



# Blockchain for Real World Applications

Rishabh Garg | BITS India | Founder & CEO, Scholars Park  
ISBN: 9781119903734

Published by:  
**John Wiley & Sons, Inc. New York, US**

Ta knjiga objašnja višestruki karakter tehnologije blockchain i njezine otpornosti na manipulaciju ekosistema do provođenja stvarnih djelatnosti, takvih kao obrazovanje, zaštita zdravlja, nekretnost, prijevoz, bankarstvo, poslovanje, upravljanje lancem opskrbe, elektronični trgovina i decentralizirane financije. Čitatelji otkriju potencijalne primjene tehnologije blockchain u svim važnim područjima života i nauče se služiti transakcijskim postupcima. Priča je transparentna, s zanimljivim primjerima iz stvarnog svijeta i pouzdanom objašnjenjem za čitatelje. Zbog jednostavnosti teme ova knjiga je korisna za svakog obrazovanog i poduzetnika.

*Indraneel Shankar Dani  
bivši dodatni glavni tajnik, zastupnik, Indija.*

Nalazimo se usred još jedne velike revolucije zvane BLOCKCHAIN, distribuirane baze podataka koja održava stalno rastući popis zapisa, zvanih blokovi. Ovaj krajolik inovacija predstavlja samo 12 godina rada elitne skupine štrebera, kriptografa i matematičara.

U vremenima koja dolaze, blockchain će prožimati svaku ljudsku težnju, čineći procese učinkovitima i pametnima. Kako se puni potencijal ovih prodora u društvu ostvaruje, stvari će se postupno početi događati drugačije - međunarodni prijenosi novca bit će brži i pouzdaniji; provjera će biti lakša; identitet će biti globalan, decentraliziran; i nijedna osoba - bilo administrator, menadžer, industrijalac, start-up, poslodavac, pružatelj usluga, pedagog, student ili korisnik, neće ostati nedirnuta. Očito je da će svijet morati raširenih ruku prihvatiti ovu tehnologiju.

S obzirom na to, autor čvrsto vjeruje da bi svaki dio društva trebao biti svjestan blockchaina, bilo da se radi o tehnolozima u početnicima, entuzijastima u početnicima ili netehničkim korisnicima decentraliziranih aplikacija. Ovaj članak, koji je izdvojen iz knjige, **'Blockchain za aplikacije u stvarnom svijetu'**, koju je napisao **Rishabh Garg**, a objavio *John Wiley & Sons Inc. SAD*, pruža dubinsko razumijevanje blockchain ekosustava, arhitekture, Ethereum, Hyperledgera i kriptovaluta. nakon čega slijedi sveobuhvatna rasprava o mogućim upotrebama blockchaina kao što su kriptografija, kibernetička sigurnost, upravljanje identitetom, provjera vjerodajnica, certifikacija poslova, zdravstvena skrb, daljinsko praćenje zdravlja, transplantacija organa, genomika, farmaceutski lanac opskrbe, hrana i civilne potrepštine itd. Snimke zaslona uživo i povezane kodne ćelije, koje se nalaze između teksta, pomoći će čitateljima da razumiju bankarstvo, poslovanje, decentralizirane financije, tržište predviđanja, upravljanje portfeljom, kvadratno financiranje, grupno financiranje, e-trgovinu itd. s *de novo* pristup.

Sadržaj pruža praktičan postupni mehanizam za svakog čitatelja da implementira vlastiti sustav za pohranu temeljen na sadržaju. Naš pristup je pomoći vam u upravljanju ovom revolucionarnom tehnologijom upoznavajući vas sa svakim njezinim detaljem. Uz ovu novu tehnologiju pod vašom kontrolom, moći ćete pristupiti značajkama blockchaina jednako lako kao da koristite jednostavnu mobilnu aplikaciju. Dakle, pridružite se blockchain revoluciji; naučite kako razvijati decentralizirane aplikacije; i biti ispred svojih vršnjaka.



