Univerzitet Donja Gorica

Fakultet za informacione sisteme i tehnologije

Podgorica

Blockchain tehnologija i njen uticaj na sigurnost podataka

DIPLOMSKI RAD

Student: Mark Camaj

Broj dosijea: 20/040

Podgorica, sep 2023.godine

Univerzitet Donja Gorica

Fakultet za informacione sisteme i tehnologije

Podgorica

Blockchain tehnologija i njen uticaj na sigurnost podataka

DIPLOMSKI RAD

Mentor: prof. dr Armin Alibašić

Student: Mark Camaj

Broj dosijea: 20/040

Podgorica, sep 2023.godine

APSTRAKT

Sposobnost blokčejna, koji je prvi put upotrijebljen 2009. godine, da garantuje sigurnost, integritet i anonimnost podataka bez potrebe da treća strana bude angažovana u transakcijama ili ugovorima, izaziva stalno interesovanje.

Sadržaj ovog rada ima za cilj da istraži kako bi blokčejn tehnologija mogla da revolucioniše bezbjednost podataka u nizu sektora i disciplina.

Govorit ćemo o značaju bezbjednosti podataka u trenutnom digitalnom okruženju, naglašavajući nedostatke i poteškoće sa kojima se suočavaju stari centralizovani sistemi. Ovo će naglasiti potrebu za pouzdanijim i decentralizovanijim pristupom blockchain tehnologiji zaštiti podataka. Blockchain ima mogućnost da u potpunosti promjeni procedure bezbjednosti podataka zahvaljujući tehnologiji distribuirane knjige, metodama šifrovanja i algoritmima konsenzusa.

U radu će se razmatrati praktična upotreba blokčejna za poboljšanje bezbjednosti podataka, uključujući bezbjedno djeljenje podataka i upravljanje pristupom, kao i smanjenje prevara i kršenja podataka.

Skalabilnost, potrošnja energije i regulatorna pitanja će se istražiti kao potencijalna ograničenja i poteškoće u korišćenju blokčejn tehnologije.

Ovaj rad isto tako ima za cilj da ponudi koristan uvid u održivost i prepreke u vezi sa implementacijom blockchain tehnologije iz razloga bezbjednosti podataka kroz dubinski pregled relevantne literature, studija slučaja i empirijskih istraživanja. Rezultati svega ovoga će nam pomoći da steknemo temeljna znanja o tome kako tehnologija blokčejn može da zaštiti osjetljive podatke i očuva integritet podataka, otvarajući vrata za njenu širu primjenu u različitim industrijama.

Ključne riječi: Blockchain tehnologija, bezbjednost podataka, decentralizovani sistemi, distribuirana knjiga, kriptografske tehnike, konsenzus algoritmi, djeljenje podataka, kontrola pristupa, kršenje podataka, prevara, skalabilnost, potrošnja energije, regulatorna razmatranja.

ABSTRACT

The capability of blockchain, which was first used in 2009, to guarantee security, integrity, and anonymity of data without the need for a third party to be engaged in transactions or contracts, has drawn ongoing interest.

The subject of this paper intends to explore how blockchain technology could revolutionise data security across a range of sectors and disciplines.

We will discuss the significance of data security in the current digital environment, emphasising the flaws and difficulties that old centralised systems confront. This will emphasise the necessity for blockchain technology's more reliable and decentralised approach to data protection. Blockchain has the ability to completely change data security procedures thanks to distributed ledger technology, encryption methods, and consensus algorithms.

The paper will discuss practical uses of blockchain to improve data security, including safe and secure data sharing and access management, as well as reducing fraud and data breaches. Scalability, energy usage and regulatory issues will be explored as potential limitations and difficulties in using blockchain technology.

This thesis aims to offer a useful insight into the sustainability and obstacles related to the implementation of blockchain technology for data security reasons through an in-depth review of relevant literature, case studies and empirical research. The results of this study will help us gain fundamental knowledge of how blockchain technology can protect sensitive data and maintain data integrity, opening the door for its wider application in various industries.

Keywords: Blockchain technology, data security, decentralized systems, distributed ledger, cryptographic techniques, consensus algorithms, data sharing, access control, data breach, fraud, scalability, energy consumption, regulatory considerations.

SADRŽAJ

APSTRAKT 3

ABSTRACT 4

1. UVOD 7

1.1. Ideja rada i cilj rada 7

1.2. Očekivanje od rada 7

1.3. Tema u okviru mreže međuzavisnosti 8

2. BLOCKCHAIN TEHNOLOGIJA 9

2.1. Što je "BLOCKCHAIN"? 9

2.2 Historija Blockchain-a 10

2.3. Kako funkcioniše Blockchain? 12

2.3.1 Vizuelni prikaz blokčejna 13

2. 4. Radni postupak Blockchaina 14

2. 4. 1. Transparentnost i sigurnost 14

2.5. Zašto je Blockchain potreban? 15

2.5. Prednosti blockchain tehnologije 17

2.6. Prednosti Blockchain-a u kontekstu bezbjednosti podataka 18

2.7. Nedostaci blockchain tehnologije 20

3. SIGURNOST PODATAKA 21

3.1 Sigurnost podataka kroz godine 23

3.2 Vrste kontrola bezbjednosti podataka 25

3.3 Razmatranja o bezbjednosti podataka: 27

3.4. Sigurnosne karakteristike blokčejna 29

4. ZAKLJUČAK 31

5. PRAKTIČNI RAD *32*

5.1 Webstranica BDS **32**

LITERATURA *34*

Izvori sa interneta: **37**

Lista slika i grafika: **37**

Simboli i skraćenice **37**

1. UVOD

1.1. Ideja rada i cilj rada

Tema ovog diplomskog rada je da upozna i da predstavi Blockchain tehnologiju i njen uticaj na sigurnost podataka.

U današnjem povezanom digitalnom svijetu, bezbjednost podataka se pojavila kao glavni prioritet za sve strane, uključujući pojedince, preduzeća i vlade. Potrebna su inovativna riješenja koja bi mogla da poboljšaju procedure bezbjednosti podataka zbog sveprisutnosti sajber prijetnji i sve većeg obima i osetljivosti podataka koji se generišu. Sa uvođenjem Bitcoin-a 2009. godine, blokčejn tehnologija je prvi put puštena u upotrebu. Od tada se pojavila kao remetilačka sila koja ima kapacitet da u potpunosti promjeni način na koji obezbjeđujemo i štitimo podatke.

Blockchain, tehnologija koja je decentralizovana i otporna na neovlašćene promjene, predstavlja održivu zamjenu za konvencionalne centralizovane sisteme, koji su skloni greškama. Blockchain nudi bezbjednu i otvorenu platformu za upravljanje i verifikaciju digitalnih transakcija i informacija korišćenjem tehnologije distribuirane knjige, kriptografskih metoda i konsenzus algoritama.

Cilj ovog diplomskog rada je da istraži dramatične efekte blockchain tehnologije na bezbjednost podataka i procjeni kako bi mogla da revolucioniše svijet informacionih sistema i tehnologije. Ovaj rad isto tako ima za cilj da rasvijetli prednosti, probleme i buduće izglede primjene blokčejn tehnologije za jačanje bezbjednosti podataka posmatranjem aplikacija iz stvarnog svijeta, ispitivanjem studija slučaja i opsežnim istraživanjem.

1.2. Očekivanje od rada

Istražićemo osnovne ideje blockchain tehnologije tokom ovog rada, uključujući njene vodeći principe, arhitekturu i djelove. Pogledaćemo kako decentralizovana i nepromjenljiva priroda blockchaina obezbjeđuje integritet podataka, povjerljivost i autentičnost. Takođe ćemo razmotriti nekoliko kriptografskih metoda koje se koriste u blokčejnu za zaštitu podataka od neovlašćenog pristupa i manipulacije. Pored toga, praktični efekti blockchain tehnologije na bezbjednost podataka u nekoliko preduzeća i domena biće istraženi u ovom diplomskom radu. Pogledaćemo kako blokčejn promoviše povjerenje u digitalne ekosisteme omogućavajući bezbjedno i zaštićeno čuvanje zapisa, poboljšavajući djeljenje podataka i upravljanje pristupom, smanjujući opasnost od kršenja podataka i prevare i još mnogo toga.

1.3. Tema u okviru mreže međuzavisnosti

Pojam mreža međuzavisnosti postao je ključan u današnjem digitalnom dobu, oblikujući naš profesionalni i lični život. Ta mreža se sastoji od veza između nekoliko različitih stvari, uključujući ljude, organizacije, uređaje i sisteme, i to je komplikovana struktura koja se širi. Zbog ove međusobne povezanosti, informacije, resursi i usluge mogu se brzo razmjenjivati širom svijeta, što bi bilo nemoguće bez upotrebe digitalne tehnologije u našem svakodnevnom životu.

Postavlja se pitanje: Kako se može osigurati integritet, povjerljivost i dostupnost podataka u ovom sve složenijem ekosistemu međuzavisnosti? Ovaj diplomski rad se bavi upravo ovim pitanjem, a posebno će istražiti ulogu tehnologije blockchain-a u očuvanju sigurnosti podataka unutar ove mreže međuzavisnosti.

Od ključne je važnosti prepoznati da korišćenje blockchain tehnologije za bezbjednost podataka nije bez svojih poteškoća. Glavne prepreke širokoj upotrebi blokčejn tehnologija uključuju skalabilnost, potrošnju energije, interoperabilnost i regulatorna pitanja. Pored toga, ovaj rad će istražiti ova ograničenja i ponuditi prijedloge za potencijalna riješenja.

U zaključku, konačni cilj ovog diplomskog rada je da unaprijedi naše razumijevanje blockchain tehnologije i kako ona utiče na bezbjednost podataka. Nastojimo da damo korisne uvide donosiocima odluka u oblasti informacionih sistema i tehnologije posmatrajući njihove moguće primjene, prednosti i prepreke. Namjera je da ovo istraživanje otvori vrata pouzdanijoj i sigurnijoj digitalnoj budućnosti.

2. BLOCKCHAIN TEHNOLOGIJA

2.1. Što je "BLOCKCHAIN"?

Riječ "blokčejn" se odnosi na činjenicu da se tehnologija sastoji od lanca blokova. Svi transakcijski podaci se čuvaju u decentralizovanoj, digitalnoj i otvorenoj knjizi. Zamislimo blockchain kao Google dokument da bismo ga bolje razumjeli. Zatim zamislimo da imamo kopije tog Google dokumenta na svim računarima. Pored toga, u blokčejnu, računari se nazivaju čvorovima i povezani su jedan sa drugim preko iste mreže. [1]

Ovo ukazuje da je sistem decentralizovan, što znači da nijedna organizacija nema potpunu kontrolu nad svim aktivnostima koje se odvijaju u digitalnoj knjizi. Blockchain stvara peer-to-peer (P2P)[1] sistem, što čini sistem sigurnim i pouzdanim. Knjiga je otvorena za sve, činjeći je javnom i transparentnom.

Google tabela sadrži podatke koji se ponavljaju na svim čvorovima, što ukazuje da se identične informacije čuvaju na svakoj mašini. Podaci koji se šalju u sistem isti su za svakog korisnika i izvedeni su iz svake transakcije ili aktivnosti koju korisnik uradi.

Novi blok se dodaje u mrežu svaki put kada se transakcija ili druga aktivnost izvrši na blokčejnu. Ali se brzo prikazuje dok se formalno ne dokumentuje. Detalji predstavljeni u svakoj transakciji mogu uključivati dan i vrijeme kada je transakcija izvršena, uključene strane, pošiljaoca, primaoca i iznos koji je prenjet (ako je u pitanju novac). Blockchain se isto tako odnosi na bazu podataka sastavljenu od diskretnih blokova koji su digitalno povezani. To znači da nije koncentrisana na jednom mestu već se sastoji od niza malih baza podataka koje su digitalno povezane i koje sadrže informacije o svim digitalnim transakcijama, uključujući podatke iz matičnih knjiga, izvoda iz matičnih knjiga i drugih ugovora koji se tiču autorskih prava, između ostalih, u koje nije učestvovao nijedan poznati regulator.

"*Do sada će inovativnom investitoru biti jasno da prostor blockchain tehnologije još uvijek napreduje i da će to nastaviti da radi u godinama koje dolaze*". [2]

[1] P2P je koncept i model komunikacije i distribucije podataka, softvera ili resursa između računara ili uređaja direktno, bez centralnog posrednika ili servera.

2.2 Historija Blockchain-a

Od svog početka 2009. godine, blockchain tehnologija je doživela nevjerovatnu evoluciju. Prva aplikacija zasnovana na blokčejnu, Bitcoin, označila je početak svega. Bitkoin je dizajniran sa ciljem da se uvede decentralizovana digitalna valuta koja bi funkcionisala nezavisno od centralizovanih vlada i finansijskih organizacija.

Blockchain, tehnologija koja podržava Bitcoin, poslužila je kao kamen temeljac za promjenu paradigme u bezbjednosti podataka i povjerenju. Njegov tvorac je neuhvatljivi Satoši Nakamoto.

On je fundamentalnu ideju Blockchain-a prvi je predstavio u dokumentu pod nazivom *„Bitcoin: A Peer-to-Peer Electronic Cash System"*[2] koji se smatra polaznom tačkom za sve koji su zainteresovani za ovu temu.

Ako bismo dalje pojednostavili stvari radi lakšeg usvajanja ove ideje, počeli bismo tako što bismo imali jednu glavnu knjigu u kojoj se evidentiraju sve transakcije umjesto da svako vodi svoje knjige i posebnu evidenciju svake transakcije. Ova glavna knjiga bi bila otvorena za javnost, dostupna svima i potpuno decentralizovana, što znači da niko ne bi posjedovao, kontrolisao je ili upravljao njenim podacima.

