće priprema na neki drugi oblik napada.



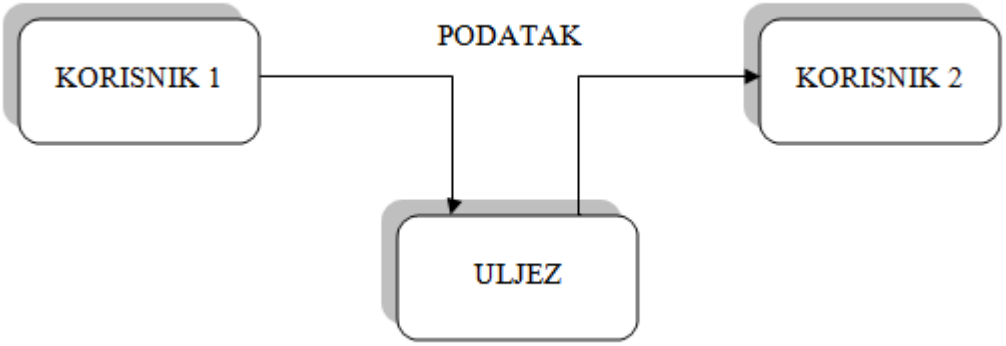
Slika 4 – Presretanje podataka

Izvor : Izradio autor

- **Modificiranje podataka**

Ovdje se radi o aktivnom napadu koji utječe na integritet sustava. Prekida se normalan protok podataka, ti se podaci mijenjaju i krivotvore, i kao takvi plasiranju dalje u sustav. Iako se radi

o izmjeni postojećih podataka, moguće je da takav napad ostane neprimijećen duže ili kraće vrijeme. Zbog toga je važno vršiti kontrolu podataka unutar sustava, s ciljem bržeg otkrivanja ovakvih napada.

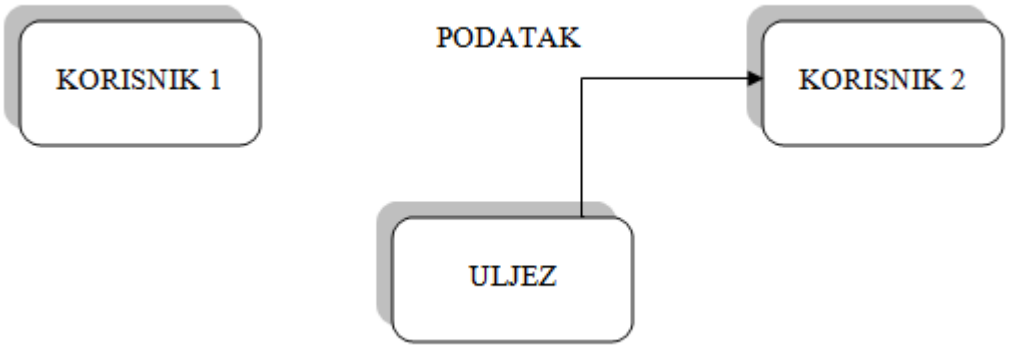


Slika 5 – Modificiranje podataka

Izvor : Izradio autor

- **Krivotvorenje podataka**

Ova vrsta aktivnog napada direktno utječe na autentičnost. Napadač stvara i plasira potpuno nove i neželjene podatke u sustav, generira lažni promet ili izdaje neovlaštene naredbe.



Slika 6 – Krivotvorenje podataka

Izvor : Izradio autor

Svaki napad nanosi štetu - materijalnu, nematerijalnu ili reputacijsku. Krađa podataka, neovlaštena uporaba tih podataka, manipuliranje i krivotvorenje podataka koji se plasiranju u sustav - svi ovi napadi mogu imati negativne posljedice po organizaciju. Zbog toga je iznimno bitno pravovremeno zaštititi informacijske sustave.

3.2. Područja informacijske sigurnosti

Za pravilno određivanje potrebnih razina zaštite, a u cilju zaštite informacijske imovine potrebno je od strane organizacije definirati područja informacijske sigurnosti.

Područja informacijske sigurnosti predstavljaju podjelu informacijske sigurnosti na pet područja, s ciljem sustavne i učinkovite realizacije donošenja, primjene i nadzora mjera i standarda informacijske sigurnosti.

Područja informacijske sigurnosti za koja se propisuju mjere i standardi informacijske sigurnosti su:

- sigurnosna provjera,
- fizička sigurnost,
- sigurnost podatka,
- sigurnost informacijskog sustava te
- sigurnost poslovne suradnje.

Mjere informacijske sigurnosti su opća pravila zaštite podataka koja se realiziraju na fizičkoj, tehničkoj ili organizacijskoj razini. Način na koji državni sektor uređuje područje informacijske sigurnosti opisan je u članku 10. Uredbe o mjerama informacijske sigurnosti (NN br. 46/2008).

Mjere informacijske sigurnosti za područje sigurnosna provjera su:

- popis dužnosti i poslova za koje je potrebno uvjerenje o sigurnosnoj provjeri (certifikat)
- postupak za izdavanje certifikata
- upitnik za sigurnosnu provjeru
- pisana suglasnost osobe za koju se provodi sigurnosna provjera
- izdavanje certifikata
- sigurnosno informiranje
- nacionalni registar izdanih certifikata, rješenja o odbijanju izdavanja certifikata i potpisanih izjava o postupanju s klasificiranim podacima

- registar zaprimljenih certifikata i potpisanih izjava o postupanju s klasificiranim podacima.[12]

Mjere iz ovog područja provode se za osobe koje imaju pristup klasificiranim podacima stupnja tajnosti: vrlo tajno, tajno, povjerljivo.

Mjere informacijske sigurnosti za područje fizička sigurnost su:

- višestruke zone
- sigurnosne zone
- administrativne zone
- plan fizičke sigurnosti
- procjena učinkovitosti mjera fizičke sigurnosti
- kontrola osoba
- pohrana klasificiranih i neklasificiranih podataka
- tehnički sigurni prostori
- fizička sigurnost informacijskih sustava
- oprema za fizičku zaštitu klasificiranih podataka.[13]

Mjere iz ovog područja provode se radi neovlaštenog pristupa, odvraćanja i otkrivanja zlouporaba, otkrivanja i odgovora na sve sigurnosne ugroze.

Mjere informacijske sigurnosti za područje sigurnosti podataka su:

- klasificiranje i deklasificiranje podataka,
- označavanje podataka;
- pristup podacima;
- zaštita podataka;
- sustav registara;
- evidencija korištenja klasificiranih podataka;
- postupanje u izvanrednim situacijama;

[12] *Uredba o mjerama informacijske sigurnosti*, II. Mjere informacijske sigurnosti za područje sigurnosne provjere, članak 11, https://narodne-novine.nn.hr/clanci/sluzbeni/2008_04_46_1547.html, NN 46/08, datum pristupa: 13.04.2020.

[13] *Uredba o mjerama informacijske sigurnosti*, III. Mjere informacijske sigurnosti za područje fizičke sigurnosti, članak 15, https://narodne-novine.nn.hr/clanci/sluzbeni/2008_04_46_1547.html, NN 46/08, datum pristupa: 13.04.2020.

- ustupanje klasificiranih podataka drugoj državi ili međunarodnoj organizaciji.[14]

Mjere iz ovog područja provode se radi klasificiranja i deklasificiranja podataka, reguliranja pristupa, korištenja, pohrane, postupanja u izvanrednim situacijama i razmjene podataka s međunarodnim organizacijama.

Mjere informacijske sigurnosti za područje sigurnosti informacijskog sustava su:

- mjere zaštite informacijskog sustava
- upravljanje sviješću o sigurnosti te
- planiranje djelovanja u izvanrednim okolnostima.[15]

Mjere iz ovog područja provode se radi zaštite hardvera, softvera, medija za pohranu podataka, upravljanja konfiguracijom i sustavom korisničkog pristupa, kontrole povezivanja i uporabe informacijskih sustava, zaštitom od rizika elektromagnetskog zračenja i primjene kriptografske zaštite.

Mjere informacijske sigurnosti za područje sigurnost poslovne suradnje su:

- sklapanje klasificiranih ugovora
- certifikat poslovne sigurnosti
- sigurnosni uvjeti za sklapanje klasificiranih ugovora
- prijevoz klasificiranog materijala
- pristup klasificiranim podacima prilikom međunarodnih posjeta
- razmjena osoba u sklopu projekata ili programa.[16]

Mjere iz ovog područja poduzimaju se u cilju definiranja uvjeta za sudjelovanje na klasificiranim natječajima za pravne i fizičke osobe koje će u okviru klasificiranih ugovora pristupati u objekte i prostore u kojima se obrađuju klasificirani podaci.

---

[14] *Uredba o mjerama informacijske sigurnosti*, IV. Mjere informacijske sigurnosti za područje sigurnosti podataka, članak 32, https://narodne-novine.nn.hr/clanci/sluzbeni/2008_04_46_1547.html, NN 46/08, datum pristupa: 13.04.2020.

[15] *Uredba o mjerama informacijske sigurnosti*, V. Mjere informacijske sigurnosti za područje sigurnosti informacijskog sustava, članak 45, https://narodne-novine.nn.hr/clanci/sluzbeni/2008_04_46_1547.html, NN 46/08, datum pristupa: 13.04.2020.

[16] *Uredba o mjerama informacijske sigurnosti*, VI. Mjere informacijske sigurnosti za područje sigurnosti poslovne suradnje, članak 67, https://narodne-novine.nn.hr/clanci/sluzbeni/2008_04_46_1547.html, NN 46/08, datum pristupa: 13.04.2020.

3.3.Mjere i standardi informacijske sigurnosti

Mjere informacijske sigurnosti su opća pravila zaštite podataka koja se realiziraju na fizičkoj, tehničkoj ili organizacijskoj razini.“[17]

Uredba o mjerama informacijske sigurnosti navodi „*mjere informacijske sigurnosti za područje sigurnosti podataka su:*

- *klasificiranje i deklasificiranje podataka;*
- *označavanje podataka;*
- *pristup podacima;*
- *zaštita podataka;*
- *sustav registara;*
- *evidencija korištenja klasificiranih podataka;*
- *postupanje u izvanrednim situacijama;*
- *ustupanje klasificiranih podataka drugoj državi ili međunarodnoj organizaciji*.“[18]

Postoje različite mjere zaštite, a mogu se razvrstati u nekoliko kategorija.

- **Normativne mjere**

Normativne mjere su tzv. ne tehničke mjere, a odnose se na pravne, organizacijske i kadrovske mjere. Cilj ovih mjera je povećanje produktivnosti cjelokupnog sustava, uz istovremeno značajno poboljšanje efikasnosti sistema zaštite. Neke od tih mjera mogu biti reguliranje prava pristupa i korištenja podataka, postavljanje programskih ograničenja, edukacija kadra o informacijskoj zaštiti, usklađivanje s pravnim normama, izrada pravilnika i procedura za zaštitu i postupanje s podacima unutar poduzeća, uvođenje novih zaštitnih mjera i sl.

[17] *Zakon o informacijskoj sigurnosti*, I. Osnovne odredbe, članak 1., NN 79/07, https://www.zakon.hr/z/218/Zakon-o-informacijskoj-sigurnosti, datum pristupa 28.05.2020.

[18] *Uredba o mjerama informacijske sigurnosti*, IV. Mjere informacijske sigurnosti za područje sigurnosti podataka, članak 32., NN 46/2008., https://narodne-novine.nn.hr/clanci/sluzbeni/2008_04_46_1547.html, datum pristupa 28.05.2020.

- **Fizičko-tehničke mjere**

Ova vrsta mjere oslanja se na spremnost organizacije na financijske investicije. Važno je dobro procijeniti mogućnosti i potrebe organizacije i tome prilagoditi fizičko-tehničke mjere. Kako bi se maksimalno iskoristile, ove mjere moraju biti usklađene i provođene s normativnim mjerama.

- **Kriptografske mjere**

Kriptografska zaštita sve je važnija i popularnija mjera zaštite podataka. Omogućuje visok nivo zaštite uz umjerena financijska ulaganja. Osim softverskih rješenja (blockchain, privatni i javni ključevi...), na tržištu se pojavljuju i hardverska rješenja (kriptirani USB stikovi, mobiteli i tableti...). Uz ovu vrstu mjera važno je istovremeno provođenje normativnih mjera.

Ured vijeća za nacionalnu sigurnost RH navodi *„najpoznatije međunarodne norme koje se bave informacijskom sigurnošću su ISO 27001 i ISO 27002, odnosno paleta normi ISO 27000. Te se norme stalno mijenjaju i dorađuju kako bi bile dio sustava u kojem su usklađene s drugim normama (primjerice s normom ISO 9001, koja se bavi upravljanjem kvalitetom poslovanja) i međusobno. Norma ISO 27001 bavi se uspostavom sustava upravljanja informacijskom sigurnošću, koji se označava kraticom ISMS (engl. Information Security Management System). U toj normi su određeni ciljevi koje organizacija treba postići kako bi imala učinkovit sustav zaštite svojih podataka. ISO 27002 se bavi načinima, postupcima i najboljim praksama pomoću kojih se ti ciljevi mogu postići. U tom smislu je i tvrtka certificirana za HRN ISO/IEC 27001 usklađena i s hrvatskim propisima informacijske sigurnosti koji vrijede isključivo za – NEKLASIFICIRANE podatke (NN 46/08, Uredba o mjerama informacijske sigurnosti, članak 8.).*

Vezano za klasificirane podatke, isti izvor u nastavku navodi: *„za zaštitu KLASIFICIRANIH podataka razine OGRANIČENO primjenjuju se, uz spomenutu normu ISO 27001 dodatno i druge mjere. Za zaštitu KLASIFICIRANIH podataka POVJERLJIVO i više, primjenjuju se zakonski i podzakonski akti informacijske sigurnosti, a posjedovanje certifikata ISO 27001 nije niti dovoljno niti nužno. Naravno, uspješna provedba norme kao što je ISO 27001, može olakšati provedbu propisanih mjera i standarda*

informacijske sigurnosti jer su neki sigurnosni zahtjevi slični te sama realizacija može biti lakše usklađena.“[19]

3.4. Norma ISO 27001

Razvoj i širenje informacijske tehnologije u sva područja poslovanja, dovelo je do sve veće potrebe za zaštitom digitalne imovine. Razvojem tehnologije, razvijali su se i standardi i norme za učinkovitije upravljanje informacijskom sigurnošću. Jedna od prvih prihvaćenih normi je BS7799 norma, koju je razvijena 1995. godine u Velikoj Britaniji od strane British Standards Institution (BSI). Standard je zamišljen da omogući efektivno upravljanje sigurnošću informacijskih sustava. Uvođenjem novih tehnologija, novih zakona i propisa, iz BS779 norme razvijen je međunarodni standard ISO 27001.

ISO 27001 je međunarodno priznata norma čiji je temeljni cilj osigurati i zaštiti informacijski sustav neke organizacije. Ova norma je primjenjiva na sve djelatnosti, a ne samo na IT sektor. ISO 27001 nije tehnička norma, nego norma upravljanja koja sadrži smjernice i specifikacije za razvoj sustava upravljanja informacijskom sigurnošću - ISMS (*Information Security Management System*). ISMS sistemski pristupa sigurnosti informacija i uključuje sve procese, zaposlenike i IT sustav, a može se prikazati preko PDCA modela (*Plan-Do-Check-Act*).

[19] Ured Vijeća za nacionalnu sigurnost RH, (2014), *Ako je informacijski sustav usklađen s HRN ISO/IEC 27001/27002 je li usklađen i s hrvatskim Propisima informacijske sigurnosti o informacijskim sustavima?*, https://www.uvns.hr/hr/ako-je-informacijski-sustav-uskladjen-s-hrn-iso-iec-27001-27002-je-li-uskladjen-i-s-hrvatskim-propisima-informacijske-sigurnosti-o-informacijskim-sustavima, datum pristupa sadržaju: 01.02.2020

Slika 7 - PDCA ciklus

Izvor: *Norme informacijske sigurnosti ISO/IEC 27K*, Javor Bogadi, univ.spec.oec, Ministarstvo obrane Republike Hrvatske, Odsjek za poslove obrane Virovitica

Slika 7. prikazuje PDCA ciklus i faze od kojih se sastoji:

- PLAN – uspostavlja se ISMS,
- DO – implementacija i upravljanje ISMS-om,
- CHECK – praćenje i provjera ISMS-a,
- ACT – održavanje i poboljšavanje ISMS-a.

Vidljivo je da se PDCA ciklus stalno ponavlja i ne prekida, čime se osigurava ažurnost kontinuirana kontrola upravljanja informacijskom sigurnošću.