**Rishabh Garg** | **BITS Indija** | Osnivač i izvršni direktor, Scholars Park radio je u Data Science za Indian Institute of Technology, New Delhi; brand partner s Cuvette; SDE sa ServiceNow, Swiggy i Ethan AI. Stekao je specijalizaciju iz Blockchaina na Sveučilištu Buffalo, NY; Applied Data Science with Python sa Sveučilišta u Michiganu, SAD; i upravljanje ulaganjima sa Sveučilišta u Ženevi, Švicarska (kroz MOOC).

Napisao je knjigu o **Blockchain for Real World Applications** (John Wiley & Sons Inc. US) i drugu o **Self Sovereign Identities** koja je objavljena na šest međunarodnih jezika u Njemačkoj, Francuskoj, Italiji, Moldaviji, Španjolskoj i Portugalu. Recenzent je časopisa pri IEEE Internet of Things i član programskog odbora te recenzent međunarodnih konferencija koje organizira AIRCC u Torontu (Kanada), Youngsu (Australija) i Londonu (UK).

Rishabh je dobitnik Nacionalne nagrade za iznimna dostignuća u inovacijama od predsjednika Indije i Nacionalne nagrade za inovacije CSIR od premijera Indije.

## BLOCKCHAIN: SKORA REVOLUCIJA

Knjigovodstvo je kamen temeljac civilizacije još od babilonskog doba jer je razmjena vrijednosti zahtijevala da dva stranca vjeruju računima jedan drugome. I dalje trebamo integrirani sustav koji može bilježiti sve naše transakcije, održavati društvo organiziranim i održavati povjerenje javnosti [Garg, 2023]. Čitaj više, [Blockchain for Real World Applications - Rishabh Garg, John Wiley & Sons, Inc. US, 01-388: ISBN - 9781119903734](#).

Tehnička arhitektura i protokoli **Distributed Ledger Technology** (DLT) omogućuju istovremeni pristup, provjeru i nepovratno ažuriranje podataka preko mreže koja obuhvaća više čvorova ili lokacija. Blockchain je jedan od njegovih mnogih oblika kao što su **DAG**, **Hashgraph**, **Holochain** i **Tempo** (Radix). Blockchain je skora revolucija i potpuno novi protokol za razvoj aplikacija. Poput interneta prije četvrt stoljeća, blockchain aplikacije mogle bi prožeti naš svakodnevni život u nadolazećim godinama [Garg, 2022].

Blockchain je u biti digitalna knjiga koja prati transakcije. Transakcije mogu označavati bilo što - gotovinu, digitalne valute, dionice ili bilo koju drugu imovinu. Blockchain može zadovoljiti širok raspon uvjeta za stjecanje ili namirenje te imovine putem takozvanih pametnih ugovora.

Način na koji se transakcije bilježe na više računala unutar decentralizirane mreže razlikuje blockchain od jednostavne knjige. Nakon što se postigne konsenzus, svaki čvor na mreži zajedno ažurira svoju kopiju glavne knjige. U nedostatku konsenzusa, ostatak mreže trenutno prestaje pokušavati dodati ili ukloniti čvor.

Blockchain koristi računovodstvo s trostrukim unosom, gdje se jedan unos vrši na kreditnoj strani, drugi na debitnoj strani, a treći u nepromjenjivoj zajedničkoj knjizi – kojom upravljaju napredni matematički algoritmi i neprobojna kriptografija. Čitaj više, [Blockchain for Real World Applications - Rishabh Garg, John Wiley & Sons, Inc. US, 01-388: ISBN - 9781119903734](#).

Blockchain je niz blokova koji čine sveobuhvatan popis transakcija koje se prenose i repliciraju preko mreže kao digitalna javna knjiga. Blockchain ekosustav sastoji se od **čvorova** – korisnika ili računala – koji održavaju potpunu kopiju zapisa ili glavne knjige, dok su **blokovi** formati

podataka koji se koriste za pohranu zapisa o transakcijama i njihov prijenos između svih čvorova u mreži [Garg, 2021].

Stuart Haber i W Scott Stornetta [1991] prvi su predstavili koncept blockchaina. Ali Satoshi Nakamoto, osoba iza pseudonima, popularizirao ga je 2008. kako bi mogao poslužiti kao javni dnevnik bitcoin transakcija. Programabilni pametni ugovori, konstitucionalni dizajn i blockchain konsenzusni protokol ključna su područja inovacija tijekom proteklog desetljeća i pol.