Svaki put kada je izvršena transakcija, kao što je slanje bitkoina sa jedne adrese na drugu, ona je zabilježena, sačuvana i vremenska oznaka. Niko ne bi mogao da trguje nečim što ne posjeduje jer: [3]

- Ne bi bio sinhronizovan sa zapisima o transakcijama ili drugim korisnicima sistema.
- Pravila se uspostavljaju na samom početku i sprovode u djelo preko programskog koda.

Srazlogom da je istorija svake transakcije sačuvana i dostupna u realnom vremenu, proizilazi da se ne može desiti da se isti proizvod razmjenjuje više puta.

Kao što sve ima svoj digitalni trag i evidenciju, dva poslovna partnera mogu brzo i elektronski da izvrše bilo kakvu razmjenu vrijednosti bez potrebe za posrednicima ili dodatnim naknadama, bez obzira na to koliko su udaljeni jedan od drugog ili koliko malo znaju jedni o drugima. Kada je zadatak (transakcija) završen, on je zauvek zaključan i ne može se promjeniti.

Iako je koncept Blockchain-a široko priznat, postoje različita mišljenja o tehnologiji, pa čak i o njenoj istoriji. U Nakamotoovom (2008) bijeloj knjizi 3[2], termini „blok“ i „lanac“ su korišćeni pojedinačno, a ideja je prvobitno nazvana blokčejn [4]. Međutim, koncept se na kraju sveo na frazu „Blockchain“ do 2016. godine.

Kada govorimo o istoriji i hronološkom razvoju blokčejna, prikladno je istaći najvažnije momente u razvoju ovog fenomena:

Mi identifikujemo pronalazak Bitcoina kao početnu inovaciju (događaj) Blockchain-a. Još jedna inovacija bi bila koncepcija Blockchain tehnologije, odnosno, upotreba Bitcoina u brojnim tehnološkim aplikacijama, bankarskom i finansijskom sektoru i korporativnim poduhvatima.

Prema statistikama Dona Tapscotta i Alexa Tapscotta u 2017 godini, preko 15% banaka širom svijeta koristilo je Blockchain tehnologiju. [5]

„Pametni ugovor“ bi bio treća inovacija, koja bi se odmah stavila u Blockchain i koristila kao legitimni i dostupni podaci. Pored korišćenja zajmova ili obveznica kao finansijskih instrumenata umjesto bitkoina i drugih kriptovaluta[3], ovo bi takođe uključivalo i njih. "Dokaz udjela" i "dokaz o radu" bila bi četvrta inovacija. Ove kompanije, koje se obično nazivaju „rudarima“, zadužene su za ogromne centre podataka i za sigurnost se oslanjaju na plaćanja kriptovalutama. Skaliranje blokčejna je šesti ključni razvoj. Uvjek radu na unapređenju tehnologije i ubrzanju svih procedura. Njihov cilj je da olakšaju rad uz održavanje bezbjednosti i sigurnosti.

Ovdje ispitujemo glavne prekretnice i istorijska dostignuća u blokčejn tehnologiji. Istražujemo kako se blokčejn tehnologija razvila izvan valute, pokrivajući značajne inicijative i platforme kao što je Ethereum, koji je ponudio funkcionalnost pametnih ugovora i otvorio vrata za decentralizovane aplikacije (DApps)[4].

---

[2] Bijela knjiga je izveštaj ili uputstva koji nudi gledište organa koji ga izdaje o teškoj temi, dok čitaocima pruža jednostavne informacije. Namjenjena je da pomogne čitaocima da shvate situaciju, pronađu riješenje ili dođu do izbora.

[3] Kriptovaluta je oblik digitalne imovine koja se koristi kao sredstvo razmijene, koristeći kriptografiju kao način obezbjeđivanja sigurnosti transakcija, kontrole stvaranja dodatnih novčanih jedinica i radi potvrde transfera valute.

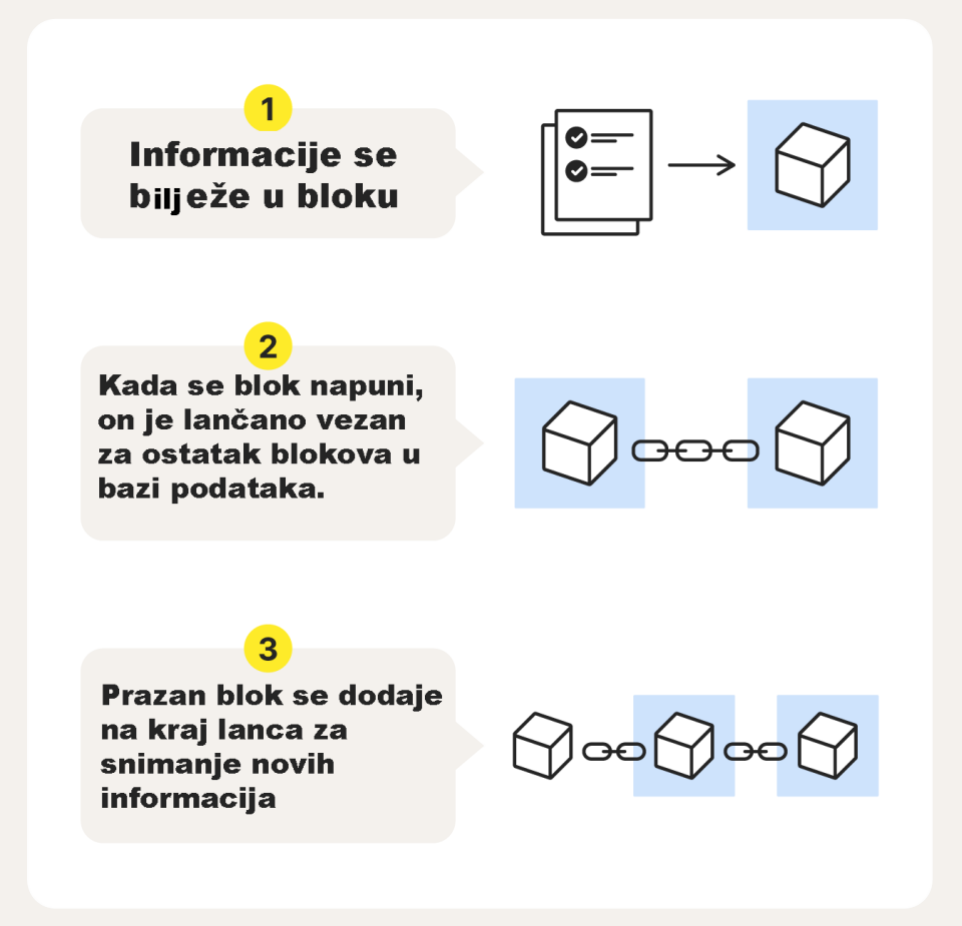
[4] Decentralizovane aplikacije su softverski programi koji rade na decentralizovanim računarskim platformama kao što je blockchain.

Takođe je pokriven razvoj blokčejn napora zasnovanih na konzorcijumu kao što su Hyperledger[5] i Corda[6], koji su imali za cilj da ispune posebne zahteve preduzeća.
Ovo ilustruje kako je blokčejn evoluirao od svojih beznačajnih početaka do remetilačke sile sa potencijalom da promjeni industrije i redefiniše politike bezbjednosti podataka proučavajući istorijsku pozadinu tehnologije.

2.3. Kako funkcioniše Blockchain?

Blockchain je online baza podataka, popularno korišćena za transakcije kriptovaluta, koje čuvaju informacije hronološki i u blokovima.

Slika 1: Prikaz kako funkcioniše Blockchain?



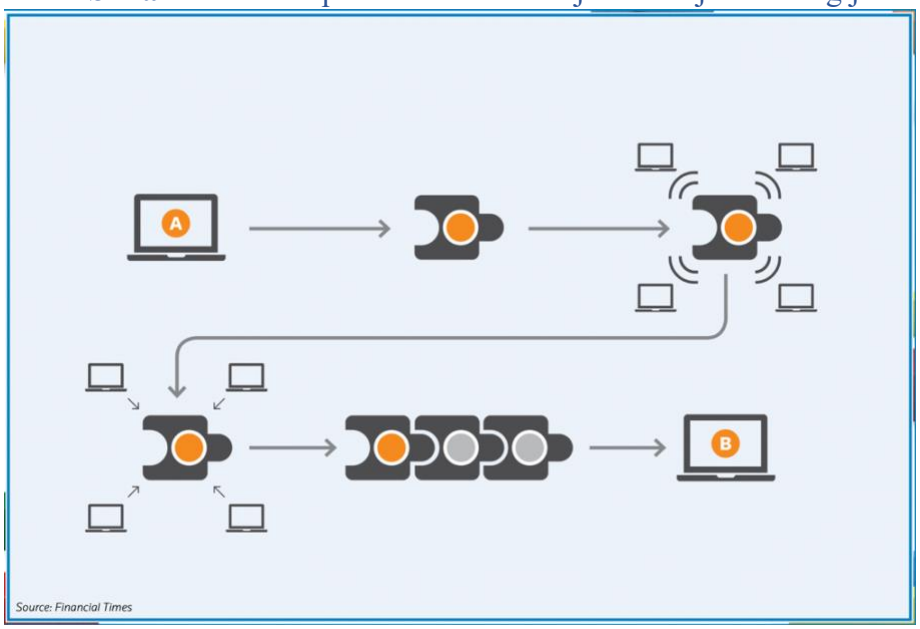
[5] Hyperledger je inicijativa Fondacije Linux koja pruža razne projekte i okvire za razvoj poslovnih blokchain aplikacija

[6] Corda je otvorena platforma za razvoj distribuiranih aplikacija (DLT) sa fokusom na kompleksne transakcije među organizacijama.

2.3.1 Vizuelni prikaz blokčejna

Blokčejn je mreža međusobno povezanih, digitalno logički uređenih blokova koji sadrže informacije. Kada se memorija bloka (dostupni prostor za skladištenje podataka i informacija) potroši, on se povezuje sa sljedećim blokom, stavljajući ga u neispitanu seriju. Ranije smo ukratko napomenuli da svaki blok ima svoj ID, ili heš (Hash), koji je različit za svaki blok kao i heš bloka koji je došao prije njega. "Svaki blok[7] sadrži heš onog prije njega, što pomaže u povezivanju blokova zajedno da se konstruišu lanci blokova. Jedini blok bez heša prethodnog bloka je Genesis blok. Potpuno je kreiran iz nule i ne uključuje prethodne hešove blokova. Heš bloka se mjenja svaki put kada se pokuša modifikovati podaci ili informacije sadržane u njemu. Prema tome, promjena heša jednog bloka će promjeniti i sve povezane blokove. " [6]

Slika 2 : Vizuelni prikaz funkcionisanja Blokčejn tehnologije



Izvor: Rennock, M. et al. (2018) Blockchain technology and regulatory investigations, str. 3. (https://www.steptoe.com/images/content/1/7/v3/171269/LIT-FebMar18-Feature_Blockchain.pdf)

Osobe koje verificiraju podatke koji se stavljaju u blokove su poznati kao rudari. Privatnost svih prikupljenih podataka i informacija je snažno zaštićena načinom na koji se svi čuvaju i snimaju u blokovima. Svakih 10 minuta, Blockchain ažurira svoje podatke i informacije.

[7] Blokovi su strukture podataka unutar blockchain baze podataka, gdje se podaci o transakcijama ublockchainu kriptovalute trajno bilježe.

2. 4. Radni postupak Blockchaina

Radni postupak svake Blokčejn mreže, i Blockchaina ima svoju određenu proceduru. Za početak svaki blok ima svoj ID koji se naziva *Hash* pomoći koga ga pronalazimo. Ovaj ID nazivamo i svojevrsnim kodom kojim su svi blokovi čvrsto i neraskidivo povezani i bilo koja promjena podataka, unošenje novih ili brisanje postojećih ili bilo koji drugi vid falsifikovanja, prosto nije izvodljiv. Nije iz prostog razloga što prednost u slučaju poslovanja, u slučaju hakovanja postaje mana, moralo bi da se hakuje čitav niz blokova, što posao čini nemogućim. [7]

"Blockchain tehnologija je šifrovana, koristi tešku enkripciju koja uključuje javne i privatne ključeve za održavanje virtuelne bezbjednosti." [8]

2. 4. 1. Transparentnost i sigurnost

U Blokčejin tehnologiji transparentnost dolazi u svom punom obliku. Svaka istorija transakcije ima svoj nesumnjiv trag i dostupna je na evidenciju zainteresovanim korisnicima. Ovdje je interesantno reći da svaki učesnik mreže dijeli iste originalne podatke iz distributivne knjige, odnosno nema pojedinačnih kopija jednog dokumenta, već svi dijele iste originalne podatke. Mjenjanjem jednog podatka, svi podaci vezani za taj dokument u nizu lanca automatski bivaju korigovani i promjenjeni, tako da prostora za grešku nema. Kao rezultat toga, podaci koji se čuvaju na blockchainu su pouzdaniji, stabilniji i transparentniji od podataka obrađenih korišćenjem dugotrajnih konvencionalnih procedura.

I ako smo u gornjem djelu rada već više puta pominjali sigurnost, veoma je bitno da se o ovome govori jer je kao glavna mana i prepreka za brže širenje i prosperitet Blokčejn tehnologije, pominjana baš sigurnost. Za početak treba istaći da je ova tehnologija bezbjednija od drugih sistema na više načina, a prvi od njih bi bio da bilo koja transakcija koja se obavlja prije snimanja, mora biti odobrena. Ona dobija svoju šifru (kodirana) i povezana sa predhodnom tek kada bude odobrena. Svi podaci se čuvaju na različitim računarima, preko mreže, tako da je sve decentralizovano, a samim tim i otežano hakerima da pokvare podatke i učine ih nevalidnim. Veliki je akcenat dat na zaštitu ličnih, zdravstvenih, finansijskih ili službenih podataka i tu su mobilisane sve snage u sprečavanju prevara i nezakonitog ponašanja.