Uvođenjem norme ISO 27001 u organizaciju prvenstveno se dobiva osiguranje bolje zaštite digitalnog sustava i podataka. Norma pokriva 11 područja - potrebno je postići 39 kontrolnih ciljeva i sadrži 133 kontrole, a sve u svrhu identifikacije, upravljanja i smanjenja prijetnji informacijske sigurnosti.[20] Također se rad i sve aktivnosti unutar organizacije usklađuju sa

[20] Bogati, J., *Norme informacijske sigurnosti ISO/IEC 27K*, Ministarstvo obrane RH, Odsjek za poslove obrane Virovitica, Praktični menadžment, Vol.II, br.3, str. 112-117

važećim zakonskim aktima. Povećava se efikasnost i pouzdanost sustava u slučaju katastrofe. Vrši se i obuka zaposlenika čime se dodatno povećava osviještenost i naglašava važnost održavanja informacijske sigurnosti na svim razinama. Potrebno je naglasiti da ISO 27001 ne uklanja sve sigurnosne rizike, već ih minimizira unutar prihvatljivih okvira. Uvođenje ISO 27001 standarda u neku organizaciju je dobrovoljno i nije obveza. Međutim, dobivanje certifikata dokaz je da organizacija ozbiljno pristupa zaštiti digitalne imovine kojom upravlja i samim time je privlačnija budućim poslovnim partnerima. Certifikat izdaju ovlaštene institucije.

4. ZAKONSKI PROPISI U PODRUČJU ZAŠTITE PODATAKA

U Republici Hrvatskoj informacijsku sigurnost regulira Zakon o informacijskoj sigurnosti (NN79/07), a primjenjuje se na:

- državna tijela
- tijela jedinica lokalne i regionalne samouprave
- pravne osobe s javnim ovlastima, koje koriste klasificirane i neklasificirane podatke
- fizičke i pravne osobe koje pristupaju ili imaju mogućnost pristupa klasificiranim i neklasificiranim podacima.[21]

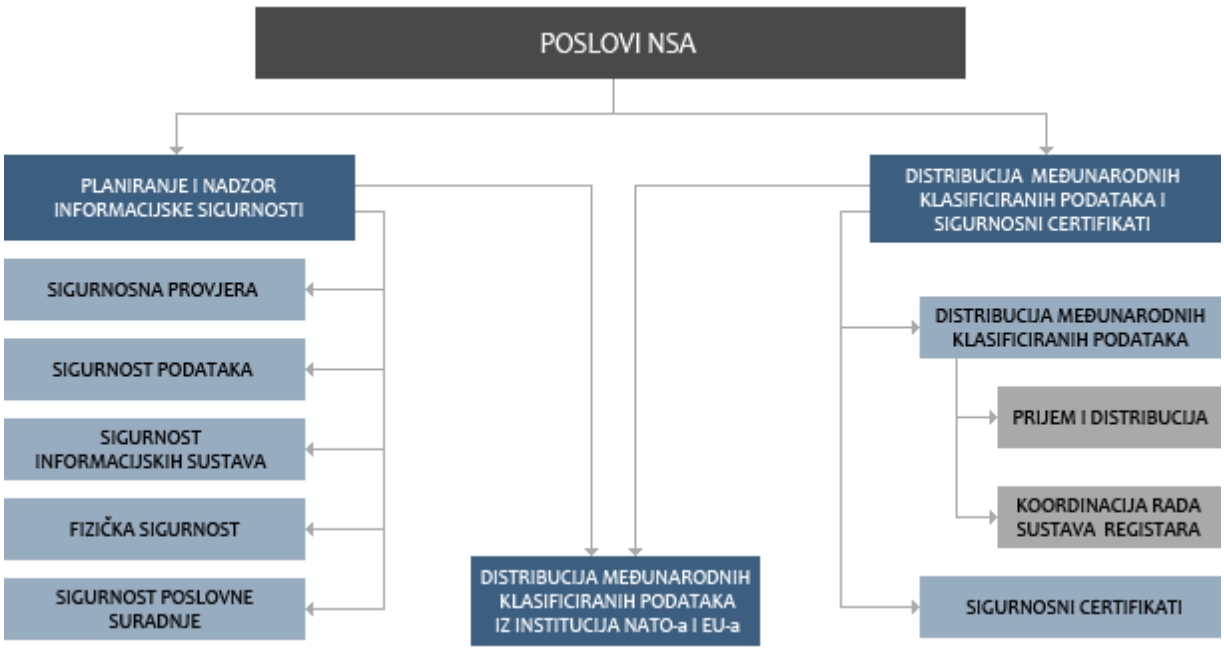
Ured Vijeća za nacionalnu sigurnost *„središnje je državno tijelo za informacijsku sigurnost – hrvatski NSA (National Security Authority). U tom smislu, Ured koordinira i usklađuje donošenje i nadzire primjenu mjera i standarda informacijske sigurnosti u okviru područja sigurnosne provjere, fizičke sigurnosti, sigurnosti podataka, sigurnosti informacijskih sustava i sigurnosti poslovne suradnje (hrvatski DSA) te izdaje certifikate za fizičke i pravne osobe za pristup nacionalnim, NATO i EU klasificiranim podacima.“*[22]

Unutar Ureda nalazi se Središnji registar koji je *„nadležan za prijem i distribuciju međunarodnih klasificiranih podataka te za koordinaciju rada Sustava registara u državnim tijelima u RH koja primaju međunarodne klasificirane podatke. Kao NSA tijelo Ured ostvaruje i koordinira međunarodnu suradnju u području informacijske sigurnosti te*

[21] *Zakon o informacijskoj sigurnosti*, I. Osnovne odredbe, Članak 1., NN 79/07, https://www.zakon.hr/z/218/Zakon-o-informacijskoj-sigurnosti, datum pristupa: 07.05.2020.

[22] Ured Vijeća za nacionalnu sigurnost RH, (2014), Informacijska sigurnost - NSA, https://www.uvns.hr/hr/o-nama/djelokrug/informacijska-sigurnost-nsa, datum pristupa sadržaju: 01.02.2020.

odlukom Vlade u ime RH zaključuje međunarodne sigurnosne ugovore za zaštitu klasificiranih podataka.“ [23]



Slika 8 - Shematski prikaz djelokruga NSA

Izvor : Ured Vijeća za nacionalnu sigurnost, Shematski prikaz djelokruga NSA, 2014., raspoloživo na: https://www.uvns.hr/hr/o-nama/djelokrug/shematski-prikaz-djelokruga-nsa, (18.02.2020.)

Ulaskom Republike Hrvatske u Europsku uniju, sklopljeni su temeljni akti vezani za zaštitu i postupanje s podacima. Radi se o Ugovoru između Republike Hrvatske (dalje u tekstu: RH) i Europske unije o sigurnosnim postupcima za razmjenu tajnih podataka (NN MU 9/06) i Sigurnosni aranžman između UVNS-a (Ured Vijeća za nacionalnu sigurnost), GSCSO (Glavno tajništvo Vijeća Europske unije) i ECSD (Uprava za sigurnost Europske komisije) za zaštitu klasificiranih podataka razmijenjenih između EU i RH.

Agencija za zaštitu osobnih podataka navodi kako je osobni podataka „...*svaka informacija koja se odnosi na fizičku osobu koja je identificirana ili se može identificirati; osoba koja se može identificirati je osoba čiji se identitet može utvrditi izravno ili neizravno, posebno na*

[23] Ured Vijeća za nacionalnu sigurnost RH, (2014), Informacijska sigurnost - NSA, https://www.uvns.hr/hr/o-nama/djelokrug/informacijska-sigurnost-nsa, datum pristupa sadržaju: 01.02.2020.

osnovi identifikacijskog broja ili jednog ili više obilježja specifičnih za njezin fizički, psihološki, mentalni, gospodarski, kulturni ili socijalni identitet."[24]

Zaštita podataka nužna i za poslovne korisnike, ne samo za privatne osobe. Poslodavac je u cilju zaštite informacijske imovine, dužan poštivati zakone vezane za nezakonito prikupljanje, obradu i korištenje klasificiranih podataka i informacija.

U Zakonu o zaštiti tajnosti podataka definiraju se obveze pravnih osoba i navedeno je da „*pravna osoba dužna je čuvati kao tajnu i podatke:*

1) koje je kao poslovnu tajnu saznala od drugih pravnih osoba,

2) koji se odnose na poslove što ih pravna osoba obavlja za potrebe oružanih snaga, redarstvenih vlasti Republike Hrvatske ili drugih javnih tijela, ako su zaštićeni odgovarajućim stupnjem tajnosti,

3) podatke koji sadrže ponude na natječaj ili dražbu - do objavljivanja rezultata natječaja odnosno dražbe,

4) podatke koji su zakonom, drugim propisom ili općim aktom doneseni na temelju zakona utvrđeni tajnim podacima od posebnog gospodarskog značenja."[25]

Zlouporaba tehnologije sve je prisutnija, a blockchain nije izuzetak. Decentralizacija, anonimnost i sve šira mogućnost primjene omogućuju provođenje raznih ilegalnih aktivnosti poput pranja novca, financiranja terorističkih organizacija i krađe osobnih podataka. Upravo je zbog toga nužno regulirati blockchain tehnologiju.

Hrvatsko zakonodavstvo nije reguliralo korištenje blockchaina u svrhu platnog prometa i provođenja financijskih usluga, dok je EU 3. listopada 2018. godine donijela Rezoluciju o decentraliziranom vođenju evidencija transakcija[26]. Ovom je rezolucijom EU priznala blockchain kao alat koji može pomoći u poboljšanju raznih sektora gospodarstva i kvalitetu

[24] AZOP - Agencija za zaštitu osobnih podataka, (2020), *Općenito o zaštiti osobnih podataka*, https://azop.hr/info-servis/detaljnije/opcenito-o-zastiti-osobnih-podataka, datum pristupa sadržaju: 07.02.2020.

[25] *Zakon o zaštiti tajnosti podataka*, NN 108/96, VIII. Poslovna tajna, članak 20, https://www.zakon.hr/z/748/Zakon-o-za%C5%A1titi-tajnosti-podataka, datum pristupa 02.04.2020.

[26] Prijedlog Rezolucije 24.09.2018. podnesen nakon pitanja za usmeni odgovor B8-0405/2018, podnesenog u skladu s člankom 128. stavkom 5. Poslovnika o decentraliziranom vođenju evidencije transakcija i lancima blokova: izgradnja povjerenja poslovanjem bez posrednika (2017/2772(RSP)), Eva Kaili u ime Odbora za industriju, istraživanje i energetiku

javnih usluga. Uspješnost integracije ove tehnologije u financijski sektor najuspješnije je proveo Lihtenštajn. Iako Lihtenštajn nije članica EU, ova država prepoznala je potencijal nove tehnologije te je blockchain uključen u osnovnu granu gospodarstva. Istovremeno su postavljeni novi pravni okviri kojima se pruža sigurnost kako korisnicima, tako i pružateljima ovih usluga.

U svrhu sprečavanja pranja novca i financiranja terorizma, sve se više primjenjuju AML (Anti Money Laundering) i CTF (Counter-Terrorist Financing), koji propisuju obvezu i kontrolu identiteta korisnika u svrhu procjene korištenja tehnologije u nezakonite svrhe. Glavni instrumenti AML-a i CTF-a su KYC (Know Your Customer) i KYT (Know Your Transaction). KYC zahtjeva da pružatelj usluge od svojih korisnika zatraži osobne podatke (ime, prezime, adresa stanovanja…). Ti se podaci uspoređuju sa listom osoba za koje se sumnja da su uključene u nelegalne aktivnosti. Tek nakon provjere se omogućuje ili odbija pružanje određene usluge. KYC procedura je obavezna za sve pružatelje usluga koje se temelje na blockchain tehnologiji, prilikom prihvaćanja novih korisnika. Ova je procedura propisana petom „*Direktivom o sprečavanju korištenja financijskog sustava u svrhu pranja novca ili financiranja terorizma 2015/849*“ ili skraćeno AML5D. Europski parlament usvojio je ovu direktivu u lipnju 2018. godine, a Hrvatski sabor uključio je navedenu Direktivu u „*Zakon o sprečavanju pranja novca i financiranju terorizma*“ od 25. travnja 2019. godine. Međunarodna organizacija FATF (Financial Action Task Force) također se uključila u regulaciju transakcija kripto valuta te je u veljači 2019. godine izdala smjernice za nadzor kriptovaluta. Te smjernice propisuju prikupljanje i pohranu informacija o primatelju i pošiljatelju sredstava u svrhu dostave nadležnim tijelima u slučaju potrebe.

Uz sve navedeno, potrebno je spomenuti akte i zakone koji reguliraju područje zaštite podataka.

- **Opća uredba o zaštiti podataka (GDPR)**

Uredba EU o zaštiti podataka (dalje u tekstu kao: Uredba i GDPR) je donesena od strane Europskog parlamenta i Vijeća 27. travnja 2016. godine. Od toga datuma počinje teći prijelazno razdoblje od dvije godine te je GDPR u potpunosti primjenjiv od 25. svibnja 2018. godine. Osnovni cilj same Uredbe jest zaštita osobnih podataka pojedinca, odnosno omogućiti pojedincu pravo da u potpunosti ima nadzor nad osobnim podacima. U nastavku rada uredba će biti dodatno objašnjena.

- **Zakon o zaštiti tajnosti podataka**

Ovaj zakon bio je na snazi od 31. prosinca 1996. godine, a prestao je važiti stupanjem na snagu Zakona o tajnosti podataka dana 7. kolovoza 2007. godine, osim glave 8 i 9. Ovaj dio zakona odnosi se na poslovnu tajnu i profesionalnu tajnu te ih definira.

- **Zakon o tajnosti podataka**

Zakon je na snazi od 7. kolovoza 2007. godine (NN br. 79/07, 86/12). U Zakonu se navodi da se „*ovim Zakonom utvrđuju pojam klasificiranih i neklasificiranih podataka, stupnjevi tajnosti, postupak klasifikacije i deklasifikacije, pristup klasificiranim i neklasificiranim podacima, njihova zaštita i nadzor nad provedbom ovoga Zakona.*“ Definiraju se pojmovi kao što su podatak, klasificirani i deklasificirani podaci, vlasnik podatka, certifikat i sl.

- **Kazneni zakon**

Dio zakona koji se odnosi na zaštitu podataka je „Glava dvadeset peta (XXV) – Kaznena djela protiv računalnih sustava, programa i podataka“. Ovaj dio zakona definira neovlašteni pristup, ometanje rada računalnog sustava, oštećenje računalnih podataka, neovlašteno presretanje računalnih podataka, računalno krivotvorenje, računalna prijevara, zlouporaba naprava i teška kaznena djela protiv računalnih sustava, programa i podataka. Kazneni zakon (NN br. 125/11, 144/12, 56/15, 61/15, 101/17, 118/18, 126/19) za pojedino kazneno djelo propisuje i primjerene kazne:

- za neovlašteno prikupljanje, obrada ili korištenje osobnih podataka fizičkih osoba, predviđena je kazna zatvora do jedne godine (članak 146.)
- za neovlašteno otkrivanje profesionalne tajne od strane odvjetnika, javnog bilježnika, zdravstvenog radnika, psihologa, vjerskog ispovjednika, predviđena je kazna do jedne godine (članak 145.)
- za neovlašteni pristup informacijskom sustavu ili podacima predviđena je kazna zatvora do dvije godine (članak 266.)
- za omogućavanje pristupa tajnim podacima neovlaštenoj osobi, predviđena je kazna zatvora od šest mjeseci do pet godina (članak 347.)
- za odavanje tajnih podataka stranoj državi ili organizaciji predviđena je kazna zatvora od jedne do deset godina (članak 348.).

4.1. Opća uredba o zaštiti podataka (GDPR)

GDPR kratica je od engleskog naziva „General Data Protection Regulation“. Radi se o novom aktu koji štiti privatnost i osobne podatke, a primjenjuje se u svih 28 država članica EU. Uredba je usvojena 27. svibnja 2016. godine. Tada je počelo dvogodišnje prijelazno razdoblje te je navedena Uredba stupila na snagu 25. svibnja 2018. godine. Valja napomenuti kako, za razliku od direktive, uredba ima izravan učinak te je direktno primjenjiva u svim državama članicama EU bez potrebe donošenja provedbenih zakona.

Ova uredba donosi promjene koje će utjecati na poslovanje većine tvrtki, posebno na dio koji se odnosi na zaštitu i obradu podataka. Ne obrađuju sve tvrtke osobne podatke svojih klijenata s ciljem profita, ali sve tvrtke obrađuju podatke svojih zaposlenika i kandidata za posao. Ovaj dio poslovanja mora biti usklađen s GDPR-om.

Unatoč tome što je uredba izravno primjenjiva, države članice EU obvezale su se, s obzirom na osjetljivost i složenost područja primjene, donijeti provedbeni zakon. Tako je Republika Hrvatska donijela Zakon o provedbi Opće uredbe o zaštiti podataka (NN br. 42/18), čijim su donošenjem ujedno van snage stavljeni:

- Zakon o zaštiti osobnih podataka (NN br. 103/03, 118/06, 41/08, 130/11),
- Uredba o načinu vođenja i obrascu evidencije o zbirkama osobnih podataka (NN br. 105/04)
- Uredba o načinu pohranjivanja i posebnim mjerama tehničke zaštite posebnih kategorija osobnih podataka (NN br. 139/04).