## **BLOCKCHAIN VREMENSKA TRAKA**

Tijekom proteklih 15 godina bilo je mnogo inovacija u blockchain tehnologijama konsenzusa, programabilnim pametnim ugovorima i fiducijarnoj arhitekturi.

### **BLOCKCHAIN 1.0**

Blockchain 1.0 korišten je kao digitalna valuta za trgovanje velikih razmjera, transakcije male vrijednosti, forex, igranje i pranje novca. Brojne su prednosti korištenja blockchain tehnologije za digitalnu valutu, ali njezina temeljna prednost je ta što pruža sigurnu i sigurnu platformu za prijenos imovine bez potrebe za posrednicima ili ugovornim stranama. Sada je dostupno više od 4500 različitih vrsta kriptovaluta. Najpopularniji su Bitcoin (2009), Litecoin (2011), Namecoin (2011), Dogecoin (2013) i Peercoin, s ukupnom tržišnom kapitalizacijom od 295 milijardi USD (2012).

### **BLOCKCHAIN 2.0**

Proširenje Blockchain 2.0 aplikacija omogućilo je pametne ugovore, decentralizirane aplikacije (dApps) i decentralizirane autonomne organizacije (DAO). Odigrao je ključnu ulogu u određenim područjima financija - bankarstvu, trgovanju dionicama, kreditnim sustavima, financiranju opskrbnog lanca, kliringu plaćanja, borbi protiv krivotvorenja, uzajamnom osiguranju i narušavanju tradicionalnih valuta i metoda plaćanja. Olakšao je implementaciju pametnih ugovora korištenjem nekih programabilnih jezika ugovora, uključujući Ethereum, Codius i Hyperledger.

### **BLOCKCHAIN 3.0**

Osim u valuti i financijama, Blockchain 3.0 uspio je uspostaviti dominaciju u područjima kao što su obrazovanje, zdravstvo, znanost, transport i logistika. Uključuje sofisticiraniju vrstu pametnog ugovora za stvaranje decentralizirane organizacijske jedinice koja stvara vlastita pravila i pruža znatnu autonomiju.

### **BLOCKCHAIN 4.0**

Blockchain 4.0 razvija se u poslovni ekosustav za mase. To je spoj blockchaina s najopsežnijim opcijama vrhunskih tehnologija budućnosti kao što su Internet of Things, računalstvo u oblaku, umjetna inteligencija i robotika. Ispitivanjem potencijala virtualnih lanaca blokova unutar jednog lanca blokova, sustav može zaraditi nesputanu skalabilnost. Blockchain 4.0 odnosi se na ideje i

rješenja koja racionaliziraju tehnologiju za poslovne potrebe, posebice industriju 4.0 i trgovinu. Blockchain tehnologija može se koristiti za poboljšanje različitih procesa uključujući upravljanje opskrbnim lancem, korporativni tijek rada, financijske transakcije, prikupljanje podataka IoT - a, nadzor zdravlja, upravljanje imovinom i kreditne sustave.

Stoga blockchain 4.0 obećava digitalnu arhitekturu koja kombinira automatizaciju, odgovornost i zaštitu privatnosti kako bi se stvorilo iskustvo bez problema u stvarnom svijetu [**Garg, 2021; 2023**].

## **BLOCKCHAIN ARHITEKTURA**

Blockchain provjerava valjanost transakcija tehnikom asimetrične kriptografije. Ovdje se koristi matematički proces poznat kao **hash funkcija** za pretvaranje bilo kojeg podatka u niz alfanumeričkih vrijednosti. To je proces koji se zove **enkripcija** koji kodira čitljiv tekst koji može pročitati samo osoba koja ima tajni kod ili ključ za dešifriranje. Postoje dva glavna oblika enkripcije - **asimetrična enkripcija** (javni ključ) i **simetrična enkripcija**. Simetrična enkripcija ima samo jedan privatni (tajni) ključ, a koriste ga sve strane u komunikaciji i za šifriranje i za dešifriranje.