2.5. Zašto je Blockchain potreban?

Potreba za poboljšanom bezbjednošću podataka, privatnošću i integritetom postaje sve važnija u današnjem digitalnom okruženju. Dugotrajne slabosti tradicionalnih centralizovanih sistema uključuju pojedinačne tačke kvara, povrede podataka, nedostatak transparentnosti i zabrinutost za povjerenje. Zbog ovih nedostataka, sada postoji veća potreba nego ikada za najsavremenijim riješenjima koja mogu da riješe ove osnovne probleme i povećaju povjerenje u bezbjednost podataka.

Da bi se ispunila ova potražnja, blockchain tehnologija se pojavila kao potencijalna opcija. Blockchain nudi novu paradigmu za upravljanje podacima i sigurnost korišćenjem tehnologije distribuirane knjige[8]. Srazlogom da je blokčejn decentralizovan, on eliminiše potrebu za jednim centralnim autoritetom i umjesto toga distribuira kontrolu i ovlašćenja za donošenje odluka preko mreže učesnika. Bezbjednost i pouzdanost podataka sadržanih u blokčejnu poboljšani su decentralizacijom, koja obezbjeđuje da nijedan entitet ne može da mjenja podatke.

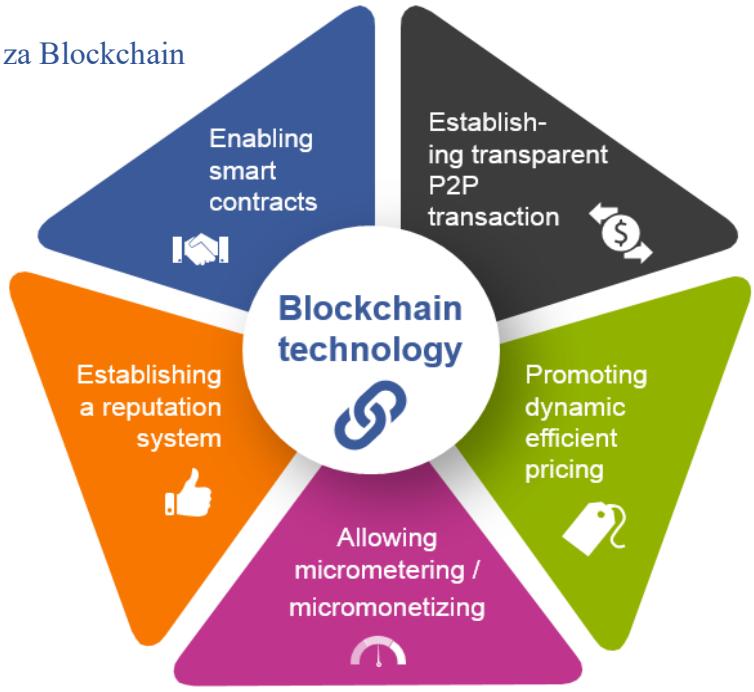
Pored toga, sloj bezbjednosti je uključen u nepromjenjivost podataka blockchain-a. Bez saglasnosti korisnika mreže, skoro je teško promjeniti ili ukloniti informacije nakon što su uskladištene na blokčejnu. Blockchain je posebno pogodan za aplikacije u kojima su kvalitet podataka i revizija od suštinskog značaja, kao što su finansijske transakcije, upravljanje lancem snabdijevanja i medicinski kartoni, jer se radi o ovoj osobini.

Štaviše, otvorenost i slijedljivost blokčejna doprinose njihovom značaju u ispunjavanju zahtjeva za bezbjednošću podataka. Svi korisnici mogu da vide svaku transakciju koja je snimljena na blockchain-u, što ga čini transparentnim i podložnim kontroli. Podstičući povjerenje među članovima mreže i sprečavajući prevare, ova otvorenost smanjuje potrebu za posrednicima i pojednostavljuje procedure.

Blockchain tehnologija se pojavila kao obećavajuće riješenje za riješavanje hitne potrebe za poboljšanom bezbjednošću podataka, privatnošću i integritetom u današnjem digitalnom pejzažu (Smith, 2022) [9].

[8] Distribuirane knjige- distribucija se odnosi na proces i logistiku stavljanja na raspolaganju kupcu.

Slika 3: Potreba za Blockchain



Izvor: (https://iloan.lk/wp-content/uploads/2019/05/2.png)

Pametni ugovori, koji su samoizvršni ugovori sa utvrđenim pravilima direktno snimljenim u blokčejn, su još jedan koncept koji je uveo blokčejn. Pametni ugovori zamjenjuju potrebu za konvencionalnim procedurama upravljanja ugovorima automatizacijom i sprovođenjem uslova ugovora. Pametni ugovori zasnovani na blokčejnu poboljšavaju efikasnost, smanjuju troškove i smanjuju rizik od prevarnih aktivnosti ukidanjem posrednika i automatizacijom izvršenja ugovora.

Pored toga, blockchain je neophodan iz više razloga nego samo zbog povećanja bezbjednosti podataka u preduzećima. Riješenja zasnovana na blokčejnu pružaju brže, sigurnije i pristupačnije opcije u sektorima kao što su doznake, gde prekogranične transakcije ponekad podrazumijevaju dugotrajne procedure i značajne troškove. Peer-to-peer transakcije su omogućene decentralizovanom arhitekturom blokčejn tehnologije, koja smanjuje troškove transakcije i uklanja potrebu za posrednicima, istovremeno održavajući sigurnost i integritet gotovine koja se prenosi. U zaključku, nedostaci i slabosti centralizovanih sistema, koji dugo nisu garantovali prihvatljivu sigurnost podataka, privatnost i integritet, rađaju potrebu za blokčejn tehnologijom. Blockchain nudi revolucionarni pristup za postizanje ovih ciljeva korišćenjem svoje decentralizovane arhitekture, nepromjenljivosti, transparentnosti i mogućnosti pametnih ugovora. Blockchain je pozicioniran kao vrijedan alat za brojne kompanije i aplikacije u digitalnoj eri zbog svoje sposobnosti da poboljša bezbjednost podataka, ubrza procedure, uštedi troškove i podstakne povjerenje.

2.5. Prednosti blockchain tehnologije

Prednosti blockchain tehnologije imaju fokus na jake karakteristike bezbjednosti podataka sistema. Blockchain nudi poseban metod za upravljanje podacima i bezbjednost korišćenjem decentralizovane i distribuirane tehnologije knjige, povećavajući povjerenje, transparentnost i integritet. *"Kao što je istraženo u knjizi 'Blockchain Security: Theory and Solutions', sigurnost je ključna komponenta blockchain tehnologije (Defrawy & Youssef, 2018 Godina, str. 42)."* [10] . Neke od prednosti blockchain tehnologije i ilustrovanja kako ona ima sposobnost da prevaziđe probleme sa bezbjednošću podataka u digitalnoj eri su:

1. Poboljšana bezbjednost podataka: Koristeći kriptografske metode, blockchain tehnologija obezbjeđuje podatke i obezbjeđuje njihovu tajnost, integritet i validnost. Blockchain-ova decentralizovana struktura smanjuje mogućnost jedne tačke kvara i povećava njenu otpornost na hakere i manipulaciju. Nepromjenljiv lanac podataka koji se može revidirati proizvodi svaku transakciju koja je vremenski označena, šifrovana i povezana sa onom prije nje na blok lancu.

2. Transparentnost i mogućnost kontrole: Korišćenjem decentralizovane mreže učesnika za potvrđivanje transakcija, blockchain uklanja potrebu za posrednicima i centralizovanim autoritetom. Učesnici mogu više vjerovati jedni drugima zbog decentralizovane prirode mreže, koja sprečava bilo koji entitet da ima potpunu kontrolu. Procedure konsenzusa blokčejna osiguravaju da transakcije odobrava većina korisnika, čime se povećava pouzdanost sistema.

3. Decentralizacija i povjerenje: Sve strane mogu da pregledaju i potvrde transakcije koje su snimljene na blokčejnu zahvaljujući njegovoj transparentnosti. S obzirom da se svaki disparitet ili sumnjivo ponašanje može brzo otkriti i pratiti do njegovog izvora, ova otvorenost poboljšava odgovornost i eliminiše lažne operacije. Blockchain je posebno koristan u sektorima kao što su upravljanje lancem snabdijevanja i finansijske usluge jer može da revidira i verifikuje transakcije u realnom vremenu.

4. Integritet i nepromjenljivost podataka: Podaci koji su uskladišteni na blokčejnu ne mogu se mjenjati ili uklanjati bez saglasnosti svih korisnika mreže. Blockchain tehnologija garantuje integritet i trajnost podataka jer je prikladna za aplikacije u kojima je neovlašćeno manipulisanje podacima zabrinjavajuće zbog njihove nepromjenljivosti. Nepromjenljivost blokčejna obezbjeđuje tačnost i pouzdanost sačuvanih podataka, bilo da se radi o finansijskim transakcijama, medicinskim kartonima ili intelektualnoj svojini.

2.6. Prednosti Blockchain-a u kontekstu bezbjednosti podataka

Postoje nekoliko prednosti korišćenja blockchain tehnologije, posebno u pogledu bezbjednosti podataka. Veća zaštita podataka, integritet i pouzdanost koju obezbeđuje njihova decentralizovana priroda, kriptografska bezbjednost, transparentnost i nepromjenljivost.
Prema Antonopoulosu (2014)[9], blockchain tehnologija omogućava veću privatnost korisnicima. [11]
Mehanizmi konsenzusa, tehnologija distribuirane knjige, skalabilnost i pametni ugovori su dodatne karakteristike koje doprinose opštoj bezbjednosti i efikasnosti sistema zasnovanih na blokčejnu. Blockchain tehnologija nudi riješenja koja mjenjaju igru i koja imaju sposobnost da revolucionišu nekoliko sektora i postave nova mjerila za bezbjednost podataka u digitalnom svijetu dok firme rade na zaštiti svojih podataka i pojednostavljivanju procesa.

Prilagodljivost (Skalabilnost): je prednost blockchaina, omogućavajući veću propusnost transakcija kako se mreža širi. Blockchain tehnologija može obraditi veliki broj transakcija bez žrtvovanja njegove efikasnosti ili sigurnosti zahvaljujući tehnologiji distribuirane knjige i konsenzus algoritmima. Ova prilagodljivost je posebno važna u sektorima koji zahtjevaju veliku obradu transakcija, kao što su bankarstvo, lanac snabdijevanja i zdravstvena zaštita. [12]

Nepromjenljivi revizorski trag: Kapacitet blokčejna da proizvede nepromjenljivi revizorski trag je jedna od njegovih glavnih prednosti. Lanac nepromjenljivih podataka se kreira kada je svaka transakcija na blok lancu vremenski označena i povezana sa onom prije nje. Ovaj revizorski trag daje svim transakcijama jasnu, provjerljivu evidenciju, poboljšavajući odgovornost i olakšavajući efikasne procedure revizije. On promoviše povjerenje zainteresovanih strana dok pomaže firmama da se pridržavaju regulatornih standarda.[13]

Poboljšana privatnost: Zaštita privatnosti ugrađena u blokčejn tehnologiju daje korisnicima kontrolu nad njihovim podacima uz održavanje otvorenosti.

[9] Andreas M. Antonopoulos je poznat kao stručnjak za kriptovalute i blockchain tehnologiju. On je autor i govornik koji je igrao značajnu ulogu u popularizaciji i razumijevanju kriptovaluta, posebno bitcoina, i blockchain tehnologije. Njegova knjiga "Mastering Bitcoin," objavljena 2014. godine, postala je jedan od klasičnih izvora za razumijevanje bitcoina i kriptovaluta.

Pseudonimnost je karakteristika javnih blokčejnova, gdje se korisnici prepoznaju po njihovim posebnim kriptografskim ključevima, a ne po ličnim podacima. Privatni blok lanci, s druge strane, nudi paradigmu ograničenog pristupa koja dozvoljava samo ovlašćenim stranama da pregledaju podatke i komuniciraju sa njima. Ove karakteristike privatnosti zadovoljavaju različite slučajeve korišćenja i zakonske zahtjeve uz održavanje ravnoteže između otvorenosti i tajnosti.[14]

Ugovori koji se sami izvršavaju, ili „pametni ugovori“, napisani su u kodu i čuvaju se na blokčejnu. Oni automatizuju izvršenje ugovora, ukidajući potrebu za posrednicima i smanjujući mogućnost prevare ili manipulacije od strane ljudi. Garantujući da se uslovi ugovora automatski podržavaju i potvrđuju od strane blokčejn mreže, pametni ugovori poboljšavaju bezbjednost. Smanjenjem oslanjanja na posrednike, oni poboljšavaju efikasnost, pojednostavljuju operacije i nude još jedan stepen zaštite. [15]

Međuorganizacijska saradnja ili saradnja između mnogih entiteta je bezbjedna i transparentna zahvaljujući blockchain tehnologiji. Blockchain promoviše povjerenje i podržava efikasan protok podataka između zainteresovanih strana nudeći zajedničku i nepromjenljivu knjigu. Smanjuje troškove i pojednostavljuje procedure ukidanjem zahtjeva za posrednicima ili spoljnim dobavljačima povjerenja. Ova prednost je posebno važna za preduzeća sa više strana, kao što je upravljanje lancem snabdijevanja, jer omogućava praćenje u realnom vremenu, sljedljivost i odgovornost u cijeloj mreži lanca snabdijevanja. [16]

2.7. Nedostaci blockchain tehnologije

Iako su potencijalne prednosti blockchain tehnologije privukle veliku pažnju, važno je uzeti u obzir i ove faktore. Ovaj diplomski rad isto tako ispituje nedostatke blockchain tehnologije sa posebnim naglaskom na njene karakteristike bezbjednosti podataka. Iako blockchain nudi poboljšanu sigurnost podataka na mnogo načina, postoji nekoliko problema i prepreka koje se moraju uzeti u obzir.[17] Za preduzeća i ljude koji žele da iskoriste potencijal blockchain tehnologije dok minimiziraju opasnosti, razumijevanje njenih granica je od suštinskog značaja.