Za bolje razumijevanje, potrebno je definirati pojmove koje uvodi sama Uredba;

Ispitanik je fizička osoba čiji se podaci prikupljaju i obrađuju. Ima pravo u bilo kojem trenutku dobiti informaciju koje njegove osobne podatke organizacija posjeduje i u koju ih svrhu koristi, može zatražiti brisanje svih osobnih podataka i može pokrenuti sudski postupak ako smatra da su se osobni podaci koristili van okvira GDPR-a.[27]

Vlasnik podataka je organizacija koja vrši prikupljanje podataka jednog ili više ispitanika i odgovorna je za usklađenost sa GDPR-om.[27]

[27] *GDPR – osnovni pojmovi* (2017), http://www.hrportal.com.hr/hr/gdpr/, datum pristupa: 15.03.2020.

Voditelj obrade je fizička ili pravna osoba koja sama ili u suradnji s drugima određuje svrhu i sredstva obrade osobnih podataka.[28]

Službenik za zaštitu osobnih podataka (DPO – *Data Protection Officer*) je osoba zadužena za kontrolu i usklađenost organizacije sa GDPR-om. Imenovana je od strane Voditelja obrade. Prema GDPR-u, službenika je potrebno imenovati ako organizacija ima više od 20 zaposlenih, ako raspolaže i obrađuje veliku količinu osobnih podataka ili ako vrši obradu osobnih podataka za drugu organizaciju.[27]

Izvršitelj obrade može biti ista osoba kao i Voditelj obrade ili može biti vanjski suradnik s kojim je sklopljen ugovor o pružanju ove usluge.[27]

Osobni podaci su svi podaci koji se odnose na neku osobu, tj. podaci koji mogu dovest do utvrđivanja identiteta nekog pojedinca. U osobne podatke se između ostalog ubraja identifikacijski broj, lokacija, fizičke osobine, genetski materijal, socijalni identitet, vjerska stajališta i dr.[29]

Cilj ove Uredbe je spriječiti zlouporabu privatnih podataka korisnika. Anketa „Eurobarometra“ pokazala je da dvoje od pet ispitanika brine da će netko koristiti njihove podatke bez da su ih o tome obavijestili. Analiza koju je provela „RSA Security“ također je dala slične podatke. Od 7.500 ispitanih osoba iz Francuske, SAD-a, Italije, Njemačke i Ujedinjenog Kraljevstva, čak 80% strahuje od povrede privatnosti. Zabrinutost se najviše odnosi na financijske i bankovne podatke, privatne lozinke i osobne podatke. Zanimljiv je podatak da 62 % korisnika za gubitak podataka okrivljuje tvrtke kojima su dali te podatke. Čak 72 % ispitanika bi bojkotiralo tvrtku koja ne štiti dovoljno privatnost korisnika, a 50 % ispitanika bi radije kupovalo kod onih tvrtki koje mogu dokazati da štite podatke klijenata.

Primjena GDPR odnosi se samo na osobne podatke. U te podatke ulaze podaci pomoću kojih se velikom vjerojatnošću može utvrditi nečiji identitet. Zaštita ostalih podataka, koji ne ulaze u osobne podatke, regulirani su nacionalnim zakonodavstvom država članica.

---

[28] *Što je voditelj obrade/izvršitelj obrade?*, Europska komisija, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_hr, datum pristupa: 15.03.2020.

[29] *GDPR i osobni podaci* (2018), GDPRinformer, https://gdprinformer.com/hr/gdpr-clanci/gdpr-osobni-podaci, datum pristupa: 15.03.2020.

„GDPRinformer“[30] na službenim stranicama navodi da GDPR pokriva slijedeće kategorije podataka:

- osnovni podaci – ime i prezime, broj osobne iskaznice, lokacijski podaci
- podaci s kreditnih kartica
- zdravstveni karton
- biometrijski podaci (sken rožnice, otisci prstiju itd.)
- genetski podaci (DNA i sl.)
- vjerska i filozofska uvjerenja
- etnička pripadnost
- ekonomsko stanje
- članstvo u sindikatu
- seksualna orijentacija i spolni život
- IP adrese
- osobne poruke e-pošte
- kolačići u pregledniku
- pseudonimizirani podaci.

Primjenjujući GDPR uredbu na blockchain, može se izvesti zaključak da blockchain tehnologija nije u skladu s GDPR. Zapis svih provedenih transakcija, informacije dostupne svima u svakom trenutku, pohranjene na svakom računalu na mreži i bez mogućnosti promjene zapisa ukazuju na neusklađenost s temeljnim zahtjevima GDPR-a. Ovo je posebno izraženo kod javnog blockchain-a. Privatni i hibridni blockchain se mogu uskladiti s zahtjevima GDPR jer imaju mogućnost kategoriziranja informacija na javne i privatne. Na ovaj način se podaci zaštićeni Uredbom (ime i prezime, IP adrese...) mogu „sakriti“. Ti bi podaci bili i dalje zapisani na mreži, ali ne bi bili vidljivi korisnicima. Druga je mogućnost korištenje hash funkcije na osobne podatke koji bi na taj način bili kriptirani.

Cilj Uredbe jest primjenjivost na postojeće ali i na nadolazeće tehnologije. Budući da svaki blockchain sadrži osobne podatke, kao i podatke o provedenim transakcijama, mora biti usklađen s GDPR. Blockchain je decentraliziran sustav, dok GDPR polazi od pretpostavke da se radi o centraliziranom sustavu koji obrađuje osobne podatke. Osnovni problem je nemogućnost brisanja jednom učitanih podataka u blockchain. To znači da jednom učitani

[30] www.gdprinformer.com , datum pristupa 02.04.2020.

podaci ostaju u blockchainu dokle god taj blockchain postoji - ti su podaci dostupni svim korisnicima i ne postoji mogućnost na „*right to be forgotten*“, kao pravo propisano GDPR-om.

Dodatni je problem što GDPR traži definiranje voditelja obrade, što je znatno otežano kod blockchain tehnologije budući da se svi korisnici blockchaina uklapaju u ovu ulogu. Svaka osoba koja je pretrpjela materijalnu ili nematerijalnu štetu zbog neovlaštenog korištenja osobnih podataka, ima pravo na naknadu štete od voditelja obrade. U praksi to znači da bi se naknada štete mogla tražiti od svih korisnika blockchain-a.

Iako je dio navedenih problema rješiv kod korisnika privatnih blockchain-a (gdje je sustav centraliziraniji), razvidno je da su potrebna nova tehnološka rješenja kako bi se sustav uskladio s GDPR-om. Trenutno postoje tri rješenja (koja najviše obećavaju):

- Off-chain – obrada podataka se vrši izvan blockchaina, a na blockchain se pohranjuje samo hash koji služi kao jedinstveni identifikator,
- Side-chain – korištenje paralelnog blockchaina na koji se spremanju osobni podaci,
- Zero knowledge proof – dokazivanje uključenim stranama je li neki prijedlog istinit pomoću kriptografskih tehnika, bez otkrivanja informacija o tom prijedlogu.

Sve veća opasnost od korištenja blockchain tehnologije u ilegalne svrhe zahtjeva donošenje pravnog okvira. Istovremeno, zagovornici blockchain-a se protive ovakvom nadzoru budući da je sam blockchain osmišljen da bude decentraliziran, odnosno bez centralnog entiteta. Vidljivo je da su donesene regulative teško primjenjive na postojeći blockchain i jasno je da će se morati postići kompromis s developerima, a sve u svrhu daljnjeg razvoja ove tehnologije.

5. BLOCKCHAIN TEHNOLOGIJA

Omogućujući distribuciju digitalnih informacija bez kopiranja, blockchain tehnologija otvorila je vrata novoj vrsti interneta. Izvorno osmišljen isključivo za digitalne valute, blockchain je tehnologija sa širokim spektrom mogućnosti i velikim potencijalom.

Sam naziv blockchain sastoji se od dva pojma – „*block*“ i „*chain*“. „*Block*“ se odnosi na transakcije, dok „*chain*“ opisuje način na koji su povezani blokovi. Lanac neprestano raste,

novi blokovi se stvaraju svakom novom transakcijom i kriptiranjem. Proces stvaranja blokova naziva se rudarenje („*mining*“).

Najjednostavnije rečeno, blockchain je vremenski obilježen niz nepromjenjivih zapisa podataka, kojima upravlja skupina računala, a koja nije u vlasništvu jedinstvenog entiteta. Svaki od blokova podataka je povezan sa drugim blokovima koristeći kriptografske protokole i zajedno čine lanac podataka.[31]

Blockchain je baza podataka u koju je moguće spremati podatke, informacije i dokumente. Kada se radi o kripto valutama, radi se o zapisima transakcija. Naziv koji se još koristi je „*distributed ledger*“, a može se prevesti kao „glavna knjiga“. Blockchain je kompletan popis svih transakcija neke kripto valute, odnosno glavna knjiga u kojoj je kronološki zapisana povijest svih transakcija. Prednost ove tehnologije je što je moguće na transparentan, jeftin i siguran način provoditi transakcije, verifikacije i automatizacije. Sam sustav je odlično zaštićen i koncipiran na način da je gotovo nemoguće probiti, odnosno manipulirati podacima. Ova metoda je prvenstveno razvijena za bitcoin ali se danas koristi i u drugim virtualnim valutama. Primarno se koristi za verifikaciju transakcija digitalnih valuta ali primjena može biti puno šira jer je moguće digitalizirati, kodirati i umetnuti praktički bilo koji dokument u blockchain.

Blockchain nema centralnu vlast. Ledger je zajednički i nepromjenjiv, sve zapisane informacije su svima vidljive i sve je transparentno. Svaka promjena u blackchain-u je vidljiva svima i svi su odgovorni za svoje postupke.

Blockchain ne nosi transakcijske troškove, samo infrastrukturne. Blockchain je jednostavan, ali genijalan način prijenosa informacija s točke A na točku B na potpuno automatiziran i siguran način. Jedna strana u transakciji pokreće postupak stvaranjem bloka. Taj blok provjerava na tisuće računala distribuiranih po mreži. Provjereni blok je dodan u lanac koji se pohranjuje preko mreže, stvarajući ne samo jedinstveni zapis, već i jedinstveni zapis s jedinstvenom poviješću. Falsificiranje jednog zapisa značilo bi falsificiranje cijelog lanca u milijunskim primjerima. To je gotovo nemoguće. Bitcoin koristi ovaj model za monetarne transakcije, ali može ga se primijeniti na mnogo drugih načina.

[31] Pratap M., (2018), *Blockchain Technology Explained: Introduction, Meanina, and Applications*, https://hackernoon.com/blockchain-technology-explained-introduction-meaning-and-applications-edbd6759a2b2, datum pristupa: 01.05.2020.

Sigurnost blockchain-a bazira se na ključnim obilježjima ove tehnologije, a to su decentralizacija, anonimnost, nepromjenjivost i integrirani kriptografski protokoli. Predviđen je za rad u decentraliziranom okružju, što je omogućeno spajanjem nekoliko osnovnih tehnologija kao što je kriptografski hash, kriptografski digitalni potpis i mehanizam konsenzusa sudionika sustava.

Iako je Bitcoin najpoznatija blockchain aplikacija, primjena u raznim drugim aplikacijama nadilazi svijet kripto valuta.

Omogućeno je decentralizirano provođenje transakcija što uveliko smanjuje troškove i poboljšava učinkovitost. Isključivanje treće strane kao posrednika omogućuje uštedu i široku primjenu u svim vrstama korištenja digitalne imovine. Uz sve ovo, blockchain tehnologija jedna je od najperspektivnijih tehnologija namijenjenih novim internetskim zahtjevima kao što su pametni ugovori, IoT i sigurnosni protokoli.

Blockchain ne samo da može prenijeti i pohraniti novac, već može u potpunosti zamijeniti sve procese i poslovne modele koji se oslanjaju na naplatu troškova provedenih transakcija. Velike tvrtke poput „Uber“ i „Airbnb“ razmišljaju o uvođenju blockchain tehnologije u svoj sustav naplate. Integracija bi bila relativno jednostavna (kodiranje i praćenje podataka vezanih za vožnju automobilom ili noćenje), a ušteda bi bila više nego značajna jer se u potpunosti ukida treća strana (strana koja provodi transakcije i naplaćuje naknadu). Blockchain omogućuje mikro transakcije, što pruža veliku mogućnost primjene u on-line industriji. Naplata sadržaja na video servisima, e-knjiga, video igara za računala ili mobitele i slične sadržaje moguća je u iznosima od npr. 1/100 centi. Glazbeni izvođači mogu iskoristiti prednosti blockchain tehnologije za direktnu naplatu svoje glazbe, isključujući velike glazbene servise poput Apple ili Spotify. Glazba se može ukodirati u sam blockchain i može funkcionirati kao oblak. Pretplate i streaming korištenjem ove tehnologije postaju suvišni.

U svijetu financija, primjena je očigledna, a uvođenjem blockchain tehnologije revolucionarne promjene su neizbježne. Promijeniti će se način rada burzi, plasiranje zajmova i ostalih bankovnih usluga. Svaka financijska ustanova koja temelji zaradu na naknadama za provođenje transakcija, morati će se promijeniti iz temelja. Burzovni posrednici više neće dobivati provizije, princip rada kupi/prodaj će nestati, a bankari će postati tek financijski savjetnici.

Informacije koje se nalaze na blockchain-u postoje kao zajednička, neprekinuta baza pohranjena istovremeno na svim računalima priključenima na mrežu. Ne pohranjuje se ni na jednom mjestu, svi zapisi su javni i lako provjerljivi.

5.1. Blockchain podjela

Blockchain se može podijeliti na tri osnovna tipa:

- javni blockchain
- privatni blockchain
- hibridni blockchain.[32]

Javni blockchain je blockchain kojem može pristupiti svatko, kao korisnik, developer ili član zajednice. U potpunosti je transparentan, sve su transakcije javne i dostupne svima na uvid, a zabilježene su redoslijedom kojim su provedene. U potpunosti je decentraliziran i ne postoji središnje kontrolno tijelo. Zbog toga je javni blockchain vrlo otporan na bilo koji oblik cenzure ili pokušaja gašenja. Kao primjer javnog blockchain-a možemo navesti Bitcoin i Ethereum.

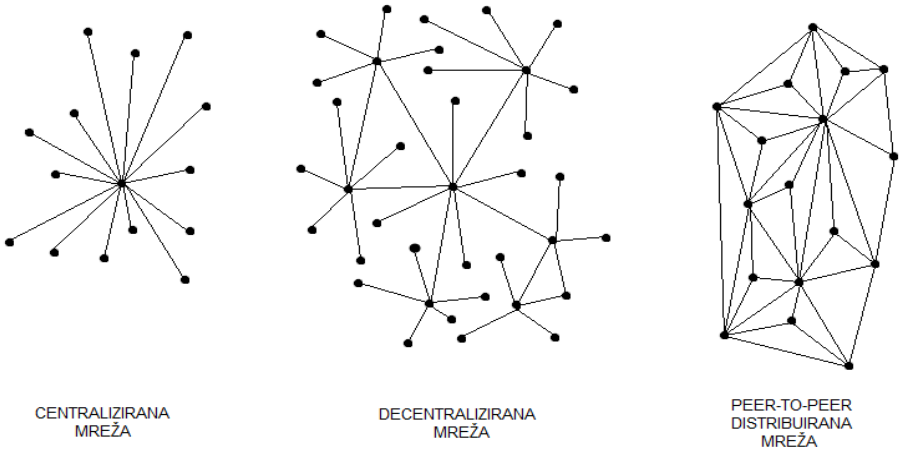
Privatni blockchain nije dostupan svima – kako bi netko pristupio potrebno je dobiti odobrenje zajednice. Sve su transakcije privatne i vidljive su samo članovima. Privatni blockchain najčešće koriste veliki poslovni sustavi, kao siguran način razmjene informacija, bez opasnosti od neovlaštenih vanjskih upada. Ovaj blockchain nije u potpunosti decentraliziran već postoji tijelo koje daje odobrenja ili odbija zahtjeve za pristup. Hyperledger i R3 Corda primjer su privatnog blockchain-a.

Hibridni blockchain ima karakteristike i javnog i privatnog blockchain-a. U praksi, to znači da postoji fleksibilnost koja omogućuje da dio podataka bude javan i vidljiv svima, a dio podataka ostaje privatan i vidljiv samo nekim članovima. Ovaj blockchain koriste poslovni sustavi koji na taj način distribuiraju informacije, uz jednostavnu kontrolu pristupa i bez potrebe za stvaranjem klasične baze podataka. Primjer ovakvog blockchain-a je Dragonchain.

[32] Glowacki J., (2018), *Blockchain: Public, Private or Hybrid?*, https://medium.com/@jackglowacki/blockchain-public-private-or-hybrid-664d4a413331, datum pristupa: 20.05.2020.

5.2. Blockchain struktura

Blockchain se temelji na decentraliziranoj „peer-to-peer“ mreži. To je način povezivanja računala u mrežu bez centralne točke (slika 8).