1. Izazovi skalabilnosti: Skalabilnost blockchain tehnologije je jedno od glavnih pitanja. Vrijeme obrade i resursi potrebni za dodavanje novih transakcija mogu se drastično povećati kako se veličina lanca blokova širi. Blockchain može postati manje koristan za aplikacije velikog obima kao što su obrada plaćanja u realnom vremenu ili sektori sa intenzivnim podacima kao rezultat sporije brzine transakcija i većih troškova. Konstantna je borba da se pronađu načini za povećanje skalabilnosti blokčejna bez žrtvovanja njegove bezbjednosti.

2. Potrošnja energije: Blockchain mrežama je potrebno mnogo procesorske snage i energije, posebno onima koje koriste tehnike konsenzusa dokazivanja rada. Proces rudarenja, koji potvrđuje transakcije i štiti blockchain, koristi značajnu količinu energije. Da bi se smanjio ekološki otisak blokčejn tehnologije, potrebne su energetski efikasnije procedure konsenzusa zbog velike potrošnje energije.

3. Regulatorni i pravni izazovi: Regulativa i pravna pitanja su postavljena zbog decentralizovane prirode blockchain tehnologije. Posebne karakteristike blokčejna, uključujući prekogranične transakcije, pametne ugovore i nedostatak centralne vlasti, teško se prilagođavaju tradicionalnim pravnim okvirima i agencijama. Možda će biti neophodno da se kreiraju novi pravni okviri kako bi se na odgovarajući način riješili problemi sa jurisdikcijom, privatnošću podataka, pravima intelektualne svojine i usklađenošću sa propisima.

4. Rizici privatnosti i bezbjednosti podataka: Iako blockchain ima poboljšane bezbjednosne karakteristike, i dalje postoje prijetnje bezbjednosti i privatnosti. Javni blok lanci, koji su transparentni i otvoreni, mogu učiniti privatne podatke dostupnim neovlašćenim stranama. S druge strane, obezbjeđivanje odgovarajućih ograničenja pristupa i sprečavanje insajderskih prijetnji predstavlja poteškoću za privatne blokčejnove.

3. SIGURNOST PODATAKA

Sigurnost podataka se pojavila kao jedno od najbitnijih pitanja sa kojima ljudi, kompanije i vlade moraju da se bave u digitalnom okruženju koje se stalno mjenja. Eksponencijalno povećanje broja podataka i rastuća zavisnost od digitalne tehnologije nastala je ogromna i raznovrsna panorama rizika, u rasponu od sofisticiranih sajber napada do nenamjernih povreda podataka. Kako sve više preduzeća usvaja strategije zasnovane na podacima i digitalnu transformaciju, zaštita povjerljivosti, integriteta i dostupnosti osjetljivih podataka nikada nije bila važnija. [18]

Bezbjednost podataka se odnosi na širok spektar politika, procedura i alata koji se koriste za zaštitu digitalne imovine od neovlašćenog pristupa, modifikacije i brisanja. Ukršta se sa nekoliko disciplina, uključujući obradu, prenos i skladištenje podataka. Bezbjednost podataka je postala sve složenija i raznovrsnija kako su računarstvo u oblaku, gadžeta za Internet stvari (IoT)[10] i mobilne tehnologije sve više korišćene.
Kršenje podataka može imati ozbiljne posledice, uključujući novčane gubitke, štetu po ugled, pravne posljedice i, u određenim situacijama, prijetnju nacionalnoj bezbjednosti. Da bi bile ispred novih prijetnji, organizacije ulažu velike investicije u solidne strategije i riješenja za bezbjednost podataka.

Ključna komponenta bezbjednosti podataka je šifrovanje, koje uključuje korišćenje sofisticiranih algoritama za transformaciju podataka otvorenog teksta u šifrovani tekst. Ovo osigurava da čak i ako neovlašćeni ljudi pristupe podacima, i dalje će biti nemoguće dekodirati ih bez odgovarajućih ključeva za šifrovanje. Enkripcija od kraja do kraja sada se smatra najboljom praksom za zaštitu podataka kako u tranzitu tako iu stanju mirovanja. [19]

[10] Internet of Things (Internet Stvari)- se odnosi na koncept povezivanja različitih fizičkih uređaja i objekata na internet radi razmjene podataka i upravljanja njima. Ova tehnologija omogućava uređajima da komuniciraju međusobno i sa centralnim sistemima putem internetskog protokola.

Slika 4: Šifrovanje- algoritmi za transformaciju podataka

(Izvor: https://www.analyticsinsight.net/wp-content/uploads/2021/05/Data-Security.jpg)

Ograničavajući pristup kritičnim informacijama na osnovu korisničkih uloga, dozvola i akreditiva za autentifikaciju, tehnike kontrole pristupa igraju ključnu ulogu u bezbjednosti podataka. Korišćenje tehnologija biometrijske i multifaktorske autentikacije (MFA)[11] za autentifikaciju dodaje dodatni nivo zaštite od neovlašćenog pristupa.

Kako bi se osiguralo da se podaci mogu vratiti u slučaju gubitka podataka ili kvara sistema, redovne rezervne kopije podataka i planovi oporavka od katastrofe su ključni elementi bezbjednosti podataka. "*Rezervne kopije treba čuvati na bezbjednim lokacijama van lokacije kako bi se izbjegla krađa ili fizički gubitak podataka." [20]*

Sveobuhvatna bezbjednosna pravila, obuka osoblja i strategije reagovanja na incidente su sve uključene u bezbjednost podataka. Ljudska greška je i dalje glavni faktor koji doprinosi kršenju podataka, stoga je važno edukovati osoblje o najboljim načinima za rukovanje osjetljivim podacima i potencijalnim opasnostima po sajber bezbjednost.

[11] Multifaktorska autentikacija (MFA) je sigurnosni mehanizam koji zahtjeva od korisnika da pruži više od jednog načina autentikacije kako bi dokazao svoj identitet prilikom pristupa određenom računu ili sistemu. Ovaj pristup povećava nivo sigurnosti jer zahtjeva više nezavisnih faktora, što otežava neovlašćenim osobama da pristupe korisničkim nalozima ili podacima.

Bezbjednost podataka sada ima novu dimenziju zahvaljujući razvoju blockchain tehnologije. Integritet podataka i bezbjednost protiv neovlašćenog pristupa su obezbjeđeni decentralizovanom i nepromjenljivom knjigom blokčejn tehnologije. Blockchain tehnologija koristi kriptografske tehnike za povećanje tajnosti podataka, što je čini poželjnom alternativom za sektore koji traže pouzdana riješenja za bezbjednost podataka. [21]
Sajber opasnosti se uvek mjenjaju, uprkos izuzetnoj zaštiti koju su poboljšanja tehnologije bezbjednosti podataka ponudila. Bezbjednost podataka suočava se sa novim poteškoćama i mogućnostima zbog brzog usvajanja tehnologija u razvoju kao što su vještačka inteligencija (AI), kvantno računarstvo i 5G mreže. Da bi se zaštitile od novih napada, organizacije moraju ostati pažljive, redovno mjenjati svoje bezbjednosne procedure i raditi sa profesionalcima za sajber bezbjednost. [22]

Ukratko, bezbjednost podataka je i dalje glavno pitanje u digitalnoj eri. Zaštita osjetljivih informacija zahtjeva jake procedure bezbjednosti podataka, šifrovanje, ograničenja pristupa i obuku osoblja. Pored toga, najsavremenija tehnologija kao što je blockchain nudi intrigantne alternative za jačanje bezbjednosti podataka. Organizacije mogu da izgrade digitalno okruženje otporno na budućnost i bezbjiedno tako što će prepoznati dinamičnu prirodu prjetnji po sajber bezbjednosti i usvojiti proaktivne mjere zaštite podataka.

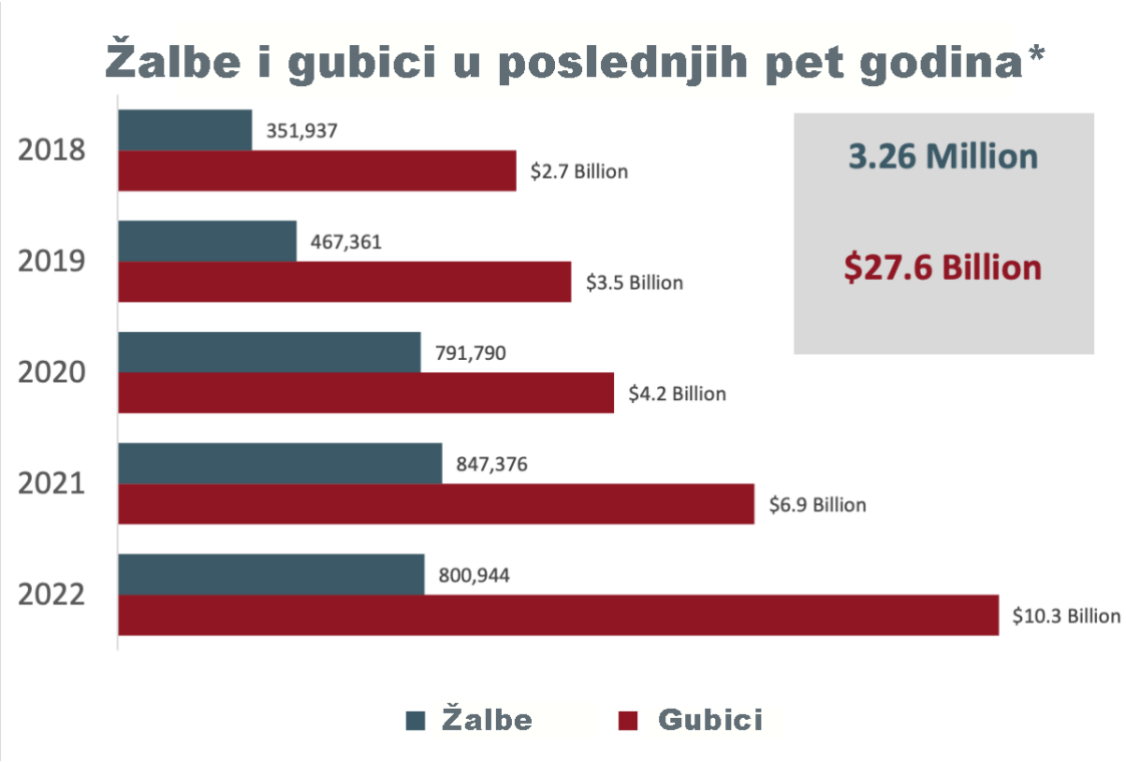
3.1 Sigurnost podataka kroz godine

Kako nam tehnologija omogućava da komuniciramo, sarađujemo i djelimo informacije, bezbjednost podataka je ključna komponenta u digitalnom svijetu. Do danas se informaciona tehnologija još uvek brzo razvija, posebno u oblastima koje uključuju specijalizovanu podijatriju. Ova sekcija će opisati transformaciju bezbjednosti u narednih nekoliko godina, naglašavajući kako su tehnologija i društveni napredak uticali na ovo.

Tokom proteklih pet godina, FBI IC3 [12] je stalno primao u proseku 652.000 pritužbi godišnje. Od 2018. bilo je 3,26 miliona žalbi i 27,6 milijardi dolara gubitaka

[12] Internet Crime Complaint Center (Centar za žalbe na internet kriminal) - specijalizovani centar koji je osnovala FBI kako bi omogućio građanima i organizacijama da prijave različite vrste internet kriminala i prevare.

Grafik 1: Žalbe i gubici podataka u posljednjih 5 godina



(Izvor: https://www.techopedia.com/cybersecurity-statistics)

Ovaj grafikon može jasno pokazati kako su prijetnje sajber bezbjednosti postale sve složenije i češće tokom vremena, naglašavajući potrebu za kontinuiranim napretkom u zaštiti podataka. Isto tako istorijski pogled na bezbjednost podataka pokazuje širinu razvoja koji se dogodio u industriji bezbjednosti informacija. Očigledno je da se bezbjednosna paradigma stalno mjenja kako bi odgovorila na nove tehničke izazove, od ranih tehnika preko šifrovanja do sofisticiranih sistemskih potreba današnjice.

Neophodno je ostati oprezan i agresivan u riješavanju opasnosti kako tehnologija nastavlja da napreduje. Bezbjednost podataka je društvena potreba koliko i tehnološko pitanje. Možemo se pobrinuti da naši digitalni ekosistemi budu sigurni, pouzdani i održivi tako što ćemo uzeti odgovarajući pristup.

3.2 Vrste kontrola bezbjednosti podataka

Obezbjeđivanje osjetljivih podataka postalo je ključno i za pojedince i za organizacije u sadašnjem digitalnom dobu. Da bi se zaštitile informacije i podržala privatnost podataka suočenih sa rastućom prijetnjom kršenja podataka i sajber napada, moraju se uspostaviti efikasni mehanizmi kontrole. Ove su ključne metode koje se moraju koristiti za garantovanje bezbjednosti podataka, uključujući šifrovanje, pravljenje rezervnih kopija, brisanje podataka, maskiranje podataka, kontrolu pristupa i rezervne kopije. Primjenom ovih mjera, ljudi i organizacije mogu ojačati svoje prakse zaštite podataka, smanjiti moguće opasnosti i promovisati bezbjedno online okruženje. [23]

Slika 5: Kontrola bezbjednosti podataka

(Izvor: https://intellipaat.com/blog/wp-content/uploads/2021/09/data-security-controls.jpg)

Zaštita podataka i povreda podataka moraju se izbjeći pridržavanjem sljedećih kontrolnih procedura:

Pristup za upravljanje - Metode primjene za ograničavanje pristupa kritičnim sistemima i podacima, kako fizički tako i digitalno. Svaki računar i gadžet moraju da imaju lozinku i da samo ovlašćeno osoblje treba da im fizički pristupi.

Autentikacija - Prioritet moraju da imaju mjere autentifikacije, kao što su ograničenja pristupa i tačna identifikacija ljudi, prije nego što se dozvoli pristup podacima. Lozinke, PIN-ovi, bezbjednosni tokeni, kartice za prevlačenje i biometrijski podaci su tipični primjeri.

Oporavak od katastrofa i pravljenje rezervnih kopija - Posjedovanje rezervnog plana za siguran pristup podacima u slučaju kvarova sistema, katastrofa, oštećenja podataka ili kršenja je ključna komponenta bezbjednosti. Kopije podataka rezervne kopije moraju se čuvati na različitim medijima, kao što su čvrsti diskovi, lokalne mreže ili oblak.

Brisanje podataka - Redovno i pravilno moraju da se odlagaju podaci. Koristi se specijalizovani softver da bi se koristile tehnike brisanja podataka, koje su bezbjednije od standardnih procedura brisanja podataka, da bi se potpuno izbrisale podatke sa bilo kog uređaja za skladištenje. Ovim se podaci štite od oporavka i izbjegavaju da dođu u pogrešne ruke.

Maskiranje podataka - Koristi se softver za maskiranje podataka da bi se pokrile osjetljive informacije tako što će se prikriti slova i brojeve proksi znakovima. Podaci se uspješno prikrivaju čak i ako im neovlašćene osobe dobiju pristup. Originalni podaci su dostupni samo ovlašćenim korisnicima.

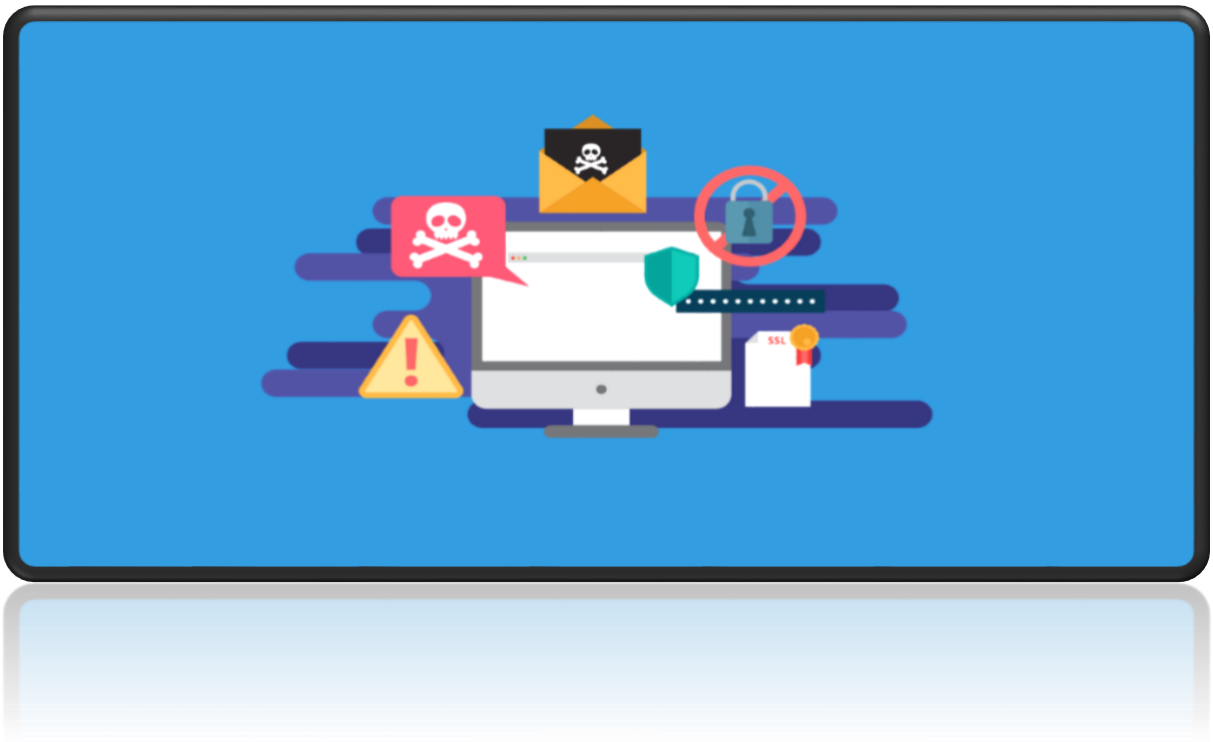
Otpornost podataka - Temeljne mjere bezbjednosti moraju da se usvoje. Opasnosti kao što su nestanci struje i prirodne katastrofe moraju da se riješe, jer one bi mogle ugroziti zaštitu podataka, Da bismo zaštitili privatnost podataka, moramo uključiti otpornost u hardver i softver.

Šifrovanje - Kompjuterske algoritme i ključeve za šifrovanje moraju da se koriste da bi se promjenili tekstualni znakovi u nečitljiv format. Materijalu mogu otključati i pristupiti samo oni koji su ovlašćeni i imaju potrebne ključeve. Širok spektar komponenti mora da se obezbjeđuju, kao što su dokumenti, baze podataka i prepiska putem e-pošte.

Još u drevnim i srednjovekovnim danima, šifrovanje se uglavnom koristilo za komunikaciju između dvije strane koja je zahtjevala da treća strana ne može da razumije poruke između druge dve strane. [24]

Suočeni sa rastućim problemima sajber bezbjednosti, zaštita važnih podataka je ključna obaveza, a ne stvar izbora. Kontrolni mehanizmi obrađeni u ovom članku, koji se kreću od otpornosti podataka i šifrovanja do kontrole pristupa i autentifikacije, djeluju kao kamen temeljac za snažnu bezbjednost podataka. Organizacije mogu bezbjedno da zaštite svoje podatke od neovlašćenog pristupa i potencijalnih povreda tako što će pažljivo pratiti ove prakse. Posvećenost zaštiti podataka treba da bude postojana kako se tehnologija razvija.

Slika 6: Bezbjednost podataka i razvijanje tehnologije



U svijetu koji je sve više međusobno povezan, usvajanje proaktivnog pristupa bezbjednosti podataka ne samo da će zaštititi neprocjenjive informacije već i promovisati povjerenje među korisnicima, klijentima i zainteresovanim stranama. [25] Bezbjednost podataka nije krajnja tačka, već kontinuirano putovanje koje zahtjeva stalnu budnost i prilagođavanje kako bismo bili ispred novih prijetnji.

3.3 Razmatranja o bezbjednosti podataka:

Organizacije i ljudi moraju biti svjesni ovih problema bezbjednosti podataka i preduzeti neophodne mjere da ih riješe. Sigurnost i integritet sistema zasnovanih na blokčejnu može se održati pažljivim očuvanjem kriptografskih ključeva, izvođenjem iscrpnih revizija koda pametnog ugovora i uzimanjem u obzir rezervnih opcija za spor pristup internetu. *"Proaktivne mjere bezbjednosti i redovno praćenje su ključni faktori za održavanje bezbjednosti podataka unutar blokčejn ekosistema." [26].*

Upravljanje ključevima: Bezbjednost blokčejna prvenstveno zavisi od upravljanja kriptografskim ključevima. Za potpisivanje transakcija, šifrovanje podataka i obezbjeđivanje pristupa digitalnim sredstvima koja se čuvaju na blokčejnu, koriste se kriptografski ključevi.

Gubitak privatnog ključa, krađa ili kompromitacija može imati ozbiljne posledice, kao što je gubitak svakog pristupa šifrovanim podacima ili neovlašćeni pristup loših aktera.
Da bi garantovali sigurnost svojih blokčejn sredstava, preduzeća i pojedinci moraju da uvedu pouzdane procedure upravljanja ključevima. Ovo podrazumijeva kreiranje robusnih ključeva, njihovo bezbjedno čuvanje pomoću hardverskih novčanika ili bezbjednih sistema za upravljanje ključevima, postavljanje procesa rezervnih kopija kako bi se sprečio gubitak ključeva i korišćenje metoda bezbjednog djeljenja ključeva samo kada je to neophodno. Sigurnost ključa se takođe može povećati upotrebom višefaktorske autentifikacije i rutinske rotacije ključeva. [27]

Ranjivost pametnih ugovora: Pametni ugovori mogu biti podložni greškama kodiranja i sigurnosnim propustima čak i ako obećavaju automatizaciju i efikasnost. Napadači mogu iskoristiti greške u programiranju pametnih ugovora da ukradu novac ili dobiju pristup privatnim informacijama.
Da bi se pronašle i popravile moguće ranjivosti, tokom kreiranja i implementacije pametnih ugovora treba sprovesti sveobuhvatne revizije koda i bezbjednosne procjene. Rizike treba smanjiti pridržavanjem najboljih praksi bezbjednog kodiranja, koje uključuju validaciju unosa, odgovarajuće rukovanje izuzetcima i korišćenje standardizovanih biblioteka. Pametni ugovori moraju biti kontinuirano nadgledani i brzo zakrpljeni kada se pronađu ranjivosti kako bi se očuvala njihova sigurnost tokom vremena. [28]

Zavisnost od internet konekcije: Potrebna je aktivna internet konekcija da biste učestvovali i pristupili blokčejn mreži koristeći blokčejn tehnologiju. Za slanje, primanje i validaciju transakcija, mrežni čvorovi zahtjevaju internet vezu. Međutim, korisnost i dostupnost riješenja zasnovanih na blokčejnu može biti ometana u okolnostima kada je internet konekcija nestabilna ili nedostupna, na primjer na udaljenim lokacijama ili tokom prirodnih katastrofa. Kontinuitet rada treba da se garantuje postojanjem rezervnih planova ili alternativnih riješenja. Korišćenje offline ili delimično offline riješenja koja se sinhronizuju sa blockchainom kada se konekcija ponovo uspostavi može biti jedna od ovih opcija. *Peer-to-peer komunikacione metode i redundantnost mrežne infrastrukture takođe se mogu koristiti za smanjenje uticaja prekida internet veze na aktivnosti blokčejna.* [29]

3.4. Sigurnosne karakteristike blokčejna

U pogledu bezbjednosti i integriteta podataka, blokčejn tehnologija pruža niz prednosti. Njegov transparentni, nepromjenljivi, decentralizovani dizajn i kriptografske bezbjednosne karakteristike nude čvrstu osnovu za zaštitu osjetljivih informacija i transakcija. Blockchain ima mogućnost da promjeni poslovanje i poboljša bezbjednost podataka u digitalnoj eri riješavanjem nedostataka konvencionalnih centralizovanih sistema. Blockchain tehnologija se pojavljuje kao održivo sredstvo za osiguranje povjerenja, transparentnosti i integriteta u digitalnom ekosistemu koji se stalno mjenja dok preduzeća traže nove načine da zaštite svoje podatke. Neke od sigurnosnih karakteristika blokčejn tehnologije su: [30]

- **Kriptografska bezbjednost:** Blokčejn tehnologija koristi kriptografske algoritme za zaštitu podataka i garantovanje anonimnosti. Informacijama snimljenim na blokčejnu mogu pristupiti i dekodirati samo ovlašćene strane zahvaljujući mehanizmima za šifrovanje, koji štite osjetljive podatke od ilegalnog pristupa. Podaci koji se čuvaju u blokčejnu dodatno su zaštićeni ovom kriptografskom bezbjednošću.