Slika 9 - Prikaz centralizirane, decentralizirane i „peer-to-peer“ mreže

Izvor : izradio autor prema izvorima s interneta

Svaka točka predstavlja „*node*“, odnosno računalo unutar mreže. Čvorovi su pojedinačna računala koja obavljaju neku funkciju nad inputima u mreži. Ne postoji središnje računalo ili server nego svako računalo unutar mreže komunicira direktno s drugim računalom unutar mreže, bez „posrednika“. Sve transakcije se verificiraju i validiraju u samoj mreži, stvaraju se novi blokovi i lanac stalno raste. Zbog decentralizacije i „peer-to-peer“ mreže, podaci su dodatno osigurani. Jednom zabilježene podatke gotovo je nemoguće manipulirati ili mijenjati, a ako dođe i do kvara na dijelu mreže, sustav može neometano funkcionirati i dalje.

Ovaj oblik umrežavanja dijeli cjelokupno radno opterećenje među svim sudionicima na mreži. Na taj se način olakšava i ubrzava rad i protok podataka cijele mreže. Istovremeno je povećana i sigurnost cijele mreže, jer ne postoji centralna jedinica preko koje se vrši protok podataka.

5.3. Centraliziran i decentraliziran sustav

Distribuirani sustav je model gdje računala na mreži komuniciraju i koordiniraju radnje prosljeđivanjem poruka. Ključno svojstvo decentraliziranih sustava je nepostojanje središnje kontrolne točke.

U knjizi „*The Gospel of Technology*“, autor Naskar piše da „s*vrha centraliziranog financijskog sustava ili bilo kojeg drugog sustava nije iskorištavanje ljudi, već osiguravanje stabilnosti u društvu.*“[33]

Vitaly Dmitriyevich "*Vitalik*" *Buterin*, suosnivač „Ethereum“ kripto valute i časopisa „Bitcoin Magazine“, smatra da postoje tri aspekta decentralizacije:

- arhitektonska decentralizacija – ovaj aspekt decentralizacije određuje kako je distribuirana mreža, a ovisi o broju fizički neovisnih hardverskih sustava u mreži, broja fizičkih računala spojenih na mrežu i broju koliko se njih može istovremeno pokvariti, a da se ne ugrozi rad cijele mreže,

- politička decentralizacija – ovaj aspekt određuje kojim stranama mreža vjeruje, odnosno koliko je donositelja odluka na mreži i koliko pojedinaca ili entiteta kontrolira računala u mreži,

- logička decentralizacija – ovaj aspekt bavi se konsenzusom na mreži, podrazumijeva da mreža može imati više varijacija vrijednosti za jednu stvar.

Vodeći se ovom teorijom, blockchain mreža je arhitektonski i politički decentralizirana. Arhitektonski jer se sastoji od mnogo računala lociranih širom svijeta, a politički je ni jedna strana ne kontrolira rad mreže.

Iako se neki dijelovi blockchain zajednice ne slažu i logički je decentralizirana, cijeli sustav radi na jednom cilju.

Tri su glavna argumenta decentralizacije i blockchain-a:

- tolerancija greške – obzirom da se cijeli sustav oslanja na mnoštvo odvojenih komponenti, mala je vjerojatnost da će decentralizirani sustav otkazati i prekinuti s radom.

[33] Naskar A., (2020), The Gospel of Technology

- otpornost na napade – decentralizirani sustavi nemaju središnju točku neuspjeha, ne postoji točka napada koja bi srušila cijeli sustav. Zbog toga je decentralizirani sustav otporniji na napade, a sami napadi traže više resursa.

- nemogućnost dogovora – dogovori sudionika u decentraliziranom sustavu s ciljem zlouporabe malo su vjerojatni. Kod centraliziranih sustava ovakav scenarij je moguć. Potrebno je nekoliko sudionika ili samo jedan u centralnoj točki kako bi došlo do zlouporabe. Kod decentraliziranih sustava, potreban bi bio dogovor većine korisnika mreže, što je skoro nemoguće.

Glavni nedostaci decentralizacije:

- gubitak fokusa – prevelika sloboda neovisnog odlučivanja na svim raznima sustava može stvoriti nejasnoće oko glavnih ciljeva i smanjiti njihovu važnost. Pojedini donositelji odluka mogu pokretati akcije koje su korisne za njihov segment, a nisu nužno korisne za cijeli sustav. Kod centraliziranih sustava, središnje tijelo donosi sve odluke, a ostatak sustava postupa po tim odlukama. Kod decentraliziranih sustava upravljanje je složeno, a donošenje odluka je sporo i ponekad zakašnjelo.

- dupliciranje poslova – po svojoj strukturi, decentralizirani sustavi su sigurni zbog koncepta suvišnosti. Svaki član sustava ponavlja isti zadatak, a to stvara neekonomičan sustav te se stvara nepotreban trošak resursa kao što su energija i novac.

- brzina reakcije – decentralizacija dovodi do gubitka brzine, odnosno produljuje se vrijeme postizanja konsenzusa određenog broja sudionika sustava. Napor potreban da se konsenzus postigne usporava proces donošenja odluka, dodatno troši resurse i smanjuje fokus na zajedničke ciljeve.

5.4. Blockchain komponente

Blockchain mreža sastoji se od čvorova ("*nodes*"). Čvor je računalo koje pokreće softver i pomaže u održavanju mreže, ponašajući se kao relej i prosljeđujući i primajući informacije s drugih računala na mreži. Svako računalo se može priključiti mreži i postati čvor, ako ima

dovoljno memorije. Primarna funkcija čvorova je da prosljeđuju informacije drugim čvorovima na mreži.[34]

Osnovne komponente od kojih se sastoji blockchain:

- čvor – računalo ili korisnik unutar blockchain mreže, naziva se još i "node"
- transakcija – najmanji dio blockchain sustava
- blok – struktura podataka koja sadrži informacije o transakcijama, distribuira se na sva računala na mreži
- lanac – niz međusobno povezanih blokova
- rudari – čvorovi koji rješavaju određena zadatke u svrhu verificiranja bloka
- konsenzus – skupna pravila za izvođenje blockchain operacija.

Način funkcioniranja blockchain-a može se objasniti u nekoliko koraka:

1. Želi se izvršiti transakcija s točke A na točku B - transakcije se ne moraju odnositi samo na kripto valute, može se raditi o dokumentima, tablicama, slikama, odnosno o bilo kojim informacijama u digitalnom obliku.
2. Transakcija generira blok – blok je potrebno validirati.
3. Blok se šalje svima na mreži – transakcija je vidljiva svima.
4. Transakcija se verificira unutar mreže - verifikacijom se provjerava imaju li strane koje vrše transakciju odobrenje. Verifikacija može biti izvršena odmah, ali i ne mora. Postoji nekoliko načina verifikacije, a najčešći je „proof-of-work" način.
5. Blok se dodaje u „public leadger" - time se stvara trajan zapis transakcije i ti se podaci više ne mogu mijenjati.
6. Transakcija prema točki B je izvršena – željena transakcija je izvršena.

Blockchain je povezani popis koji sadrži podatke ali sadrži i hash, koji služi kao poveznica sa prethodnim blokom i na taj se način stvara lanac. Zbog toga je blockchain toliko siguran način zaštite. Svaki pokušaj promjene, pa i najmanji, stvorit će efekt lavine. Ako dođe do pokušaja promjene bloka 5 od npr. strane hakera, doći će do promjene hash-a. Ta će se promjena odraziti na blok 4, što opet dovodi do promjene na bloku 3 i tako dalje. To će

[34] *Blockchain Architecture Basics: Components, Structure, Benefits & Creation,* (2019), https://medium.com/@MLSDevCom/blockchain-architecture-basics-components-structure-benefits-creation-beace17c8e77, datum pristupa: 22.04.2020.

dovesti do potpune promjene u cijelom lancu, a to je nemoguće. Na ovaj način blockchain postiže nepromjenjivost.

Javni i privatni ključ

Prilikom slanja bitcoin-a primatelju, na mreži se objavljuje namjera, a čvorovi skeniraju mrežu kako bi potvrdili postoje li sredstva za slanje i nisu li ta sredstva već poslana nekome drugome. Ako se ove informacije potvrde, transakcija se uključuje u sljedeći blok u nizu i generira se "javni ključ" koji se sastoji se od 34 slova i brojeva. Svaki "javni ključ" ima i svoj "privatni ključ" koji se sastoji od 64 slova i brojeva.

Broj znakova privatnog i javnog ključa ovisi o korištenoj enkripciji. Dok je "javni ključ" svima vidljiv, "privatni ključ" je tajan i dokaz je vlasništva.

Primjer javnog ključa:
3a7s5dae4f8w3a00s1m4trp3q8s6v9a2d8

Primjer privatnog ključa:
mg4r6q9c2d8z2h6hl3z8u2is469nq01be4ksvityxi42jtmvlgb842dur89kqx7c

Slika 10 - Primjer javnog i privatnog ključa

Izvor : Izradio autor

Svaku transakciju potrebno je potpisati privatnim ključem. Digitalni potpis šalje se u mrežu na provjeru valjanosti. Ako mreža potvrdi da je potpis napravljen privatnim ključem koji odgovara javnom ključu, transakcija će se provesti i zapisati u blok.

Hash i SHA-256 funkcije

U kontekstu blockchain-a, nepromjenjivost znači da nakon što je nešto uneseno u blockchain, više se ne može promijeniti. Ova karakteristika omogućena je korištenjem kriptografskih algoritama, konkretno hash funkcije. Hash pretvara input bilo koje duljine u output fiksne duljine. Najčešće korišten protokol je SHA-256 protokol. On omogućuje pretvaranje bilo koje količine podataka u fiksni izlaz duljine točno 256 bita. Ovo je vrlo korisno kod obrade velikih količina podataka.

"Hash" je proizvod složene matematičke funkcije koja bilo koju količinu teksta ili podataka smanjuje na niz od 64 znakova. Promjenom samo jednog znaka unutar podataka, dobije se potpuno različit "hash". Ovo je vrlo učinkovit način na koji blockchain mreža vrši provjere je li došlo do kakvih izmjena i je li transakcija ugrožena ili ne.[35]

Kao dio podataka, svaki blok sadrži hash prethodnog bloka. Ako dođe do promjene, doći će i do promjene hash-a trenutnog bloka. Ako je generiran novi blok, mora se promijeniti i hash tog bloka. Zbog toga je vrlo lako provjeriti je li došlo do promjena (željenih ili neželjenih), a istovremeno je vrlo teško utjecati na podatke od treće strane.

5.5. Blockchain nedostaci

Unatoč mnogim prednostima, blockchain ima i nedostataka. Iako je blockchain zbog svoje tehnologije i strukture jedna od najsigurnijih tehnologija, nije imun na zlouporabu.

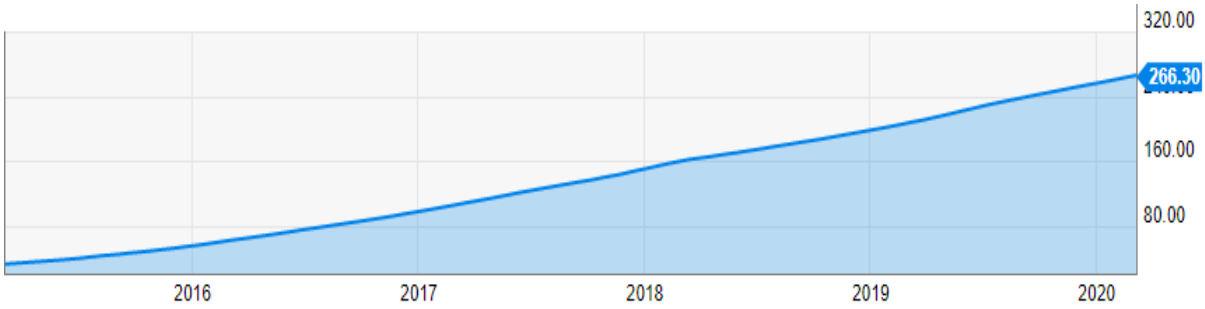
Postojeći algoritmi kao što su PoW (proof-of-work) i PoS (proof-of-stake) također nisu savršeni. PoW troši previše električne energije, a kod PoS postoji mogućnost fenomena obogaćivanja bogatih, odnosno korištenje ove tehnologije zahtjeva znatna financijska sredstva.

Govoreći o nedostacima, posebno se izdvajaju sljedeći;

- **Veličina**

Ovaj problem najlakše je prikazati na primjeru kripto valuta, gdje je blockchain temelj cijelog sustava. Svakodnevnim povećavanjem broja transakcija, raste broj blokova i samim time povećava se sam blockchain.

[35] *What Is SHA-256 And How Is It Related to Bitcoin?*, (2018), https://www.mycryptopedia.com/sha-256-related-bitcoin/, datum pristupa: 21.04.2020.



Slika 11 - Prikaz rasta Bitcoin blockchain-a

Izvor: YCharts.com, Bitcoin blockchain size, 2020., raspoloživo na: https://ycharts.com/indicators/bitcoin_blockchain_size (20.02.2020.)

Gornji graf prikazuje da je veličina Bitcoin blockchain-a na dan 05.03.2020. iznosila 266,30 GB. Prema istom izvoru, razvidno je da je u odnosu na isto razdoblje prošle godine zabilježen porast od 28,13%. Sve se transakcije moraju zabilježiti i zbog toga raste svakodnevno. Kod Bitcoin-a, veličina bloka ograničena je na 1 MB i za rudarenje jednog bloka potrebno je oko 10 minuta. Ograničenje veličine bloka i vrijeme potrebno da se stvori novi blok, ograničava blockchain na 7 transakcija u sekundi, što ne može zadovoljiti zahtjeve obrade milijuna transakcija u realnom vremenu i čini ga nekonkurentnim u visokofrekventnom trgovanju.

Sve ovo usporava rad cijele mreže i dovodi do mogućnosti neželjenog grananja blockchain-a. Rješenje u smislu povećanja veličine bloka znači da je potreban veći prostor za pohranu, što opet dovodi do smanjene brzine cijele mreže. S vremenom došlo bi i do centralizacije kako bi se uspio održati ovako veliki blockchain.

- **Curenje informacija**

Sigurnost blockchain-a je u tome da korisnici objavljuju samo generirane transakcije, a ne objavljuju svoje podatke. Međutim, budući da su sve transakcije i stanja vrijednosti vidljive za svaki javni ključ, blockchain ne može jamčiti potpunu privatnost.

Praćenjem određene transakcije i identificiranjem mrežnih čvorova preko kojih je provedena, može se doći do korisničke IP adrese, što opet dovodi do mogućnosti identificiranja pojedinca koji koristi tu IP adresu za pristup internetu.

6. BLOCKCHAIN PRIMJENA I BUDUĆI RAZVOJ

Primjena tehnologije blockchain je raznolika. U ovom dijelu obraditi će se neke od mogućnosti primjene.

- **Sigurnost**

Internet svakim danom sve više i više raste. Internetu se više ne pristupa samo preko osobnih računala. Prema prikupljenim podacima i statistikama, određeni izvori predviđaju[36]:

- u tekućoj godini na internet će biti priključeno 20.4 milijardi uređaja
- svake se sekunde na internet se priključi 127 novih uređaja
- do 2023. godine, na internet će biti priključeno 3.5 milijardi mobilnih uređaja.

Ovakvim rastom, raste i opasnost od virusa, hakerskih napada, krađe podataka i ostalih digitalnih prijetnji. Neke od mjera zaštite su filteri protiv zlonamjernih softvera gdje središnji poslužitelj usporedbom uzoraka pohranjuje i ažurira obrasce virusa. Ovakve centralizirane metode i dalje su ranjive na zlonamjerne napadače.

Blockchain može značajno poboljšati sigurnost distribuiranih mreža. Jedno takve rješenje predložio je Noyes (2016), ponudivši softver pod nazivom „BitAV“. Pomoću ovog programa, korisnici mogu sami distribuirati obrasce virusa na blockchain, čime se poboljšava tolerancija pogreške. Povećava se brzina skeniranja i sama točnost skeniranja. Blockchain se može iskoristiti u poboljšanju sigurnosne infrastrukture, primjerice za stvaranje privatnih ključeva.

- **Zaštita privatnosti**

Pristupom internetu, slanjem poruka, plaćanjem karticama i sličnim svakodnevnim radnjama, ostavljamo digitalni trag. Dok neke stvari radimo nesvjesno, pristupom društvenim mrežama svjesno dajemo informacije o sebi. Svaka objavljena slika, lokacija ili komentar ostavlja manje-više trajan digitalni trag. Blockchain ovdje nudi rješenje za poboljšanje zaštite privatnosti. Većina društvenih mreža i sličnih servisa sprema podatke na središnjim poslužiteljima (serverima).

U svom radu, Zyskind[37] predlaže decentralizirani sustav za upravljanje osobnim podacima gdje se osigurava da vlasnik zadržava vlasništvo nad osobnim podacima. Ovaj sustav nudi zaštitu nad podacima, transparentnost i preciznu kontrolu pristupa.