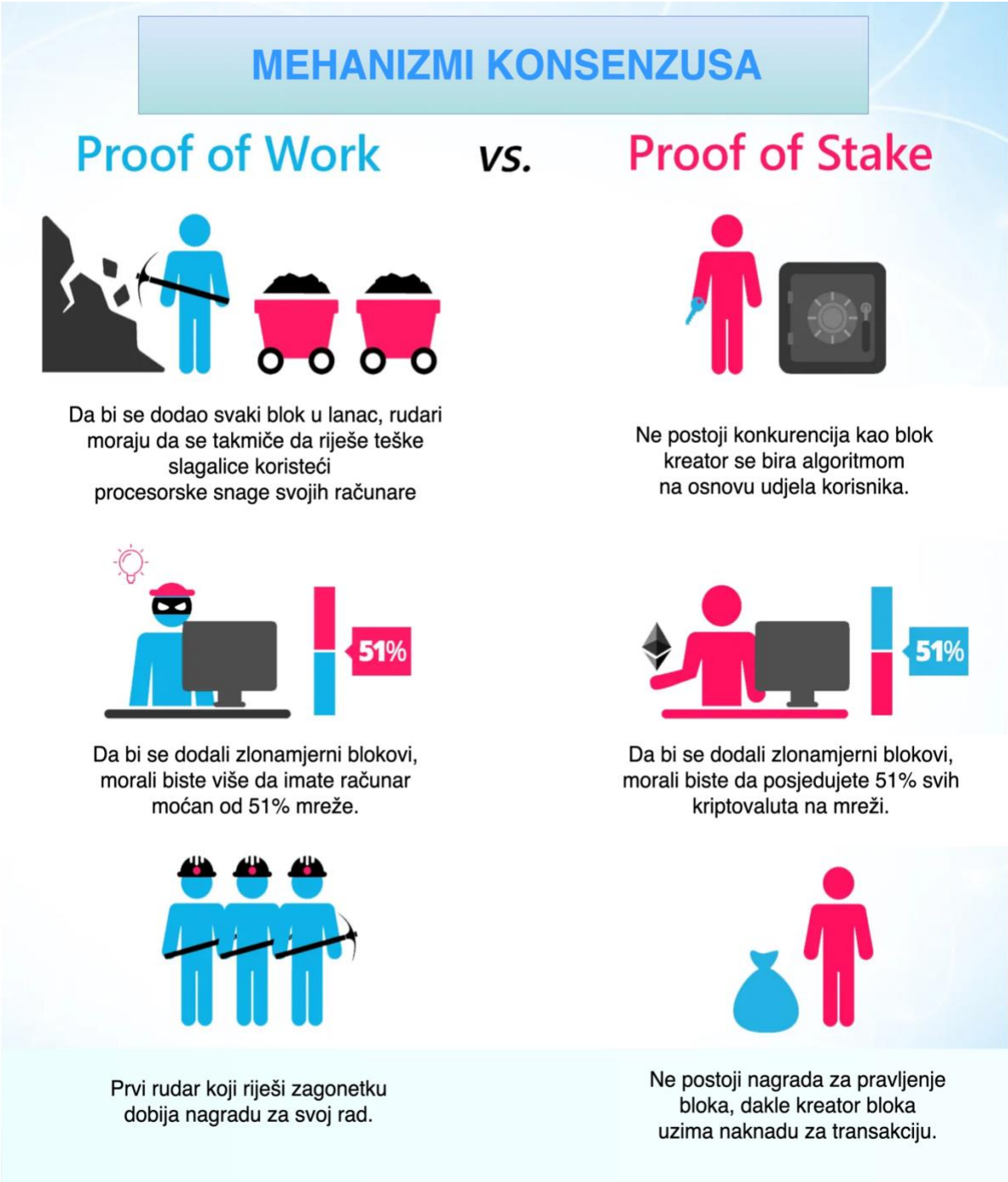
- **Tehnologija distribuirane knjige**: Zbog distribuirane prirode blockchaina, brojne verzije glavne knjige drže razni korisnici mreže. Zbog svoje suvišnosti, blockchain je otporniji na napade jer integritet sistema nije ugrožen ako je kompromitovan jedan čvor ili kopija. Srazlogom da su pojedinačne tačke kvara manje ranjive, to dodaje dodatni stepen zaštite.

- **Mehanizmi konsenzusa:** Blockchain se oslanja na brojne tehnike konsenzusa, uključujući Proof of Work (PoW)[13] i Proof of Stake (PoS)[14], kako bi potvrdio transakcije i zaštitio integritet mreže. Osiguravajući da se samo legitimne transakcije učitavaju u blok lanac, ove metode štite od lažnih aktivnosti i podržavaju sigurnost sistema. [31]

[13] POW je algoritam koji zahtjeva od računara, poznatih kao rudari, da riješe kompleksan matematički problem kako bi dodali novi blok u blockchain.

[14] POS je algoritam koji omogućava korisnicima da "ulože" svoje kriptovalute kao "udel" u mreži kako bi mogli da budu odabrani da dodaju blokove.

Slika 7: Razlika između PoW i PoS



(https://blockgeeks.com/wp-content/uploads/2019/05/proofofworkvsproofofstake-1.jpg.webp)

Obje PoW i PoS imaju svoje prednosti i mane, a što se tiče izbora, on zavisi od specifičnih zahtjeva i ciljeva blokčejn mreže. Neke kriptovalute čak koriste hibridne mehanizme konsenzusa koji kombinuju elemente i PoW i PoS da bi se postigla ravnoteža sigurnosti i efikasnosti.

4. ZAKLJUČAK

Ukratko, blockchain tehnologija ima dubok uticaj na bezbjednost podataka, predstavljajući i prednosti i moguće nedostatke. Njegov jak i pouzdan sistem upravljanja podacima potpomognut je aspektima kao što su poboljšana bezbjednost podataka, nepromjenljivost, transparentnost i decentralizacija. Blockchain tehnologija se odupire hakovanju i manipulisanju tako što obezbjeđuje tajnost, integritet i validnost korišćenjem kriptografskih protokola. Blockchain-ova decentralizovana struktura minimizira oslanjanje na pojedinačne tačke kvara, povećavajući sigurnost i otpornost podataka.

Prednosti blockchain tehnologije su jasne u njenom kapacitetu da poboljša povjerenje učesnika, promoviše transparentnost i ubrza procedure. Ima sposobnost da revolucioniše procedure bezbjednosti podataka tako što će promjeniti uspostavljene centralizovane metode u različitim poslovima. Pored toga, korišćenje blockchaina u upravljanju lancem snabdijevanja, zdravstvenim zapisima i finansijskim transakcijama obezbjeđuje integritet podataka i mogućnost revizije, poboljšavajući bezbjednost podataka u svim ovim oblastima.

Međutim, efekat blockchaina na bezbjednost podataka nije bez poteškoća. Korišćenje energije, regulatorne poteškoće i problemi skalabilnosti zahtjevaju pažljivo razmišljanje i kreativna riješenja. Pored toga, potrebna je primjena odgovarajućih ograničenja pristupa i tehnika za poboljšanje privatnosti zbog prijetnji privatnosti podataka, posebno u javnim blok-čejnovima. Organizacije moraju primjeniti proaktivne prakse bezbjednosti podataka, kao što su snažno upravljanje ključevima, dubinske revizije pametnih ugovora i pridržavanje preporučenih praksi kodiranja, kako bi u potpunosti iskoristile prednosti blokčejna uz ograničavanje rizika. Regulatorne agencije, učesnici u industriji i tehnološki stručnjaci moraju da rade zajedno na prevazilaženju pravnih pitanja i stvaranju okruženja koje podstiče primjenu blokčejn tehnologije

Sve u svemu, blockchain tehnologija ima blagotvoran uticaj na bezbjednost podataka jer pruža stabilnu i bezbjednu platformu za upravljanje podacima. Riješavanje ograničenja i poteškoća blokčejna je od suštinskog značaja za maksimiziranje njegovog potencijala kako se razvija. Možemo oblikovati budućnost u kojoj će podaci biti zaštićeni, pouzdani i dostupni u decentralizovanom i bezbjednom digitalnom okruženju prihvatanjem transformacionih moći blokčejna uz održavanje budnog pristupa zaštiti podataka.

5. PRAKTIČNI RAD

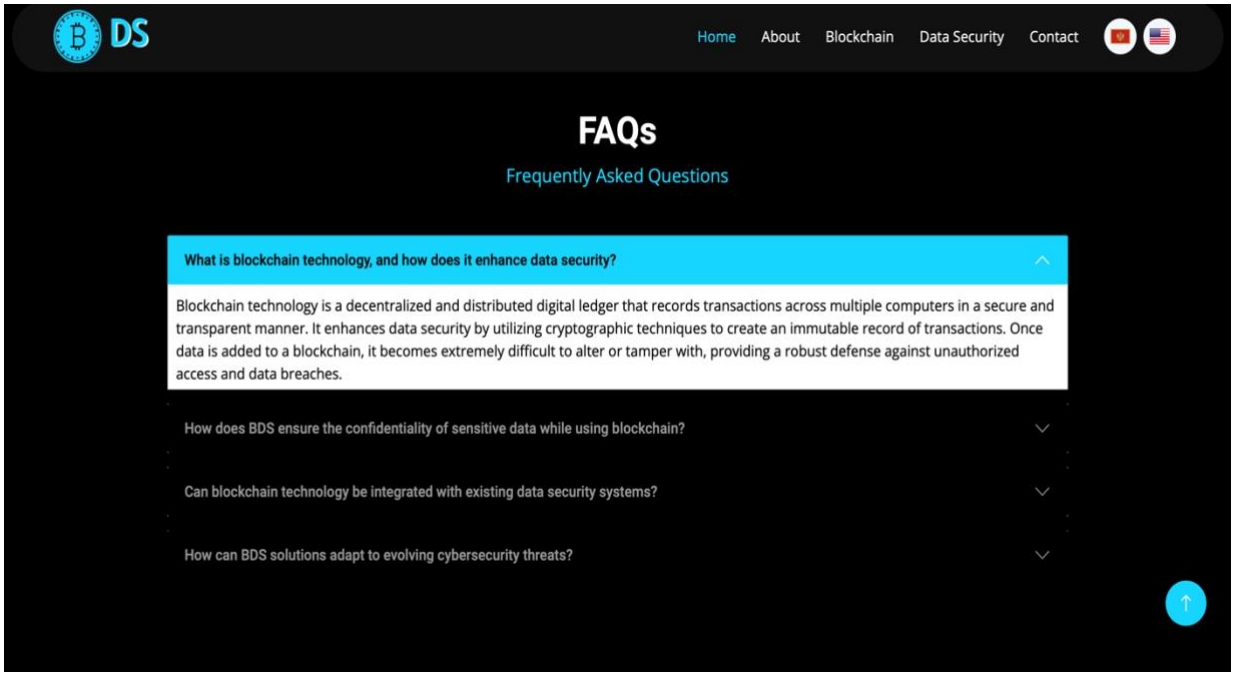
Webstranica pod nazivom „BlockchainDataSecurity (BDS)“ je kreirana da bi se demonstrirala upotreba blockchain tehnologije u bezbjednosti podataka kao dio praktične komponente ovog diplomskog rada. BDS webstranica funkcioniše kao interaktivna platforma koja posjetioce obavještava o važnosti blokčejna u zaštiti osjetljivih podataka i digitalne imovine.

5.1 Webstranica BDS

BDS websajt ima niz djelova koji ističu različite aspekte blockchain tehnologije i kako ona utiče na bezbjednost podataka. Webstranica isto tako počinje sa obrazovnim pregledom tehnologije blokčejna prije nego što se istraži potencijalna upotreba van kriptovalute. Naročito, webstranica ima sekciju „O nama“ koja elaborira cilj, znanje o blockchain-u i riješenja koje pruža BDS.

Websajt takođe pruža detalje o ključnim atributima BDS-a, kao što su njegova posvećenost jednostavnom usvajanju, bezbjednom skladištenju podataka, pristupačnosti i non-stop klijentskoj usluzi. Svaki element je ukratko objašnjen da bi se čitaocima pružila detaljna slika o prednostima koje BDS nudi.

Pored toga, BDS web-stranica sadrži još nekoliko sekcija, jedna od njih je posvećena „Bezbjednosti podataka“ koja naglašava potrebu zaštite privatnih informacija i opisuje ulogu BDS-a u postizanju ovog cilja. Sekcija pruža čitaocima informacije i edukativan pogled naglašavajući prednosti blockchain tehnologije u zaštiti podataka.



Jedna od njegovih najuočljivijih karakteristika je dio „Često postavljana pitanja“ na webstranicu BDS, gdje se daju odgovori na uobičajena pitanja vezana za blokčejn, bezbjednost podataka i BDS usluge. Korisnici mogu bolje razumjeti tehnologiju i njene posledice korišćenjem ovog sistema, koji im nudi sažete, ali korisne odgovore.

Uopšteno govoreći, BDS webstranica djeluje kao primjer iz stvarnog svijeta kako se tehnologija blokčejn može koristiti za poboljšanje bezbjednosti podataka. Dinamična platforma web-sajta prilagođena korisnicima ne samo da pokazuje potencijal blokčejna, već i pomaže ljudima da shvate kako se može koristiti u praktičnim situacijama.

Posjetite webstranicu BlockchainDataSecurity (BDS) da biste saznali više o tome kako se blockchain tehnologija koristi za bezbjednost podataka u stvarnom svijetu.

Saznajte kako razvoj blockchain-a može poboljšati zaštitu podataka i dati ljudima i kompanijama alate koji su im potrebni da zaštite svoju digitalnu imovinu.

Da biste posetili webstranicu BDS, kliknite na sledeći link:

https://diplomskirad.netlify.app/

LITERATURA

[1] *Šta je to Blockchaini kako ga možemo koristiti“,* Netokracija.rs od 15.08.2017. https://www.netokracija.rs/sta-je-to-blockchain-135366 (pristupljeno: 24.09.2023)

[2] Chris Burniske & Jack Tatar, (2018). *Cryptoassets The inovative investor's guide to Bitcoin and beyond*, Mc Graw-Hill, New York. ISBN: 978-1-26-002668-9

[3] https://startit.rs/uvod-u-blockchain/ (pristupljeno: 24.09.2023)

[4] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Bijela knjiga. Originalna bijela knjiga: https://bitcoin.org/bitcoin.pdf (pristupljeno: 24.09.2023)

[5] „*Blokčejin tehnologija: super jednostavan vodič za početnike“*, Blogovi o obrazovanju u XXI veku, 15.07.2018.

[6] Tapscott, D., & Tapscott, A. (2016). Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world. ISBN: 978-1101980132

[7] D'Aliessi, M., 2016. How Does the Blockchain Work?. [Online]. Dostupno na: https://medium.com/s/story/how-does-the-blockchain-work-98c8cd01d2ae (pristupljeno 24.09.2023)

[8] Fortney, L., 2018. Blockchain, Explained. [Online]. Dostupno na : https://www.investopedia.com/terms/b/blockchain.asp (pristupljeno: 24.09.2023)

[9] Smith, J. (2022). Blockchain Technology: A Paradigm for Data Management and Security. Journal of Information Security, 15 (2), 45-58.

[10] El Defrawy, K., & Youssef, A. (2018). Blockchain Security: Theory and Solutions. IEEE.

[11] Antonopoulos, A. M. (2014). Mastering Bitcoin: Unlocking Digital Cryptocurrencies. O'Reilly Media.

[12] A. Chauhan, O. P. Malviya, M. Verma and T. S. Mor, "Blockchain and Scalability," 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), Lisbon, Portugal, 2018, pp. 122-128, [doi: 10.1109/QRS-C.2018.00034].