- **Financijske usluga**

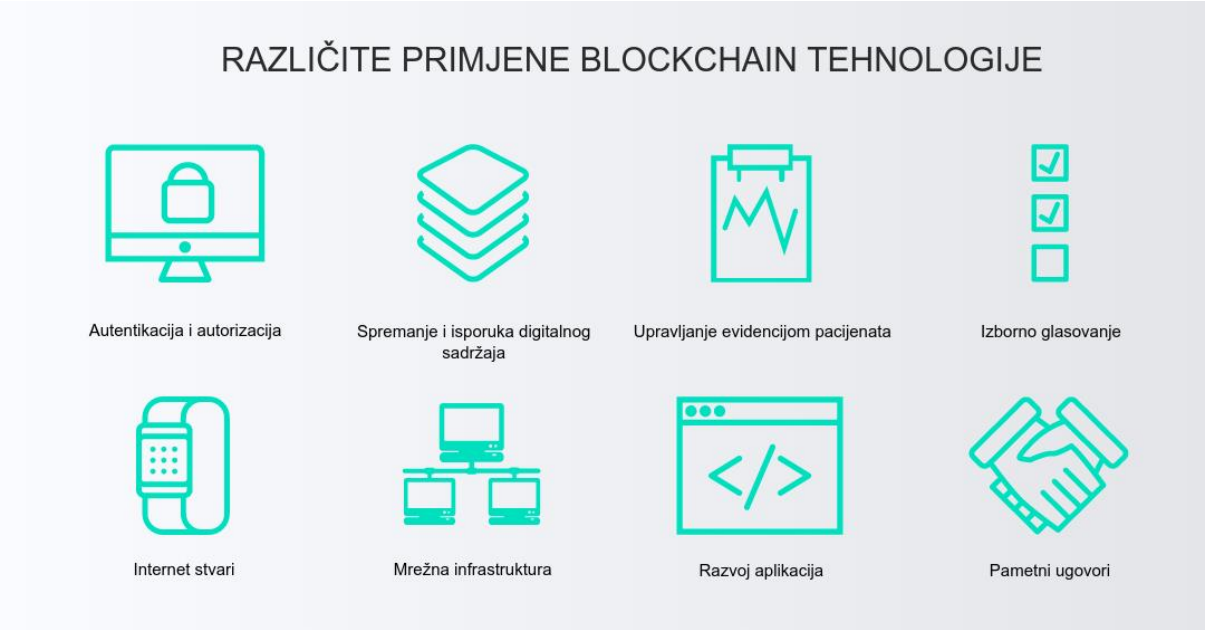
[36] www.vxchange.com , datum pristupa 02.04.2020.

[37] Zyskind, G., Nathan, O. et al. (2015) '*Decentralizing privacy: Using Blockchain to protect personal data, Secirity and Privacy Workshops* (SPW), 2015 IEEE, IEEE, pp. 180–184.

Rick Falkvinge, osnivač švedskog društva „Piratpartiet“ navodi kako će bitcoin bankama učiniti što je e-mail učinio poštanskoj industriji.

Bitcoin, prva komercijalna kripto valuta i ujedno pokazatelj prave moći blockchain tehnologije, imao je ogroman utjecaj na tradicionalno financijsko poslovanje i usluge. Peters, G.W. and Panayi, E. u svom radu iz 2015. godine pod naslovom '*Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money*', pišu o prijetnji koju blockchain predstavlja svijetu bankarstva.

Softverske tvrtke poput Microsoft Azure i IBM prepoznale su potencijal i počele su nuditi blockchain kao uslugu.



Slika 12 - Različite primjene blockchain tehnologije

Izvor: autor Aljoša Lovrić-Petrić, Bitcoin i blockchain: Internet vrijednosti, 2017., raspoloživo na: https://mercury-processing.com/hr/blog/bitcoin-blockchain-internet-vrijednosti/ (02.02.2020.)

- **P2P tržište**

Peer-to-peer predstavlja umrežavanje računala bez poslužitelja. Na ovaj način računala, odnosno korisnici, komuniciraju direktno. Blockchain omogućava ovakav način umrežavanja što otvara nove mogućnosti primjene. Razmjena podataka ili plaćanje među korisnicima na mreži uvelike je olakšano, a bez prisustva treće strane koja je u ulozi posrednika, nema ni troškova.

- **Upravljanje rizicima**

Upravljanje rizikom ima značajnu ulogu u financijskim krugovima. Pilkington u svojem radu iz 2016. godine „*Does the Fintech Industry need a New Risk Management Philosophy? A Blockchain Typology for Digital Currencies and e-money Services in Luxembourg“*, objavljenom u časopisu Social Science Research Network, pruža novi pogled na upravljanje rizikom, gdje se blockchain tehnologija koristi u analizi financijskog rizika. Pomoću blockchain-a, o ulaganjima i kolateralima može se brzo odlučivati, bez potrebe za duljim analizama i razmatranjima. Zbog same sigurnosti ove tehnologije, omogućena je veća razina transakcijske sigurnosti i istovremeno smanjen rizik čuvanja.

Veliki potencijal ove tehnologije pruža razne mogućnosti primjene. Kao mogući smjer budućeg razvoja navodi se analiza velikih podataka, pametni ugovori i kripto valute.

- **“Big data” analiza**

Blockchain se kod analize velikih podataka može najbolje iskoristiti u upravljanju podacima i analizi podataka.

Upravljanje podacima vrši se tako što se blockchain koristi za pohranu podataka, distribuciju i zaštitu. Blockchain također osigurava izvornost podataka, informacije se ne mogu krivotvoriti i teško ih je ukrasti i manipulirati njima.

Transakcije na blockchain-u mogu se koristiti za razne vrste analize. Najočitiji primjer je izdvajanje obrazaca trgovanja korisnika. Na taj se način prate navike korisnika i stvaraju se obrasci koji pomažu kod predviđanja budućih ponašanja.

- **Pametni ugovori**

Szabo N. Je u svom radu “*The Idea of Smart Contracts“* iz 1997. godine definirao pametni ugovor kao računalni protokol transakcija koji izvršava uvjete ugovora. Iako ideja postoji već dugo, blockchain može ovu ideju realizirati. Pametni ugovori mogu se integrirat u blockchain kao dio koda koji se izvršava automatski. Razvojem novih platformi, pametni ugovori mogu proširiti svoju primjenu. Jedna od tih platformi je Etherum. Razvojem blockchain-a, razvija se sve više aplikacija na osnovi temeljnih ugovora i to je nešto što je potrebno uzeti u obzir u skoroj budućnosti.

Jedna od prvih zemalja koje su prepoznale blockchain kao najbolji način zaštite podataka je Estonija. Kalle Palling, mladi estonski političar i član estonskog parlamenta, održao je 2018. godine predavanje u sklopu Zagreb Connecta na temu digitalizacije Estonije. Podijelio je svoje viđenje digitalizacije javnog i privatnog sektora, osobna iskustva, kao i daljnje planove za digitalizaciju Estonije. U intervjuu održanom nakon predavanja, izjavio je da je „*...e-Uprava strateški izbor Estonije i cilj joj je poboljšati konkurentnost zemlje te povećati dobrobit njezinih građana. Naš je san imati što je moguće manju vladu, ali vladu koja je dostupna 24 sata dnevno…. Digitalna transformacija bilo koje zemlje predstavlja društvenu i bihevioralnu promjenu. Vjerujem kako goleme promjene ponašanja u društvu, poput prihvaćanja e-identiteta, ne može promicati isključivo javni sektor – važan je i angažman privatnog sektora jer upravo oni pružaju većinu usluga koje ljudi svakodnevno koriste*."

Nakon opsežnih testiranja tehnologije koja će na najsigurniji način omogućiti digitalizaciju, Estonija se odlučila za blockchain tehnologiju. Upravo se blockchain pokazao kao najsigurnija tehnologija, ali i kao tehnologija koju je najlakše integrirati i prilagoditi širokoj upotrebi. Testira se još od 2008. godine, a od 2012. godine blockchain se koristi u estonskom nacionalnom sustavu zdravstvene zaštite, pravosudnom i zakonodavnom sustavu te se planira skoro proširenje na ostale nacionalne sustave. Upravo zbog prepoznavanja važnosti i svih prednosti digitalizacije, kao i velikog iskustva, Estonija je sjedište Centra izvrsnosti za kooperativnu kibernetičku obranu NATO-a te IT agencije EU-a. Obje navedene organizacije koriste estonsku KSI blockchain tehnologiju za zaštitu svojih sustava.

7. KRIPTOVALUTE

Blockchain je jedna od novijih i najperspektivnijih tehnologija za zaštitu podataka. Razvoj blockchain tehnologije usko je povezan s razvojem kripto valuta. Bitcoin, koji se često naziva prvom kripto valutom, doživio je velik svjetski uspjeh na tržištu. Upravo je blockchain temelj na kojem je izgrađen Bitcoin, a kasnije i sve ostale digitalne valute. Za bolje shvaćanje blockchain tehnologije i primjenu iste, potrebno je upoznati razvoj kripto valuta.

Satoshi Nakamoto ključna je osoba u stvaranju blockchain-a, bitcoin-a i kripto valuta kakve danas poznajemo. Njegov identitet nikad nije otkriven ni potvrđen pa se ni danas ne zna tko se krije iza imena i radi li se uopće o samo jednoj osobi ili grupi ljudi.

U listopadu 2008. godine objavljuje tzv. „*white paper*“, odnosno rad pod nazivom „*Bitcoin: A Peer-to-Peer Electronic Cash System*“, gdje je prvi puta riješen problem svih digitalnih valuta – „*double-spending*“. Termin „*duble-spending*“ odnosi se na rizik stvaranja duplikata digitalnih potpisa i podataka čime se stvara mogućnost slanja kopije drugoj strani, dok se istovremeno zadržava original. Jednostavnije rečeno, radi se o neovlaštenom tiskanju novca ali u digitalnom obliku. Taj je problem specifičan za digitalne valute jer se „fizički“ novac teže reproducira i lakše je uočiti nepravilnost budući da postoje nadzorna tijela. Rješenjem tog problema stvoreni su temelji za sve kripto valute.

U siječnju 2009. godine na internetu je objavljen prvi „*open Source client*“, nakon čega je stvorena Bitcoin mreža i prve jedinice nove kripto valute – bitcoin.

Do sredine 2010. godine, Nakamoto je bio glavni programer te je sve izmjene i sam razvoj programa radio isključivo on. Nakon 2010. godine, Nakamoto prepušta projekt Gavinu Andersenu.

Stvaranjem Bitcoin-a, Satoshi Nakamoto uspio je ostvariti ono što mnogi prije njega nisu – stvoriti novac koji mogu koristiti svi, ne košta ništa, nema kamata na njega, nije centraliziran i otporan je na inflaciju.

Iako je Bitcoin najpoznatija kripto valuta, nije i prva. Čak su četiri kripto valute zamišljene prije bitcoin-a – B-Money, Bit Gold, Digicash i Hashcash.

- **B-money**

“B-money” predstavljen je 1998. godine od strane računalnog znanstvenika Wei Dai. Cilj je bio stvoriti anonimni, distribuirani elektronički novčani sustav, odnosno pružiti iste ili slične usluge kao što to čine današnje kripto valute.

Wei Dai u svom radu gdje se prvi puta spominje B-money, stvara temelje suvremenog svijeta kripto valuta. Opisuje sustav kao shemu za skup digitalnih pseudonima kojima se ne može ući u trag i koji će međusobno moći plaćati novcem bez potrebe za vanjskom pomoći.

Koncept koji je osmislio Dai uključivao je i sadržavao niz značajki koje su danas postale uobičajene za kripto valute. Neke od tih značajku su “proof-of-work”, odnosno procesorski rad u stvaranju i dobivanju B-money kao i kolektivno knjigovodstvo gdje bi se bilježile sve

izvršene transakcije. Kriptografski protokoli, korištenje digitalnog potpisa ili javnih ključeva dodatno bi osigurali autentičnost provedenih transakcija, a samim time i sigurnost.[38]

"B-money" nikad nije pokrenut, sve je ostalo samo na znanstvenom radu. Međutim, ovaj rad postao je temelj za daljnji razvoj kripto valuta. Satoshi Nakamoto je prilikom razvijanja Bitcoina tražio pomoć i savjet od Wei Dai. Iako postoji puno sličnosti između Bitcoin-a i B-money, točan odnos nikad nije utvrđen, a sam Wei Dai navodi da je njegova "povezanost s projektom prilično ograničena". Iako je njegov rad pomalo zasjenjen novijim i uspješnijim projektima kripto valuta, Wei Dai ostaje primarna figura u razvoju ove industrije. Njemu u čast, najmanja jedinica kripto valute "Ether" nazvana je "wei" a mnogi developeri i članovi ove zajednice vjeruju da će se s vremenom Wei Dai otkriti kao osoba koja se krije iza imena Satoshi Nakamoto.

- **Bit Gold**

„Bit Gold" je financijski sustav koji je osmislio Nick Szabo 2005. godine. Temelji se na raznim elementima kriptografije i rudarstva u svrhu postizanja učinkovite decentralizacije. Sustav je imao svoj sistem verifikacije sličan onom koji koristi Bitcoin danas i oponašao je današnji blockchain. Ti elementi uključuju vremenski označene blokove koji su pohranjeni u registru, a generirani su na principu "proof-of-work". Prema ideju Szaba, Bit Gold sustav sastoji se od nekoliko koraka. Započinje generiranjem javnog niza izazova pomoću referentne funkcije slično kao kod bitcoina. Korisnik generira "proof-of-work", a informacije o provedenoj transakciji pohranjuju se u registru. Završava stvaranjem novog niza, čime završava prethodni niz. Ovo je slično stvaranju blokova u bitcoinu, gdje se hash adrese koriste kao zaglavlja koja upućuju na sljedeći niz blokova. To je i bila prva kripto valuta koja je pokušala riješila problem „double spending" isključujući posrednike.

Bit Gold je važan zbog nekoliko razloga:

- Prvi je izvediv prijedlog decentralizirane financijske mreže
- nudi rješenje neučinkovitosti tradicionalnog financijskog sustava i uporabe plemenitih metala kao valute
- decentralizirana financijska mreža mogla bi ukloniti ovisnost o financijskim institucijama, a istovremeno osigurati neometano i sigurno prekogranično poslovanje
- osmišljen je na protokolima koji su kasnije iskorišteni prilikom stvaranja Bitcoin-a.

[38] Frankenfield J., *B-money* (2019), https://www.investopedia.com/terms/b/bmoney.asp, datum pristupa: 20.03.2020.

Ova kripto valuta također nije zaživjela zbog ranjivosti cijelog sustava na hakerske napade („*Sybil attack*“), pa samim time nije moguće spriječiti moguće manipulacije.

- **Digicash**

„Digicash“ je prva kripto valuta koja je omogućavala anonimnost koristeći kriptografiju. DigiCash je 1989. godine osnovao David Chaum - jedan od pionira digitalnih valuta. Razvio je brojne kriptografske protokole koji su DigiCash izdvojili od konkurencije. DigiCash nije ostao na papiru kao ideja već je i pokrenut te je bio aktivan nekoliko godina. Nije doživio uspjeh kao što su očekivali njegovi tvorci i 1989. godine proglašen je bankrot, a DigiCash je prodan konkurentskoj tvrtki „eCash Technologies“.

David Chaum bio je zagovornik kriptografije javnih i privatnih ključeva, i na tome je temeljio DigiCash. Bio je potreban određeni software koji je omogućavao povlačenje bilješki iz banaka uporabom određenih šifriranih ključeva. To je omogućavalo i provođenje transakcija između pošiljatelja i primatelja. Tehnologija koju je David Chaum izumio, poznata kao “Blind Signature”, dodatno je poboljšala sigurnost i omogućila digitalna plaćanja bez mogućnosti uplitanja ili praćenja od treće strane. Iako je ova tehnologija imala potencijala da revolucionira platnu industriju, nije naišla na podršku. DigiCash sustave podržale su samo dvije banke, jedna američka i njemački Deutsche Bank. Nije uspjelo dovoljno povećati svoju korisničku bazu da podrži poslovanje i došlo je do pada cijelog sustava. Još jedna prepreka potencijalnom uspjehu bila je nemogućnost dogovora s bankama oko uključenja DigiCash sustava u kartično poslovanje. Najperspektivnija potencijalna suradnja bila je sa Citibankom, ali su se preusmjerili na druge projekte i DigiCash je odbijen.

Zbog sukoba rukovodstva i zaposlenika, Chaum je 1996. godine napustio tvrtku. Dvije godine nakon toga, proglašen je stečaj.

- **HashCash**

Na Godišnjoj međunarodnoj konferenciji o kriptografiji 1992. godine (“*Annual International Cryptology Conference*”) predstavljen je rad pod nazivom „*Pricing via Processing or Combatting Junk Mail*“. Rad su objavili istraživači Cynthia Dwork i Moni Naor. Rad sadrži detaljan opis sustava za smanjivanje neželjene pošte, odnosno „*spam*“ pošte. Uvođenje protokola poznatog kao „*pricing function*“, korisnik bi korištenjem procesorske snage dobio pristup sustavu, odnosno e-mailu.