[13] Academy, L., n.d. *How does Blockchain Work.* [Online] Pristupiti: https://www.lisk.io/academy/blockchain-basics/how-does-blockchain-work.

[14] Mahdi H. Miraz and Maaruf Ali, “Blockchain Enabled Enhanced IoT Ecosystem Security”, Proc. of the Int. Conf. on Emerging Technologies in Computing 2018 (iCETiC ‘18), Part of the Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering (LNICST), vol. 200, London, UK, 2018, pp. 38-46. Dostupno: https://link.springer.com/chapter/10.1007/978-3-319-95450-9_3

[15] Sato, Tatsuya, and Yosuke Himura. "Smart-Contract Based System Operations for Permissioned Blockchain." New Technologies, Mobility and Security (NTMS), 2018 9th IFIP International Conference on. IEEE, 2018.

[16] Kostić, Nikola & Sedej, Tomaz. (2022). Blockchain Technology, Inter-Organizational Relationships, and Management Accounting: A Synthesis and a Research Agenda. Accounting Horizons. 10.2308/HORIZONS-19-147.

[17] Sankomun, 2018. *Economic and Financial Affairs Committe*. [Online] Dostupno na: http://sankomun.com/ECOFIN_Study_Guide.pdf (pristupljeno: 17.09.2023)

[18] Lenhard, T. H. (2022). Data Security: Technical and Organizational Protection Measures against Data Loss and Computer Crime (1st ed.). Springer Wiesbaden. DOI: https://doi.org/10.1007/978-3-658-35494-7.

[19] Hua, Binjie & Wang, Zhe & Meng, Junying & Xi, HaiYan & Qi, RuiLi. (2023). Big data security and privacy protection model based on image encryption algorithm. Soft Computing. 1-13. [DOI: 10.1007/s00500-023-08548-4].

[20] Johnson, A. B., & Smith, J. D. (2023). Access control techniques and data security. Journal of Information Security, 15(3), 112-130.

[21] Ndung'u, Rachael. (2022). Blockchain as a Solution of Information Security and Data Privacy Issues: Review. International Journal of Computer Applications Technology and Research. 11. 337-340. [DOI: 10.7753/IJCATR1108.1007.]

[22] Brown, E. C., & Garcia, M. L. (2023). Challenges and Prospects in Addressing Contemporary Cyber Threats.. Journal of Cybersecurity Advances, 8(1), 45-62.

[23] Smith, E. L., & Johnson, R. M. (2023). Ensuring Data Security in the Digital Age: Strategies for Individuals and Organizations. Journal of Data Protection and Cybersecurity, 12(2), 75-90. [DOI: 10.78901/jdpc.2023.12.2.75].

[24] Olufohunsi, Temitope. (2019). DATA ENCRYPTION Olufohunsi, T.

[25] Pandya, D. et al. (2015) 'Brief History of Encryption', International Journal of ComputerApplications, 131(9), pp. 28–31. [doi:10.5120/ijca2015907390].

[26] Mohanty, S. P., & Jagadev, A. K. (Eds.). (2021). Blockchain Security in Cloud and IoT: Standardization, Advances, and Case Studies. CRC Press.

[27] Pal, Om & Alam, Bashir & Thakur, Vinay & Singh, Surendra. (2019). Key management for blockchain technology. ICT Express. 7. 10.1016/j.icte.2019.08.002. https://www.researchgate.net/publication/335325343_Key_management_for_blockchain_technology

[28] Tang, Xiangyan & Zhou, Ke & Cheng, Jieren & Li, Hui & Yuan, Yuming. (2021). The Vulnerabilities in Smart Contracts: A Survey. [DOI: 10.1007/978-3-030-78621-2_14].

[29] S. Simon. (March 1991). "Peer-to-Peer Network Management in an IB; SNA Network" IEEE Network Magazine, pp. 30-34.

[30] Nijalingappa, Pradeep & Ghonge, Mangesh & Lakshmi, Jaya. (2023). Blockchain: inherent security features of blockchain popularity and its security architecture. [DOI: 10.1016/B978-0-323-99481-1.00013-4].

[31] Lashkari, Bahareh & Musilek, Petr. (2021). A Comprehensive Review of Blockchain Consensus Mechanisms. IEEE Access. PP. 1-1. 10.1109/ACCESS.2021.3065880.

Izvori sa interneta:

https://www.isical.ac.in/~debrup/slides/Bitcoin.pdf

https://www.investopedia.com/terms/b/blockchain.asp#:~:text=changed%20without%20notice.-,Transparency,cryptocurrencies%20like%20Bitcoin%20for%20security

https://documents.uow.edu.au/~jrg/115/lectures/19dbsecurity/19dbsecurity.pdf

https://towardsdatascience.com/blockchain-technology-ensuring-data-security-immutability-7150d309352c

Lista slika i grafika:

Slika 1: Prikaz kako funkcioniše Blockchain?

Slika 2: Vizuelni prikaz funkcionisanja Blokčejn tehnologije

Slika 3: Potreba za Blockchain

Slika 4: Šifrovanje- algoritmi za transformaciju podataka

Grafik 1: Žalbe i gubici podataka u posljednjih 5 godina

Slika 5: Kontrola bezbjednosti podataka

Slika 6: Bezbjednost podataka i razvijanje tehnologije

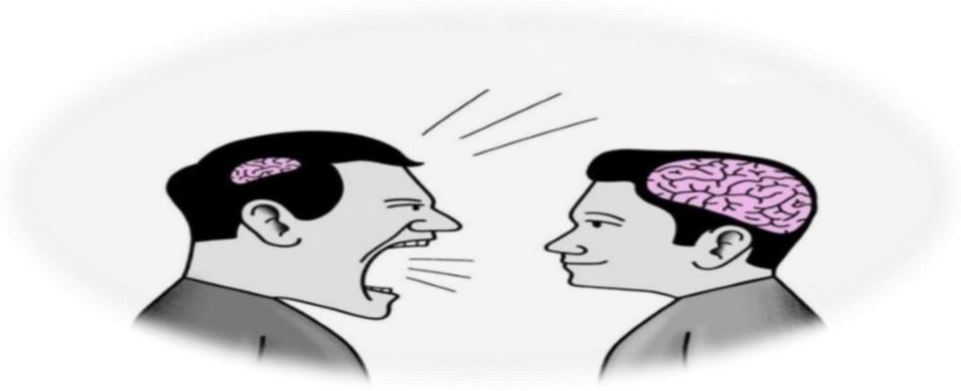
Slika 7: Razlika između PoW i PoS

Simboli i skraćenice

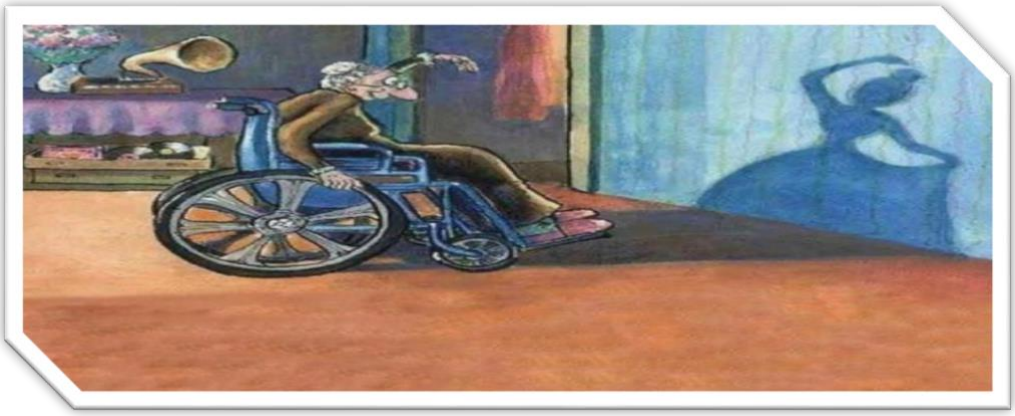
BC- Bitkoin
BT/BCHT- Blokčejn tehnologija
DF- DeepFake
P2P- Peer to peer
MFA- Multi-factor authentication
AI- Artificial Intelligence
IoT- Internet of Things
PoV- Proof of Work
PoS- Proof of Stake

ANEKS

SLIKE:



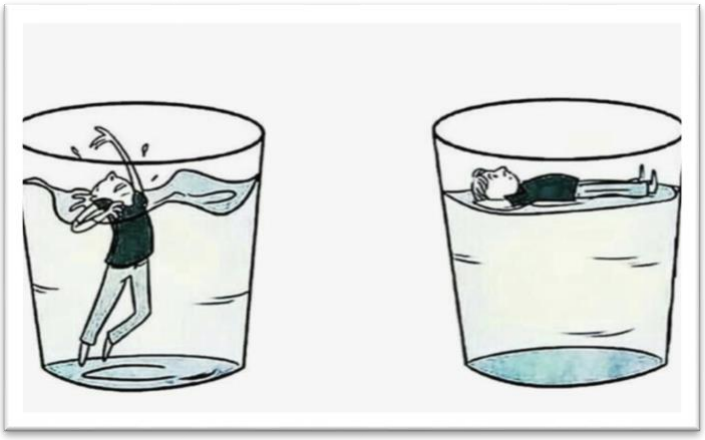
Što više znaš, to više što manje imaš da kažeš.



Nije važno kako nas drugi vide, važnije je kako mi sebe vidimo…

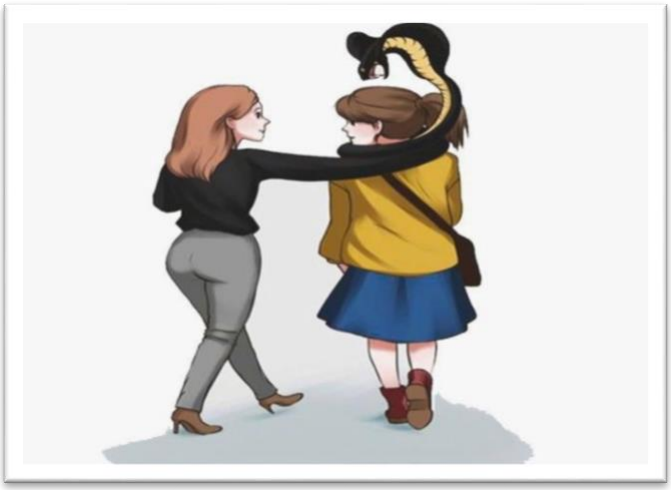
Kako mi vidimo svijet zavisi od toga kako mi želimo da ga vidimo.

Prestanite da premislite i prestanite da stvarate problem koje ne postoje.

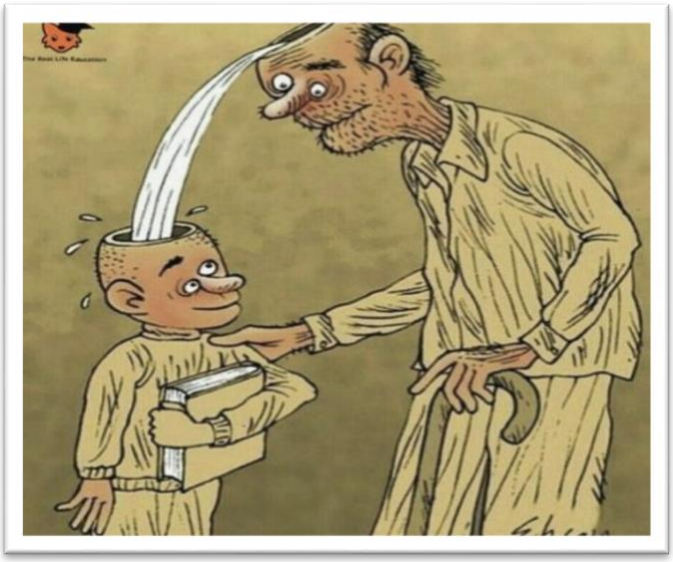


Vaša situacija je ništa, vaš odgovor je sve.

Tvoja usta možda je problem što ne možes da ideš dalje.



Nisu svi pravi sa nama…



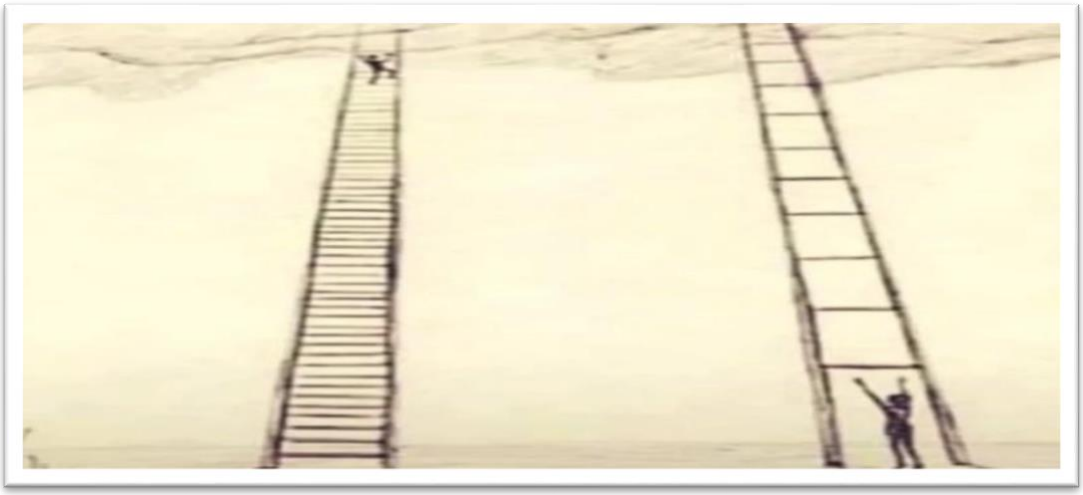
Uvijek imaj na umu da si uticaj na nečiji život.