Pet godina kasnije britanski kriptograf Adam Back predložio je sličan mehanizam i nazvao ga HashCash. Sam sustav razvijan je u svrhu sprečavanja spam mailova i DDoS napada. Temelji se na „proof-of-work“ algoritmima i generiranju valute. Koristio je kriptografsku funkciju SHA-1 za stvaranje sigurnosnih pečata i bolje kontrole rada sustava. HashCash sustav koristile su neke velike kompanije kao što su Mozilla i Microsoft, u kontroli i suzbijanju neželjene pošte.
Oko HashCash i tvorca Adam Black postoji dosta kontraverzi. Dio kripto zajednice vjeruje da je samo prepravio rad Dwork i Naor i time nije pravi tvorac ovog sustava. Isto tako navodi da Bitcoin koristi neke njegove algoritme, što se pokazalo netočnim.

Sustav nije zaživio zbog tehnoloških ograničenja. Povećanjem broja mailova poslanih kroz sustav, tražilo se sve više procesorske snage, a davne 1997. godine to nije bilo moguće (isplativo).

Unatoč tome što ni jedna od navedenih kripto valuta nije opstala, mnoge značajke i rješenja iskorištena su u stvaranju kripto valuta kakve danas poznajemo.

U nastavku je na primjeru kripto valute Bitcoin i platforme Ethereum, objašnjen način na koji blockchain tehnologija funkcionira u praksi. Zaštita podataka od iznimne je važnosti prilikom provođenja vrijednosnih transakcija i blockchain tehnologija kod trgovanja kripto valutama pokazuje sve svoje prednosti, ali i nedostatke. Decentraliziran sustav, kriptografske funkcije i sustav validacije samo su neki od sustava zaštite podataka koje koristi blockchain, a objašnjeni su u nastavku rada.

7.1.BITCOIN

Bitcoin je danas jedna od najpopularnijih kripto valuta. Prva transakcija, odnosno plaćanje provedeno je 2010. godine kada su dvije pizze plaćene sa 10.000 jedinica bitcoina. Prema današnjoj vrijednosti, radi se o nekoliko desetaka milijuna američkih dolara.

Bitcoin ima unaprijed ograničen broj jedinica koje mogu biti izdane, kao i sve ostale kripto valute. Kod bitcoin-a se radi o 21 milijun jedinica. Do danas je izdano oko 17,5 milijuna jedinica, a ostalih 3,5 milijuna će se izdati u narednih 20-ak godina. Ovaj vremenski rok se može promijeniti. S vremenom rudarenje postaje sve teže jer je verifikacija blokova sve kompliciranija. Ali treba uzeti u obzir napredak tehnologije pa postoji mogućnost da će preostale jedinice biti izdane i prije.

Kao i sve kripto valute, bitcoin je izrazito cjenovno nestabilan (volatilan). Na vrijednost utječe nekoliko faktora:

- ponuda i potražnja – ako je potražnja velika a ponuda ne zadovoljava potražnju, cijena raste. Ovdje je ponuda strogo kontrolirana jer se zna da je bitcoin ograničen na 21 milijun jedinica.

- pokušaj kontrole i nadzora – mnoge države nemaju zakonske regulative vezane za bitcoin. Na velik porast vrijednosti imala je odluka Japana koji je 2017. godine prihvatio bitcoin kao legalno sredstvo plaćanja. Uz Japan mogu se spomenuti i UK, Kanada i USA.

- utjecaj medija – pozitivni ili negativni komentari u medijima imaju jak utjecaj. Pozitivni povećavaju interes javnost a samim time raste i potražnja dok negativni komentari imaju negativan učinak.

- korisnici i developeri – zbog uspjeha bitcoin-a, pojavile su se mnoge druge kripto valute. Developeri su razvili (i razvijaju) kripto valute koje su naprednije i na korisnicima je za što će se odlučiti. Faktor povjerenja je također ključan. Informacije i iskustva koje razmjenjuju korisnici na specijaliziranim forumima također utječu na popularnost. Iako postoji već desetak godina, bitcoin je još uvijek najpopularnija kripto valuta.

- nove tehnologije – kao primjer može se navesti prihvaćanja bitcoina kao sredstva plaćanja u PayPal sustavu. I sam blockchain sustav, na kojem se temelji Bitcoin, prepoznat je kao tehnologija koja ima široku primjenu u svim granama industrije.

Ideja je bila stvoriti sredstvo razmjene koje će biti neovisno o bilo kojem obliku središnjeg tijela, koje se može elektronički prenijeti na siguran i nepromjenjiv način te bez zastoja i trenutno. Sustav omogućuje transakcije između dvije strane, pošiljatelja i primatelja, bez potrebe za središnjim tijelom poput banke. Valuta se stvara i održava elektronički, ne postoji u fizičkom obliku poput novčanice ili kovanice. Proizvodi se putem računala, rudarenjem, bilo gdje u svijetu. Bio je to prvi primjer onog što danas nazivamo kripto valute.

Bitcoin je revolucionaran. Prvi je uveo nekoliko važnih promjena koje su temelj svih današnjih kripto valuta.

- **Decentralizacija**

Najvažnija karakteristika Bitcoin-a je da je on decentraliziran. Ni jedna institucija ili pojedinac ne kontrolira bitcoin mrežu. Održava ga grupa volontera, a sastoji se od otvorene mreže računala raširenih diljem svijeta. Na ovaj je način izbjegnuta kontrola banke ili vlade nad valutom i cijelim sustavom. Riješen je i "problem dvostruke potrošnje", odnosno

mogućnost kopiranja digitalne imovine sa svrhom ponovnog korištenja. Dosad su ovu funkciju izvršavale banke, koje su imale kontrolu na tradicionalnim sustavom. Bitcoin integritet transakcija održava samostalno, koristeći kriptografiju i matematičke algoritme, putem vlastite distribuirane i otvorene mreže.

- **Ograničena ponuda**

Fiat valute (euro, dolar, jen...) imaju neograničenu opskrbu. Središnje banke mogu izdavati koliko žele i time se otvara mogućnost manipulacije vrijednošću u odnosu na ostale valute. Kod bitcoin-a, opskrba je pod strogom kontrolom temeljnog algoritma. Rudarenjem se svakog trenutka generira mali broj novih bitcoin-a i to će se nastaviti padajućom brzinom sve dok se ne postigne maksimalan iznos od 21 milijun. Ekonomski gledano, ovo bitcoin čini vrlo atraktivnim – ako potražnja raste a ponuda ostaje ista, vrijednost će se povećavati.

- **Anonimnost**

Kod tradicionalnih elektroničkih transakcija, pošiljatelj i primatelj se moraju identificirati. U bitcoin mreži ne postoji središnji validator i korisnici se ne moraju identificirati prilikom slanja ili primanja valute. Sudionici u transakciji rade u anonimnosti, sustav ne treba znati njihov identitet. Kad se podnese zahtjev za transakciju, protokol provjerava sve prethodne transakcije kako bi se utvrdilo raspolaže li pošiljatelj sredstvima i ima li ovlasti za njihovo slanje. U praksi, svaki se korisnik identificira adresom svog novčanika. Zbog moguće zlouporabe, razvijeni su alati koji uz određen napor, mogu identificirati korisnike. Također je zakonski regulirana provjera identiteta prilikom većih kupovina ili prodaja bitcoina, u svrhu sprečavanja pranja novca i drugih ilegalnih aktivnosti.

- **Nepromjenjivost**

Bitcoin transakcije ne mogu se poništiti. Jednom provedene, transakcija ostaje zabilježena u blockchain mreži i nepovratna je. U sadašnjem bankarskom sustavu, banka je središnje tijelo koje može samostalno ili na zahtjev korisnika odlučiti poništiti već provedenu transakciju. Bez centralnog tijela, za bilo kakvu promjenu u bitcoin sustavu, potrebna je suglasnost svih uključenih korisnika.

- **Djeljivost**

Najmanja jedinica bitcoin-a zove se satoshi. To je 0,00000001 dio bitcoin jedinice. Ovakva djeljivost omogućuje mikro transakcije koje tradicionalni elektronički novac ne može.

7.2. Ethereum

Za izradu blockchain aplikacija potrebno je veliko iskustvo u programiranju, poznavanje kriptografije i matematike. Ethereum je to promijenio i omogućio je brzo i kvalitetno razvijanje aplikacija korištenjem vlastitog blockchain-a.

Ethereum je otvorena platforma koja se bazira na blockchain tehnologiji i omogućava programerima razvoj decentraliziranih aplikacija razne namjene. Kreirao ga je ruski programer Vitalik Buterin krajem 2013. godine. Ideja je bila da omogući stvari koje Bitcoin nije omogućavao, odnosno da ne bude smo još jedna kripto valuta nego da se razvije u nešto mnogo veće. Vitalik Buterkin nije žalio samo proširiti izvorni kod Bitcoina, već je razvio potpuno novi blockchain kao zasebnu platformu.

Ethereum je pokrenut 2015. godine i jedan je od vodećih programerskih blockchain-ova. Kao i svaki drugi blockchain, Ethereum ima izvornu valutu pod nazivom Ether (ETH). Kao i sve ostale kripto valute, Ether je digitalni novac koji se koristi diljem svijeta za plaćanje, pohranu vrijednost ili kolateral.

Ethereum se razlikuje od ostalih jer je programibilan, može se koristiti za stvaranje novih aplikacija. Ove decentralizirane aplikacije ("dapps") koriste prednosti kripto valuta i blockchain tehnologije. Takve aplikacije su pouzdane i izvode se unutar sustava točno kao što su programirane, mogu kontrolirati digitalnu imovinu, stvarati nove financijske aplikacije i decentralizirane su, odnosno ne kontrolira ih ni jedna osoba ili entitet.[39]

Te se aplikacije mogu podijeliti u nekoliko glavnih grupa:

- „spremnici" digitalnih valuta koji omogućuju spremanje digitalnih valuta, kao i trenutne transakcije između primatelja i uplatitelja
- financijske aplikacije koje omogućuju pozajmljivanje, ili investiranje digitalnih sredstava
- decentralizirana tržišta koja omogućuju trgovinu digitalnom imovinom ili trgovinu "predviđanjima" o događajima u stvarnom svijetu
- igre gdje raspolažete stvarnim sredstvima i na taj način zarađujete ili trošite.

[39] *Use Ethereum Applications* (2020), https://ethereum.org/en/dapps/, datum pristupa: 07.06.2020.

Ethereum zajednica je jedna od najvećih i najaktivnijih blockchain zajednica na svijetu. Okuplja programere temeljnih protokola, kripto ekonomske istraživače, razne organizacije za rudarenje, programere aplikacija, tvrtke, obične korisnike i dr.

Ne postoji tvrtka ili centralizirana organizacija koja kontrolira sustav. Ethereum održava i poboljšava globalna zajednica suradnika koja radi na svemu, od temeljnih protokola do potrošačkih aplikacija.

Jedna od stvari koje je Ethereum uveo su "pametni ugovori". Radi se o računalnom programu koji služi da olakša razmjenu vrijednosti, bilo da se radi o novcu, nekretnini, nekakvom sadržaju ili datoteci. Taj se program samostalno izvršava unutar blockchain mreže kada su zadovoljeni određeni preduvjeti. Ovakav program je imun na izmjene, nisu moguće nikakve promjene kao što je cenzuriranje, malverzacija ili bilo kakav utjecaj treće strane. Dok je većina blockchain mreža na neki način limitirana, Ethereum je otvoren i dopušta korištenje bilo kojih operacija. Ovo dopušta programerima da iskoriste sve mogućnosti ove tehnologije, van dosadašnjih postavljenih limita.

Ethereum je prvi blockchain sustav koji je uključio virtualno računalo (EVM) u svoj sustav. Ova inovacija omogućuje izvršavanja svih aplikacija u mreži. Omogućuje programerima da kreiraju aplikaciju i stave ju na mrežu. Ovakvo rješenje znatno ubrzava i olakšava cjelokupan proces jer nije potrebno kreirati novi blockchain za svaku pojedinu aplikaciju kao do sada.

Ethereum je decentraliziran. Većina sustava rađena je na centraliziranom pristupu, postoji središnje mjesto pod kontrolom jedne strane (banka, država, poduzeće...) i odavde se upravlja svime. Najveći nedostatak ovakvih sustava je tzv. SPOF (*Single Point Of Failure*). Dovoljan je hakerski napad na centralni dio ili nestanak struje i cijeli sustav pada. Postoji i opasnost od krađe podataka. Većina društvenih mreža i sličnih mrežnih server traži od korisnika ustupanje određenih podataka, koji se zatim pohranjuju. Krađa od strane hakera, same kompanije ili radnika predstavlja opasnost koja se ne smije zanemariti.

Decentralizacijom se postiže autonomnost i nema kontrole od strane pojedinca. Povećava se i sigurnost jer ne postoji SPOF, jer se cijeli sustav sastoji od nekoliko tisuća računala raspoređenih po cijelom svijetu. Osobni podaci ostaju na računalima korisnika a sav sadržaj

poput aplikacija, video i audio zapisa, ostaje pod potpunom kontrolom autora i ne postoje nametnuta ograničenja pružatelja usluga (npr. Youtube, App Store...).

Prednosti decentraliziranih aplikacija:

- integritet – nemoguće je manipulirati podacima od treće strane,
- konsenzus – aplikacije rade na principu konsenzusa, odluke su jednoglasne a cenzuru je nemoguće provoditi,
- sigurnost – ne postoji centralno mjesto upravljanja i izvođenja aplikacija, nema mogućnosti hakiranja,
- aplikacije uvijek aktivne i ne može postati nedostupna ili se ugasiti.

Najveći nedostatak decentraliziranih aplikacija je ljudska greška. Aplikacija je onoliko dobra koliko je dobar programer koji ju je napisao. Greške u izvornom kodu i propusti programera mogu dovesti do grešaka u radu ili akcija koje nisu predviđene i zamišljene. Zbog nepostojanja centralnog mjesta upravljanja, gotovo je nemoguće "popraviti" grešku u aplikaciji. Zbog principa na kojem radi blockchain, za ispravljanje takve greške potreban je konsenzus svih uključenih u mrežu.

8. ISTRAŽIVANJE

Istraživanje je provedeno u obliku ankete. Anketiranje je provedeno na način da je e-mail sa anketom poslan na 20 zaposlenika različitih tvrtki s područja Varaždinske županije. Radi se o osobama zaposlenim na različitim radnim mjestima - osnivači tvrtke, članovi uprave, administracija, računovodstvo, skladište i prodavači.

Anketom su obuhvaćene ove tvrtke:

- Univerzal d.o.o. Varaždin, Bershka, Metalska industrija Varaždin, Općinski sud u Varaždinu, Marlex, OTP d.d., Global Invest d.o.o., KTC d.d., Varkom d.d., Wollsdorf components, HGSpot informatika d.o.o., Plodine d.d., Grad Varaždin, JU Gradski stanovi, Koka d.o.o., Vindija d.d., Gumiimpex-grp d.o.o., Tisak plus d.o.o., Izvor osiguranje d.d., Varteks d.d..

Anketa se sastoji od 10 pitanja:

- Molim Vas navedite naziv tvrtke u kojoj radite.
- Postoji li u tvrtki gdje radite, služba zadužena za zaštitu podataka?
- Ima li tvrtka u kojoj radite ima pravilnik ili proceduru o zaštiti poslovnih podataka?
- Jeste li upoznati s informacijskom sigurnošću i zaštitom podataka (obuka, tečaj ili seminar organiziran od strane Vašeg poslodavca)?
- Znate li koje su Vaše odgovornosti prema podacima u vlasništvu Vašeg poslodavca?
- Trebate li pristupnu šifru da bi pristupili podacima na računalu u tvrtki gdje radite?
- Vodi li Vaš poslodavac evidenciju posjetitelja, odnosno osoba koje ulaze u prostore tvrtke a nisu zaposlenici?
- Koristite li poslovno računalo za privatne svrhe (pristup društvenim mrežama, pregledavanje portala, pristup privatnom mailu...)?
- Koliko je staro računalo na kojem radite?
- Primate li na poslovni e-mail neželjenu poštu (spam, reklame, mailove nepoznatih pošiljatelja...)?
- Je li tvrtka u kojoj radite ikad pretrpjela hakerski napad, krađu ili gubitak podataka?

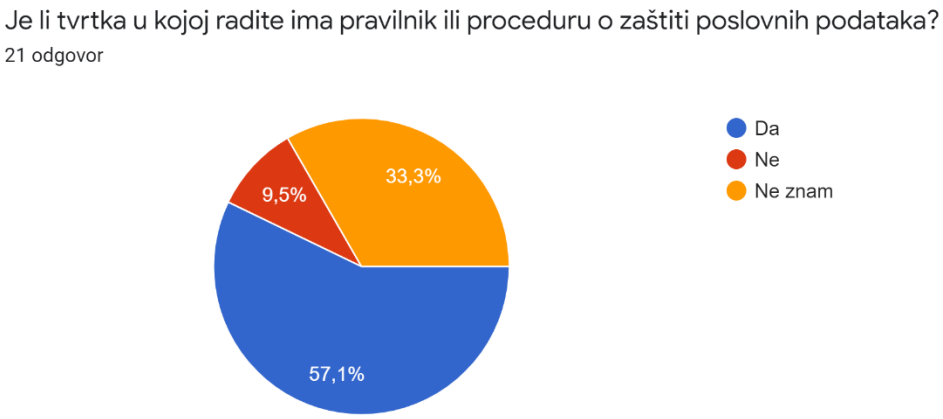
ANALIZA ANKETE

U nastavku rada, provedena je analiza za svako pitanje zasebno. Na temelju dobivenih odgovora izvučeni su zaključci koji su dodatno prokomentirani.

Graf 1 – Anketno pitanje br. 1

Izvor : izradio autor

Na ovo pitanje je 70% anketiranih dalo odgovor da postoji služba zadužena za zaštitu podataka u tvrtki gdje rade. Njih 20% dalo je odgovor da nemaju takvu službu, dok je 10% odgovorili da ne zna. Ovo pokazuje da je većina poslodavaca shvatila važnost zaštite podataka i postupa po Općoj uredbi za zaštitu podataka.



Graf 2 – Anketno pitanje br. 2

Izvor : izradio autor

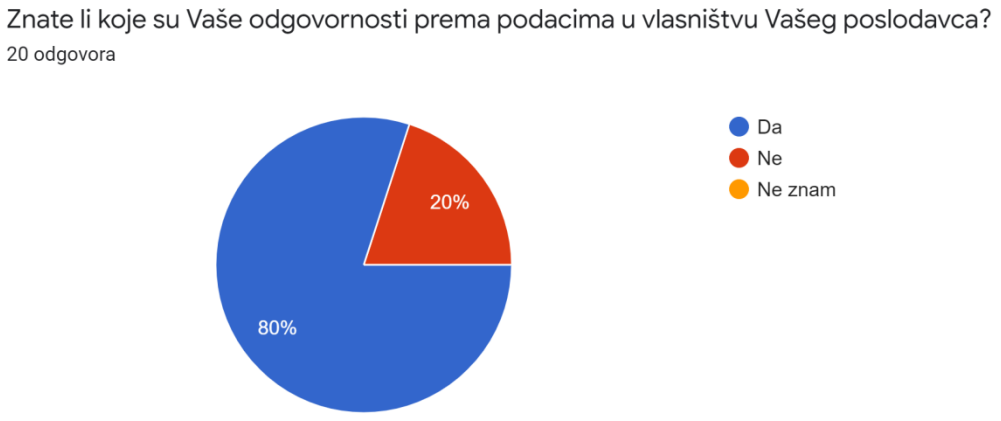
Na ovo pitanje je 55% anketiranih odgovorilo da u tvrtki gdje rade postoji pravilnik ili procedura o zaštiti poslovnih podataka. Od ostalih anketiranih, 35% odgovorilo je da ne zna a 10% je odgovorilo da pravilnik ili proceduru nemaju. Ukupno 45% onih koji nemaju

proceduru ili pravilnik o zaštiti podataka je prevelik postotak i govori da ne vode dovoljno računa o zaštiti podataka.

Graf 3 – Anketno pitanje br. 3

Izvor : izradio autor

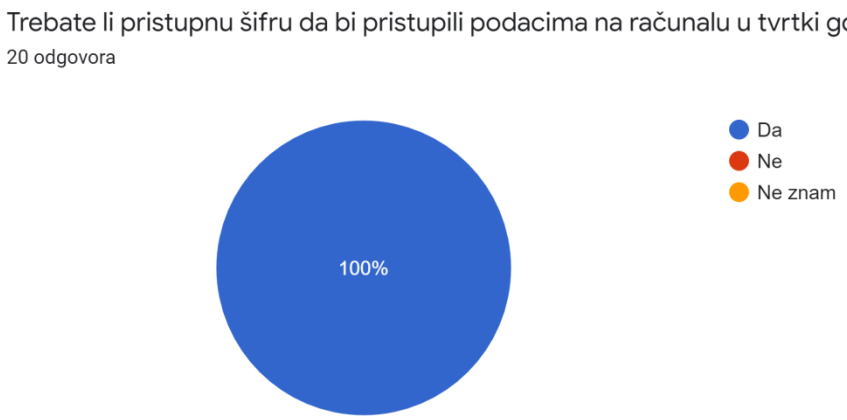
Iz odgovora na ovo pitanje vidljivo je da je 60% zaposlenika upoznato s informacijskom sigurnošću i zaštitom podataka, dok 40% nije upoznato. Slično kao i kod prethodnog pitanja, vidljivo je da poslodavci ne vode dovoljno računa o zaštiti podataka, odnosno o informiranju i obuci svojih zaposlenika.



Graf 4 – Anketno pitanje br. 4

Izvor : Izradio autor

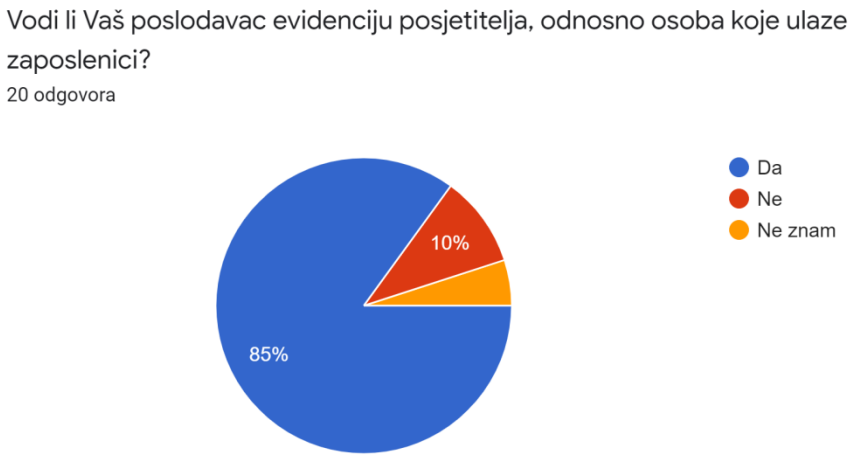
Ovdje se može zaključiti da zaposlenici znaju koje su njihove odgovornosti prema podacima poslodavca. Ukupno 80% je odgovorilo potvrdno, a 20% je odgovorilo negativno.



Graf 5 – Anketno pitanje br. 5

Izvor : Izradio autor

Na ovo pitanje je svih 100% anketiranih odgovorilo potvrdno - ispitanici trebaju pristupnu šifru za pristup podacima na računalu u tvrtki gdje rade. Zaključuje se da svi poslodavci provode barem osnovne mjere zaštite od neovlaštenog korištenja računala i podataka.

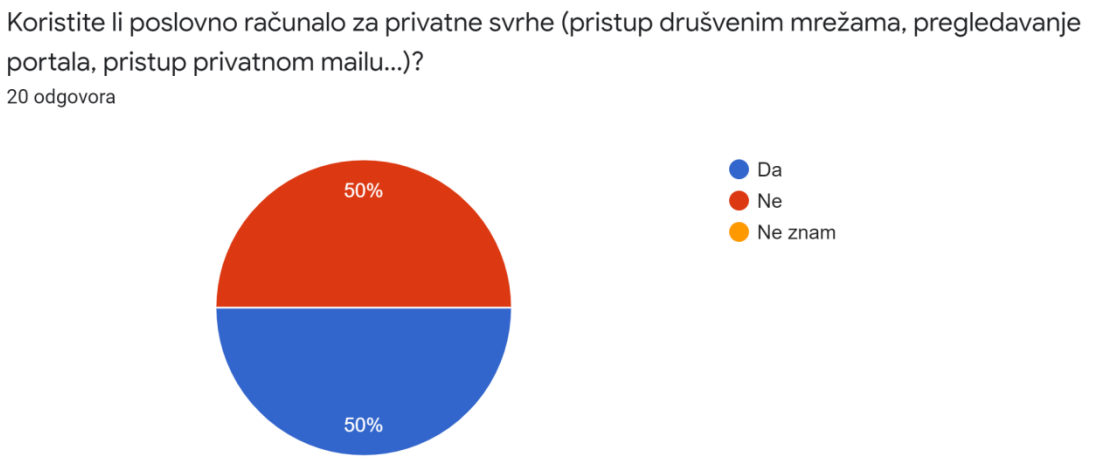


Graf 6 – Anketno pitanje br. 6

Izvor : Izradio autor

Na pitanje vodi li poslodavac evidenciju posjetitelja, odnosno osoba koje ulaze u prostore tvrtke a nisu zaposlenici, 85% anketiranih je odgovorilo da takva evidencija postoji, 10% da ne postoji, a 5% da ne zna.

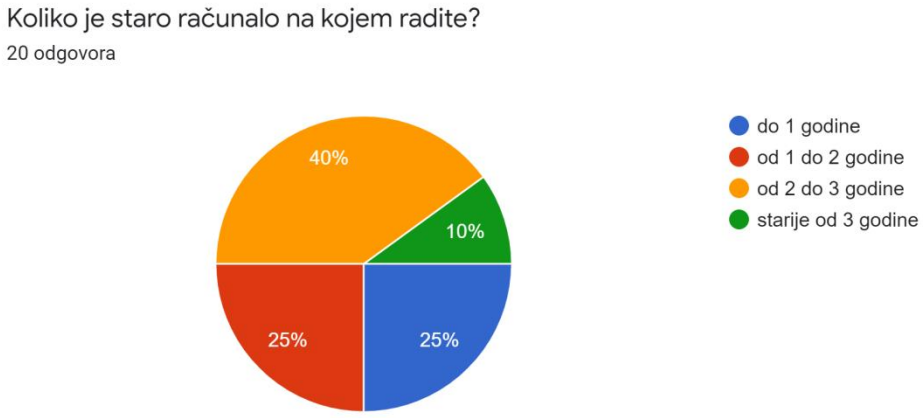
Zaključak je da većina poslodavaca vodi evidenciju posjetitelja i na taj način vrše kontrolu ulazaka.



Graf 7 – Anketno pitanje br. 7

Izvor : Izradio autor

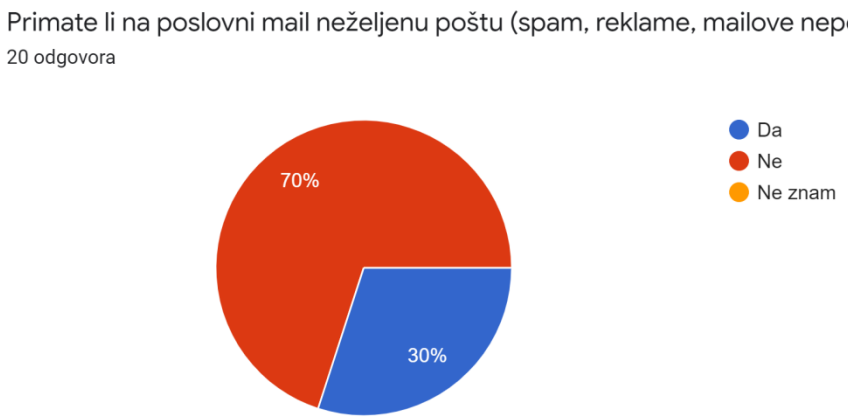
Iz odgovora na ovo pitanje vidljivo je da čak 50% anketiranih koristi poslovno računalo za privatne svrhe (pristup društvenim mrežama, pregledavanje portala, pristup privatnom mailu...). Ovaj je podatak zabrinjavajući jer pokazuje nedovoljnu osviještenost zaposlenih o opasnostima pristupa neprovjerenim internetskim izvorima. Na ovaj se način direktno ugrožava informacijska sigurnost. Radi se i o propustu poslodavca, koji raznim programskim rješenjima može ograničiti pristup svim internetskim izvorima za koje smatra da nisu nužni za rad.



Graf 8 – Anketno pitanje br. 8

Izvor : Izradio autor

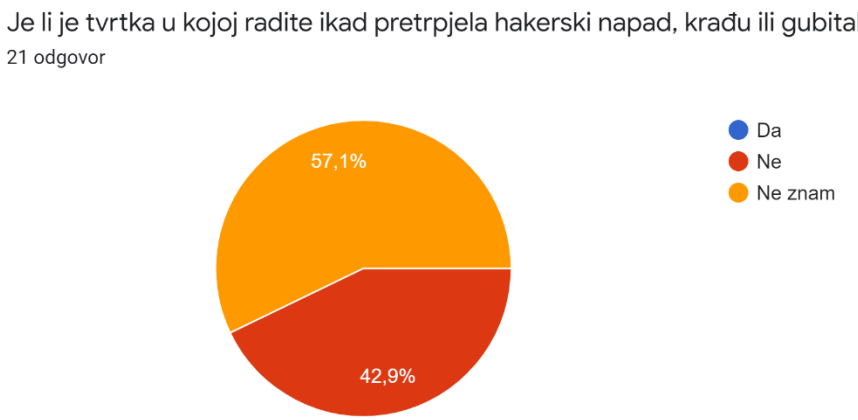
Na ovo pitanje je 25% anketiranih odgovorilo da rade na računalu starosti do godinu dana, 25% na računalu starosti od 1 do 2 godine, 40% na računalo starosti od 2 do 3 godine, a 10% radi na računalu starijem od 3 godine. Može se zaključiti da većina poslodavaca ulaže u informatičku opremu i koriste računala novije generacije.



Graf 9 – Anketno pitanje br. 9

Izvor : Izradio autor

Na ovo pitanje je 70% anketiranih odgovorilo da na poslovni mail primaju neželjenu poštu, dok je 30% odgovorilo da ne prima. Može se zaključiti da poslodavci koriste određenu programsku zaštitu (filtere) od spam pošte i na taj način djelomično štite podatke.



Graf 10 – Anketno pitanje br. 10

Izvor : Izradio autor

Na pitanje je li tvrtka u kojoj radite pretrpjela hakerski napad, krađu ili gubitak podataka, 45% anketiranih je odgovorilo da nije, a 55% je odgovorilo da ne zna. Iako je ovo zadovoljavajući rezultat, može se doći do nekoliko zaključaka. Budući da je visok postotak odgovora „ne znam“, postoji mogućnost da poslodavac skriva da je došlo do neovlaštenog upada u informacijski sustav i krađe podataka. Postoji mogućnost da takvih napad nije ni bilo, a zaposlenici to ne znaju. Moguće je i da te tvrtke, iako možda nisu zaštićene, jednostavno nisu zanimljive mete. Kako bi se došlo do ispravnog zaključka, potrebne su dodatne informacije i analiza.

Molim Vas navedite naziv tvrtke u kojoj radite.	Postoji li u tvrtki gdje radite, služba zadužena za zaštitu podataka?	Je li tvrtka u kojoj radite ima pravilnik ili proceduru o zaštiti poslovnih podataka?	Jeste li ste upoznati sa informacijskom sigurnošću i zaštitom podataka (obuka, tečaj ili seminar organiziran od strane Vašeg poslodavca)?	Znate li koje su Vaše odgovornosti prema podacima u vlasništvu Vašeg poslodavca?	Trebate li pristupnu šifru da bi pristupili podacima na računalu u tvrtki gdje radite?
Univerzal d.d.o. Varaždin	Ne	Ne	Ne	Ne	Da
Bershka	Da	Da	Da	Da	Da
Metalska industrija Varaždin	Da	Da	Da	Da	Da
Općinski sud u Varaždinu	Da	Da	Da	Da	Da
Marlex	Ne	Ne	Ne	Da	Da
OTP d.d.	Da	Da	Da	Da	Da
Global Invest d.o.o.	Da	Da	Da	Da	Da
KTC d.d.	Ne znam	Ne znam	Ne	Ne	Da
Varkom d.d.	Da	Da	Da	Da	Da
Wollsdorf components	Da	Ne znam	Ne	Da	Da
HGSpot informatika d.o.o.	Da	Da	Da	Da	Da
Plodine d.d.	Da	Ne znam	Ne	Ne	Da
Grad Varaždin	Ne	Da	Ne	Da	Da
JU Gradski stanovi	Ne	Ne znam	Ne	Da	Da
Koka d.o.o.	Da	Ne znam	Da	Da	Da
Vindija d.d.	Da	Da	Da	Da	Da
Gumimpex-grp d.o.o.	Da	Da	Da	Da	Da
Tisak plus d.o.o.	Ne znam	Ne znam	Da	Da	Da
Izvor osiguranje d.d.	Da	Da	Da	Da	Da
Varteks d.d.	Da	Ne znam	Ne	Ne	Da

Moli Vas navedite naziv tvrtke u kojoj radite.	Vodi li Vaš poslodavac evidenciju posjetitelja, odnosno osoba koje ulaze u prostore tvrtke a nisu zaposlenici?	Koristite li poslovno računalo za privatne svrhe (pristup društvenim mrežama, pregledavanje portala, pristup privatnom mailu...)?	Koliko je staro računalo na kojem radite?	Primate li na poslovni mail neželjenu poštu (spam, reklame, mailove nepoznatih pošiljatelja...)?	Je li je tvrtka u kojoj radite ikad pretrpjela hakerski napad, krađu ili gubitak podataka?
Univerzal d.d.o. Varaždin	Da	Da	od 2 do 3 godine	Da	Ne znam
Bershka	Da	Ne	od 1 do 2 godine	Ne	Ne
Metalska industrija Varaždin	Da	Da	od 2 do 3 godine	Ne	Ne znam
Općinski sud u Varaždinu	Da	Da	od 1 do 2 godine	Ne	Ne
Marlex	Ne	Da	od 1 do 2 godine	Da	Ne
OTP d.d.	Da	Ne	do 1 godine	Ne	Ne znam
Global Invest d.o.o.	Da	Ne	do 1 godine	Da	Ne
KTC d.d.	Da	Ne	od 2 do 3 godine	Ne	Ne
Varkom d.d.	Da	Ne	do 1 godine	Ne	Ne znam
Wollsdorf components	Da	Ne	starije od 3 godine	Ne	Ne
HGSpot informatika d.o.o.	Da	Ne	do 1 godine	Ne	Ne
Plodine d.d.	Da	Da	od 2 do 3 godine	Da	Ne znam
Grad Varaždin	Ne	Da	do 1 godine	Da	Ne
JU Gradski stanovi	Ne znam	Da	starije od 3 godine	Ne	Ne znam
Koka d.o.o.	Da	Da	od 2 do 3 godine	Ne	Ne znam
Vindija d.d.	Da	Ne	od 1 do 2 godine	Ne	Ne znam
Gumimpex-grp d.o.o.	Da	Ne	od 2 do 3 godine	Ne	Ne znam
Tisak plus d.o.o.	Da	Ne	od 2 do 3 godine	Ne	Ne znam
Izvor osiguranje d.d.	Da	Da	od 1 do 2 godine	Ne	Ne
Varteks d.d.	Da	Da	od 2 do 3 godine	Da	Ne znam

Tablica 2 - Pregled odgovora po ispitanicima

Izvor : Izradio autor

Manji broj anketiranih tvrtki je uzrokovan činjenicom kako se još uvijek nedovoljno tvrtki sustavno bavi organizacijom i planiranjem informacijske sigurnosti u zaštiti podataka.