Tvoje riječi su veoma važne, pazi šta govoriš...

Nikad ne govori loše riječi od gnjeva. Tvoj bijes će proći, ali riječi mogu da povrede osobe. Zato koristite dobre riječi ili ućuti.

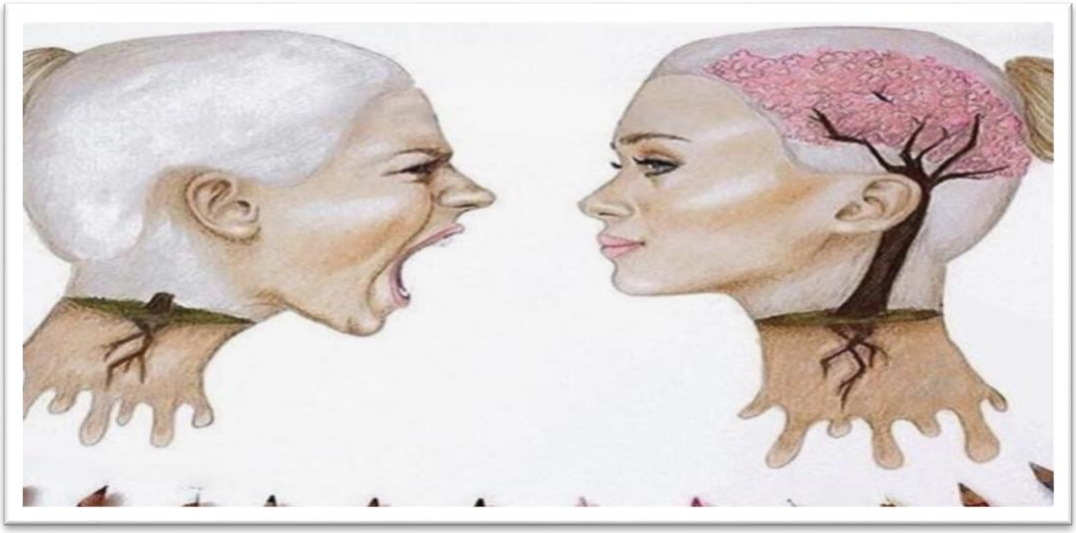
Bez obzira šta sa kojim se suočavaš u životu, Bog je još uvijek unutra kontrolu.

Ne treba da radimo dobro zbog pažnje, već zbog namjeru.



Ovdje vidimo koliko su važni mali koraci…

Nije loše biti drugačiji …



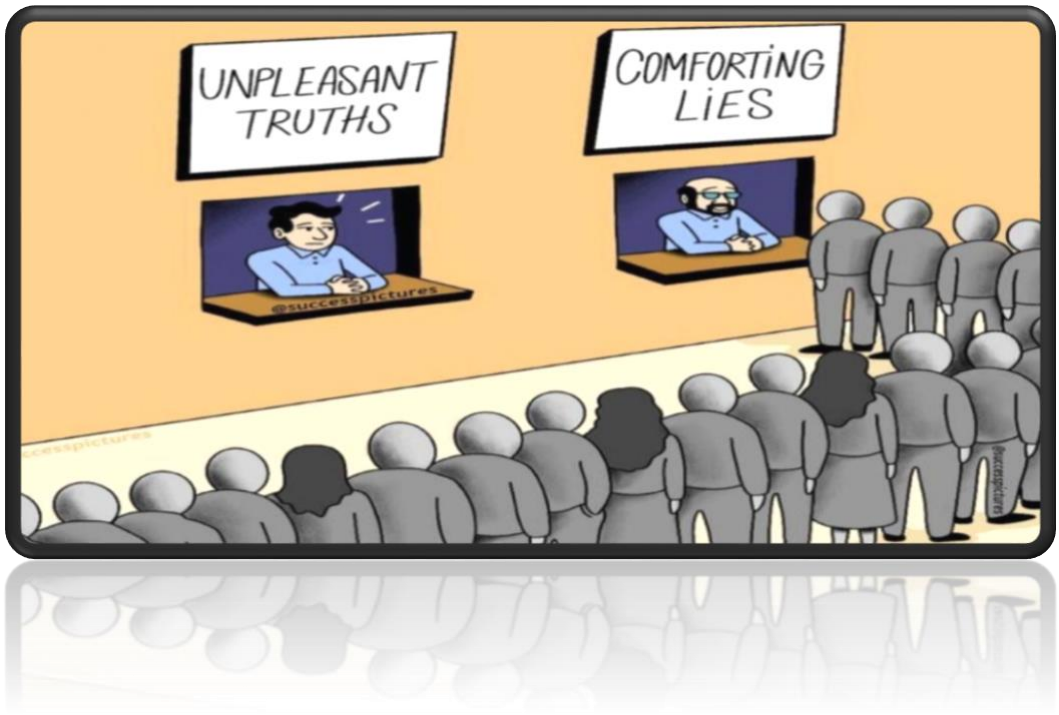
Unutrašnji rast mjenja našu stvarnost...

Shvatite kakav uticaj imate na generacije koje dolaze poslije vas…

Nije važno koliko resurse imate, ako ne znate kako da ih koristite, nikada neće vam biti dovoljno.

Vaš potencijal ne znači ništa, kada ne preuzmete akciju…

Prvi korak je uvijek najteži…



Nalazimo u periodu kada svi tražimo utehne laži i ne volimo neprijatne istine...

RIJEČI:

1. Računar - složeni je uređaj koji služi za izvršavanje matematičkih operacija ili kontrolnih operacija koje se mogu izraziti u numeričkom ili logičkom obliku
2. Svijet - zemaljsko stanje ljudskog postojanja
3. Papir je tanak pločasti materijal proizveden mehaničkom ili hemijskom obradom celuloznih vlakana dobijenih od drveta.
4. Deepfake – snimak ili slika koja je ubjedljivo izmjenjena da bi se pogrešnoprotumačilo šta neko radi ili govori.
5. Neuron – osnovna jedinica nervnog sistema
6. Opažanje – svojsvtveno tumačenje čulnih podataka
7. Percepcija – proces grupisanja čulnih utisaka
8. Učenje – proces sticanja navika, motornih vještina, znanja, intelektualnih vještina, stavova i crta ličnosti
9. Klasično uslovljavanje – učenje veze izmedju neutralne i bezuslovne draži koja za posljedicu ima uslovnu reakciju
10. Operativno učenje – opažajno uviđanje smisla
11. Kazna – averzivna draž koja dovodi koja dovodi do eliminacije ili supresije nekog ponašanja
12. Učenje uviđanjem – transfer ranije naučenih ponašanja i to naučenih posredstvom operativnog učenja
13. Učenje ugledanjem – učenje po modelu
14. Pamćenje – kognitivni proces primanja primanja, obrade, zadržavanja, aktivacije i upotrebe informacija
15. Zaboravljanje – nemogućnost reprodukcije, prepoznavanja, uštede pri ponovnom

učenju

16. Mišljenje - svaka svjesna mentalna aktivnost koja, umjesto stvarima, operiše

simbolima i predstavama

17. Test inteligencije – ispitivanje intelektualne razvijenosti pojedinca
18. Mentalni poremećaj – poremćaj funkcije mozga koji utiče na mišljenje, osjećanje i komuniciranje
19. Psihoza – mentalni poremećaj otuđenja osobe od realnosti
20. Anksioznost – osjećanje bojazni, strepnje i uznemirenosti
21. Potlačenost – obespravljenost ili potčinjenost
22. Introvertnost – otvoreni ka sebi, a zatvoren ka spoljnom svijetu
23. Ekstrovertnost – veliko interesovanje i otvorenost za ljude i stvari oko nas
24. Generalizacija - proces
25. Adaptacija - prilagođavanje uslovima okoline, razvijajući posebne osobine u pogledu svog ponašanja
26. Ljubav – ispunjenje životnog cilja
27. Tuga – tuga je osjećanje koje je okarakterisano gubitkom nekoga ili nečega
28. Samoaktualizacija – najviše ljudske potrebe i najviši nivo ljudskog razvoj
29. Odojče – stadijum razvoja djeteta u kojem u kojem, još uvijek, nema sposobnost hodanja i smislenog govora
30. Ljudsko pravo – određeno neotuđivo pravo koje stiče svako ljudsko biće po rođenju, nezavisno od pola, proijekla i pripadanja nekoj zajednici
31. Shizofrenija – mentalni poremećaj naglog prekida misaonog toka i burnopokretanje emocija
32. Psihologija – nauka o ponašanju i mentalnim procesima
33. Pedagogija – nauka koja proučava odgojne i obrazovne procese
34. Neurologija – medicinska disciplina koja se bavi poremećajima nervnog sistema
35. Psihijatrija – proučavanje i liječenje duševnih bolesti
36. Kognitivno – ono što se opažanjem saznaje

37. Motivi – činilac koji pokreće čovjeka na aktivnost
38. Anoreksija – oboljenje ljudskog organizma nastalo usljed neuhranjenosti
39. Bulimija – pretjerana potreba za hranom, patološka
40. Altruizam – nesebična briga za dobrobit drugih ljudi
41. Frustracija - osujećenje zadovoljavanja važnih motiva
42. Stav – gotovost psihe, usmjerenost ljudskog uma
43. Ličnost – neponovljiv, relativno čvrsto integrisan, stabilan i kompleksan psihički sklop
44. Fobije – Nerealni strahovi
45. San – Odmor duše i tije
46. Ego – ja
47. Superego – nad ja
48. Id - ono
49. Trauma – Negativno lično iskustvo koje ostavlja posljedice
50. Stres – Neminovnost savremenosti
51. Oporavak – Proces izlječenja koji donosi boljitak
52. Funkcionalizam –Psihološki pravac koji u nauci naglašava ulogu funkcije pojava
53. Geštalt – Psihološki pravac koji naglašava cjelinu
54. Bihejviorizam – Psihološki pravac koji naglašava ponašanje
55. Humanistička psihologija – Treća sila u psihologiji
56. Memorija – „prostor,, koji čuva naše životne priče Sreća – stanje afirmacije najviših vrijednosti
57. Nativizam – stav u filosofiji i psihologiji po kojem su neka znanja i sposobnosti urođeni
58. Vezivanje – razmjena djelova duša, poznanastva i ljubavi

59. Odrastanje – postajanje zrelom i odgovornom osobom
60. Diskriminacija – podištavanje ljudskog dostojanstva
61. Strast – kratkotrajni ali burni nalet emocija
62. Samoubistvo – lišavanje sebe prava na život
63. Sadizam – uživanje u nanošenju bola nekome
64. Mazohizam – potčinjavanje bolu
65. Ravnopravnost – uzajamno poštovanje stavova i životnih odluka
66. Homoseksualnost – istopolna ljubav
67. Inteligencija – sposobnost snalaženja u novonastaloj situaciji
68. Adrenalin – hormon nadbubrežnih žlijezda Interpretacija – viđenje situacije
69. Starenje – biološko sazrijevanje organizma
70. Život – proces stvaranja sreće i uživanja u istoj
71. Smrt – ponovno rađanje
72. Emocije – kvalitativna osobena rekcija bića na životnu situaciju
73. Emocionalna inteligencija – sposobnost razumijevanja sebe, drugih i uzajamnog odnosa
74. Temperament - kup urođenih predispozicija emocionalnog doživljavanja i reagovanja
75. Asertivnost – ponašanje u skaldu sa našim željama u svakoj situaciji izbjegavanje svađe
76. Terapija – proces ublažavanja ili otkljanjanja problema
77. EEG - elektroencefalografija
78. Mentalna bolest – Poremećaj funkcija mozga
79. Mentalna higijena – Naučna disciplina koja za cilj ima očuvanje mentalnog zdravlja
80. Opsesivno-kompulzivni poremećaj

81. Socijalizacija – Proces internalizacije i revizije socijalnih normi u cilju učenja društveno prihvatljivog ponašanja
82. Racionalizam – zastupa stav da je osnova znanja razum (um)
83. Primoravanje – efekat konteksta na kognitivnu obradu nekog materijala
84. Uviđanje – iznenadno uočavanje relevantnih odnosa među elementima stimulacija koje dovodi do željenog cilja ili ishoda (riješenje situacije/problema)
85. Afazija – poremećaji u govoru koji se javljaju kao posljedica moždanih povreda
86. Diferencijacija – razdvajanje usljed nastalih razlika
87. Psiha – um
88. Istorija - čitav niz prošlih događaja povezanih sa određenom osobom ili stvari
89. Žedan – onaj osjećaj koji imamo kada imamo potrebu da popijemo
90. Alergijska reakcija - javlja se kada imuni sistem osobe postane preosjetljiv na određene supstanc, kao što su hrana, polen, lijekovi ili pčelinji otrov...
91. Mortido – želja za smrću i samouništenjem
92. Sujeta – lažni ponos
93. Bezvrijednost – osjećaj da sopstveno biće nema nikakvu vrijednost
94. Ekstaza – doživljaj veoma snažne prijatnosti, povezan sa stanjem transa ili izmjenjene svijesti
95. Furor – afekt mržnje ili gnijev
96. Nestrpljivost – neprijatnost izazvana činjenicom da neka željka nije ostvarena
97. Šema- šira memorijska jedinica koja obuhvata organizovano znanje u čijem centru se, po pravilu, nalazi određeni pojam, ali i veliki broj drugih pojmova koji su sa njim u vezi
98. Samopouzdanje – osjećanje koje rezultira iz uvjerenja u sopstvenu sposobnost i istrajnost
99. Omraz – obostrana mržnja
100. Prezir – osjećanje koje subjekt osjeća prema nekome ko je svojim postupcima obezvrijedio neku od osnovnih ljudskih vrijednosti i time dokazao da je "nedostojno ljudsko biće"