Zaključak

Iz provedene ankete može se zaključiti kako je razina provođenja informacijske sigurnosti u tvrtkama anketiranih prilično niska. Provode se osnovne zaštite podataka poput korištenja pristupnih šifri za računala i evidencije posjetitelja. Uvođenje procedura i pravilnika o informacijskoj zaštiti, kao i ulaganje u edukaciju zaposlenih, nešto je što bi poslodavci trebali provoditi. Iz svega navedenog dolazi se do zaključka da se provodi samo osnovna zaštita, koju je potrebno podići na višu razinu.

9. ZAKLJUČAK

Blockchain tehnologija je visoko cijenjena zbog svoje decentralizirane i peer-to-peer strukture. Međutim, blockchain je uvelike zasjenjen i stavljen u drugi plan upravo zbog svoje prvotne svrhe – kripto valuta. Većina pažnje fokusirana je na Bitcoin, a ne na tehnologiji koja ga pokreće. Međutim, to se sve više mijenja i sve je jasnije da je blockchain tehnologija probila granice svoje prvotne namjene.

Zaštita podataka koja je imperativ u današnje digitalno doba, pokazalo se kao područje gdje se blockchain tehnologija može i hoće dokazati. Decentralizacija, kriptografski protokoli, struktura otporna na vanjske utjecaje, samo su neke od ključnih osobina koje izdvajaju blockchain od ostalih. Način zapisivanja podataka u blokove i povezivanje tih blokova u lanac, te nemogućnost mijenjanja podataka bez da se mijenja cijeli lanac, daje stupanj sigurnosti koji je teško nadmašiti. Anonimnost je još jedna prednost. Prilikom provođenja transakcija ili razmjene podataka preko blockchain mreže, korisnik ostaje anoniman jer se sve verificira putem javnih i privatnih kriptografskih ključeva.

Ethereum je jedan od primjera širokog područja korištenja blockchain tehnologije. Radi se o otvorenoj platformi koja je bazirana na blockchain-u i omogućava razvoj aplikacija široke namjene. Ethereum je programibilan i omogućuje rad decentraliziranih aplikacija.

Blockchain omogućuje provođenje „pametnih ugovora“. Radi se o računalnim programima koji služe za primjerice razmjenu vrijednosti, a provode se samostalno, kada su izvršeni određeni preduvjeti.

Uz sve navedene prednosti, blockchain nije savršen. Problemi poput veličine samog blockchain-a i ograničen broj transakcija u sekundi, neki su od problema koje treba riješiti.

Blockchain je besplatan, omogućava provođenje transakcija bez naknade i isključuje treću stranu koja je u ulozi posrednika koji provodi transakcije. Upravo ova prednost je ujedno i mana koja koči širu primjenu na području financija. Kada bi financijske ustanove kao što su banke prihvatile blockchain, morale bi prihvatiti činjenicu da više nisu zadužene za provođenje transakcija, a samim time više nemaju mogućnost naplaćivanja naknade i ostaju bez velikog dijela zarade.

Vitalik Buterin, jedan od suosnivača Ethereuma, izjavio je u jednom od intervjua da „*glavna prednost blockchain tehnologije je pretpostavka da je sigurnija, ali ljudima je općenito teško vjerovati u novu tehnologiju i to je paradoks koji je teško izbjeći.*“ Radi se o tehnologiji velikog potencijala, ali za sada puni potencijal ostaje neiskorišten. Blockchain je tehnologija koja tek treba pokazati svu svoju snagu i predviđanja su da će se to dogoditi u skoro vrijeme. Tehnologija koja pokreće Bitcoin je za sada u sjeni ali razvoj tehnologije i interneta postavlja izazove na koje blockchain ima odgovore i može se zaključiti da vrijeme vladavine blockchain-a kao vodeće tehnologije zaštite podataka tek dolazi.

10. IZVORI:

1. A.M.Antonpoulous. (2010). *Unlocking digital crypto-currencies*.
2. A.Barentsen, F.Schär. (2018). *A Short Introduction to the World of Cryptocurrencies*, Federal Reserve Bank
3. Androutsellis-Theotokis, S., Spinellis, D. (2004) „*A Survey of Peer-to-Peer Content Distribution Technologies*“, ACM Computing Surveys
4. Balaić, M. (2018.), *Aspekti zaštite autentičnosti i privatnosti digitalnih podataka u blockchain modelu*, Osijek 2018., Sveučilište J.J.Strosmayera u Osijeku
5. *Blockchain Architecture Basics: Components, Structure, Benefits & Creation*, (2019), https://medium.com/@MLSDevCom/blockchain-architecture-basics-components-structure-benefits-creation-beace17c8e77, datum pristupa: 22.04.2020.
6. Blockchain info, https://blockchain.info/charts (15. 2. 2015.)
7. Bogati, J., *Norme informacijske sigurnosti ISO/IEC 27K*, Ministarstvo obrane RH, Odsjek za poslove obrane Virovitica, Praktični menadžment, Vol.II, br.3, str. 112-117
8. Buterin, V. (2014) *A Next-Generation Smart Contract and Decentralized Application Platform*, White Paper, Buterin, V. (2015) On Public and Private Blockchains,
9. Corcoran, J. (2014) *Russia Seeks Fines for Using Virtual Money Like Bitcoins*, http://www.bloomberg.com/news/articles/2014-10-03/russia-seeks-fines-for-using-virtual-money-like-bitcoins (10. 2. 2020.)
10. Crypto-Currency Market Capitalizations, http://coinmarketcap.com/all/ (13. 2. 2015.)
11. Dougherty, C. (2015) *Forget Everything You Didn't Understand About Bitcoin*, http://www.bloomberg.com/news/articles/2015-01-15/bitcoin-may-succeed-as-software-not-medium-of-exchange, (08.01.2020.)
12. Frankenfield J., *B-money* (2019), https://www.investopedia.com/terms/b/bmoney.asp, datum pristupa: 20.03.2020.
13. *GDPR i osobni podaci* (2018), GDPRinformer, https://gdprinformer.com/hr/gdpr-clanci/gdpr-osobni-podaci, datum pristupa: 15.03.2020.
14. *GDPR – osnovni pojmovi* (2017), http://www.hrportal.com.hr/hr/gdpr/, datum pristupa: 15.03.2020.
15. Glowacki J., (2018), *Blockchain: Public, Private or Hybrid?*, https://medium.com/@jackglowacki/blockchain-public-private-or-hybrid-664d4a413331, datum pristupa: 20.05.2020.
16. Gregurić V., Hajdinjak N., Jakšić M., Počuča B., Rakić D., Svetličić S., Šokac D., Vlajinić D. (2019), *Informatika 5 – udžbenik u petom razredu osnovne škole*, Zagreb:

Profil Klett d.o.o., modul: Informacije i digitalna tehnologija, jedinica: Kako radi računalo, odlomak: Binarni sustav

17. *Hrvatska enciklopedija, mrežno izdanje,* Leksikografski zavod Miroslav Krleža, 2020., raspoloživo na: http://www.enciklopedija.hr/Natuknica.aspx?ID=33988, datum pristupa: 31. 5. 2020.
18. IBM (2015) IBM ADEPT *Practictioner Perspective – Pre Publication Draft*. IBM (2016) *IBM Blockchain*, http://www.ibm.com/blockchain/ (15.02.2020.)
19. ISO 27001:2013

Jaag, C., Bach, C. et al. (2016) *Blockchain Technology and Cryptocurrencies: Opportunities for Postal Financial Services, Technical Report*

20. J.Herrera, *Research and Challenges on Bitcoin Anonymity*. (2004). Autonomous University of Barcelona
21. Kazneni zakon (NN 125/11, 144/12, 56/15, 61/15, 101/17, 118/18, 126/19)
22. Klaić B., *Rječnik stranih riječi*, Nakladni zavod MH Zagreb, 1988. god.
23. Javorović B., Bilandžić M. (2007), *Poslovne informacije i business intelligence*, Zagreb: Golden marketing – Tehnička knjiga, str. 32-33
24. Merriam-Webster dictionary (2020), Dictionary, raspoloživo na: www.merriam-webster.com/dictionary/information, datum pristupa sadržaju: 11.02.2020. M.Swan, *Blockchain – Blueprint for a New Economy*. (2015). United States of America.
25. Nakamoto, S. (2008) *Bitcoin: A Peer-to-Peer Electronic Cash System*, https://bitcoin.org/bitcoin.pdf (18.01.2020.)

Naskar A., (2020), *The Gospel of Technology*

26. Noyes, C. (2016a) *Bitav: Fast Anti-Malware by Distributed Blockchain Consensus and Feedforward Scanning*

27. Noyes, C. (2016b) *Efficient Blockchain-Driven Multiparty Computation Markets at Scale, Technical Report*

28. Pratap M., (2018), *Blockchain Technology Explained: Introduction, Meanina, and Applications*, https://hackernoon.com/blockchain-technology-explained-introduction-meaning-and-applications-edbd6759a2b2, datum pristupa: 01.05.2020.
29. *Sigurnosna politika* (2009), CARNet – Hrvatska akademska istraživačka mreža, CCERT-PUBDOC-2009-05-265
30. Thomas R., *The ABCs of bitcoin And a look at its investment potential*. (2017). Wilmington Trust Corporation.

31. *Use Ethereum Applications* (2020), https://ethereum.org/en/dapps/, datum pristupa: 07.06.2020.
32. Strategija nacionalne sigurnosti (NN 73/17)
33. Uredba o mjerama informacijske sigurnosti (NN 46/2008)
34. Varga M. (2014), *Upravljanje podacima*, Zagreb: Element d.o.o., str. 2
35. *What is Blockchain Technology? A Step-by-Step Guide For Beginners* (2015), raspoloživo na: https://blockgeeks.com/guides/what-is-blockchain-technology/, datum pristupa sadržaju: 02.03.2020.
36. *What Is SHA-256 And How Is It Related to Bitcoin?*, (2018), https://www.mycryptopedia.com/sha-256-related-bitcoin/, datum pristupa: 21.04.2020.
37. Zakonu o arhivskom gradivu i arhivima (NN 61/18, 98/19)
38. Zakon o informacijskoj sigurnosti (NN 79/07)
39. Zako o provedbi Opće uredbe o zaštiti podataka (NN 42/2018)
40. Zakon o sigurnosno-obavještajnom sustavu RH (NN 79/06, 105/06)
41. Zakon o tajnosti podataka, NN 79/07, 86/12
42. Zakon o zaštiti tajnosti podataka (NN 108/96)
43. Zyskind, G., Nathan, O. et al. (2015) '*Decentralizing privacy: Using Blockchain to protect personal data, Secirity and Privacy Workshops* (SPW), 2015 IEEE, IEEE, pp. 180–184.
44. Živković, S. (2018.), *Blockchain tehnologija*, završni rad, Rijeka 2018, Sveučilište u Rijeci
45. http://www2.hgk.hr/
46. https://www.uvns.hr/
47. https://azop.hr
48. https://www.gdpr-2018.hr/
49. https://gdprinformer.com/
50. https://www.rozp.hr/
51. https://www.zakon.hr/

11. POPIS SLIKA, TABLICA I GRAFOVA

12. PRILOZI

Anketa:

1. **Postoji li u tvrtki gdje radite, služba zadužena za zaštitu podataka?**
    - Da
    - Ne
    - Ne znam

2. **Je li tvrtka u kojoj radite ima pravilnik ili proceduru o zaštiti poslovnih podataka?**
    - Da
    - Ne
    - Ne znam

3. **Jeste li upoznati sa informacijskom sigurnošću i zaštitom podataka (obuka, tečaj ili seminar organiziran od strane Vašeg poslodavca)?**
    - Da
    - Ne
    - Ne znam

4. **Znate li koje su Vaše odgovornosti prema podacima u vlasništvu Vašeg poslodavca?**
    - Da
    - Ne
    - Ne znam

5. **Trebate li pristupnu šifru da bi pristupili podacima na računalu u tvrtki gdje radite?**
    - Da
    - Ne
    - Ne znam

6. **Vodi li Vaš poslodavac evidenciju posjetitelja, odnosno osoba koje ulaze u prostore tvrtke a nisu zaposlenici?**
    - Da
    - Ne
    - Ne znam

7. **Koristite li poslovno računalo za privatne svrhe (pristup društvenim mrežama, pregledavanje portala, pristup privatnom mailu…)?**
    - Da
    - Ne
    - Ne znam

8. **Koliko je staro računalo na kojem radite?**
    - Do 1 godine
    - Od 1 d 2 godine
    - Od 2 do 3 godine
    - Starije od 3 godine

9. **Primate li na poslovni mail neželjenu poštu (spam, reklame, mailove nepoznatih pošiljatelja…)?**
    - Da
    - Ne
    - Ne znam

10. **Je li tvrtka u kojoj radite ikad pretrpjela hakerski napad, krađu ili gubitak podataka?**
    - Da
    - Ne
    - Ne znam

Sveučilište
Sjever

IZJAVA O AUTORSTVU
I
SUGLASNOST ZA JAVNU OBJAVU

Završni/diplomski rad isključivo je autorsko djelo studenta koji je isti izradio te student odgovara za istinitost, izvornost i ispravnost teksta rada. U radu se ne smiju koristiti dijelovi tuđih radova (knjiga, članaka, doktorskih disertacija, magistarskih radova, izvora s interneta, i drugih izvora) bez navođenja izvora i autora navedenih radova. Svi dijelovi tuđih radova moraju biti pravilno navedeni i citirani. Dijelovi tuđih radova koji nisu pravilno citirani, smatraju se plagijatom, odnosno nezakonitim prisvajanjem tuđeg znanstvenog ili stručnoga rada. Sukladno navedenom studenti su dužni potpisati izjavu o autorstvu rada.

Ja, MARKO VLAHOVIĆ *(ime i prezime)* pod punom moralnom, materijalnom i kaznenom odgovornošću, izjavljujem da sam isključivi autor/ica završnog/diplomskog (*obrisati nepotrebno*) rada pod naslovom BLOCKCHAIN - NOVA TEHNOLOGIJA ZAŠTITE PODATAKA *(upisati naslov)* te da u navedenom radu nisu na nedozvoljeni način (bez pravilnog citiranja) korišteni dijelovi tuđih radova.

Student/ica:
(upisati ime i prezime)

(vlastoručni potpis)

Sukladno Zakonu o znanstvenoj djelatnost i visokom obrazovanju završne/diplomske radove sveučilišta su dužna trajno objaviti na javnoj internetskoj bazi sveučilišne knjižnice u sastavu sveučilišta te kopirati u javnu internetsku bazu završnih/diplomskih radova Nacionalne i sveučilišne knjižnice. Završni radovi istovrsnih umjetničkih studija koji se realiziraju kroz umjetnička ostvarenja objavljuju se na odgovarajući način.

Ja, MARKO VLAHOVIĆ *(ime i prezime)* neopozivo izjavljujem da sam suglasan/na s javnom objavom završnog/diplomskog (*obrisati nepotrebno*) rada pod naslovom BLOCKCHAIN - NOVA TEHNOLOGIJA ZAŠTITE PODATAKA *(upisati naslov)* čiji sam autor/ica.

Student/ica:
(upisati ime i prezime)

(vlastoručni potpis)