Ovdje hash polja i šifrirani transakcijski podaci djeluju kao digitalni potpis. Izvorna kopija podataka i sigurni hash podataka šalju se primatelju. Primatelj izračunava novi hash koristeći izvorne podatke dobivene nakon dešifriranja sigurnog hash-a. Ako su oba ista, to znači da primljeni podaci nisu promijenjeni.

## **DECENTRALIZIRANI IDENTIFIKATOR**

**Decentralizirani ID -ovi** omogućuju peer-to-peer veze između dvije strane koje su globalno jedinstvene, uporne i pseudoanonimne. DID-ovi osiguravaju kontrolu vlasnika identiteta i suverenost nad identitetima jer ne ovise o centraliziranim registrima, vlastima ili dobavljačima identiteta. Budući da osoba može imati više DID-ova, teže ju je pratiti u svim njenim aktivnostima. Čitaj više, *Blockchain for Real World Applications - Rishabh Garg. John Wiley & Sons, Inc. US, 01-388: ISBN - 9781119903734*.

## **BLOCKCHAIN EKOSUSTAV**

Blockchain ekosustav je mreža korisnika koji dijele čvorove za zajedničke poslovne aktivnosti i svrhe. Svaki blockchain blok sadrži oko 1 MB podataka. Kada se popuni kapacitet podataka od 1 MB prvog bloka, informacije se kronološki pohranjuju u ovom bloku prije nego što se ponove u drugom bloku [**Garg, 2021**].

Svaki blok prima drugačiji hash koji točno odgovara nizu podataka u tom bloku kako bi se svi ti blokovi povezali u niz. Blok prima novi hash čak i ako unutar njega postoji manja promjena. Sustav se oslanja na decentralizirane baze podataka za kontrolu pojavljivanja podataka između entiteta putem P2P (peer-to-peer) mreže, gdje metode konsenzusa osiguravaju replikaciju preko čvorova mreže.

Pojedinačni čvorovi čine blockchain ekosustav, a svaki ima svoju kopiju glavne knjige. Čvorovi međusobno komuniciraju kako bi se dogovorili o zapisu glavne knjige, eliminerajući potrebu za središnjim tijelom ili bilo kojom trećom stranom za koordinaciju ili provjeru. Uz prijenos i provjeru dostavljenih podataka na blockchainu, čvorovi također pomažu u unosu novih podataka. Čin snimanja transakcija na novom bloku i njihovog dodavanja u postojeći lanac naziva se **rudarenje** i događa se kada svi čvorovi postignu konsenzus. U blockchainu, svaki blok ima svoj nonce i hash, kojem prethodi hash bloka u lancu.

Kriptografska hash funkcija generira hash u blockchainu, koji svaki ulazni niz pretvara u izlazni niz sa 64 znamenke. Nisu svi hashovi valjani. Hash bloka mora započeti s najmanje deset uzastopnih nula da bi bio kvalificiran na blockchainu. Svaki blok prima **nonce**, što je mala količina jedinstvenih podataka. Rudari se moraju neprestano baviti rudarenjem, što je proces stalne izmjene i raspršivanja podataka bloka u potrazi za funkcionalnim raspršivanjem. Kako bi pronašli valjani potpis (output), rudari moraju stalno mijenjati strukturu bloka (nonce) i koristiti puno električne energije. Što veću računsku snagu imaju, brže obrađuju različite sastave blokova kako bi pronašli dobar hash.

## JAVNI I PRIVATNI BLOCKCHAIN

Postoje tri glavne vrste blockchaine : javni, privatni i konzorcijski blockchain. Svaki korisnik koji želi sudjelovati u mrežnim transakcijama može to učiniti na **javnom blockchainu**, bez ograničenja. S druge strane, na **privatnim lancima blokova** samo čvorovi iz određene organizacije mogu sudjelovati u procesu konsenzusa. Stoga je također poznat kao dopušteni blockchain. **Consortium blockchain** je polu-privatna mreža istomišljenika za povećanje produktivnosti, odgovornosti i transparentnosti.

## BLOCKCHAIN KONSENZUS

Kako bi se postigao konsenzus o stanju blockchaine i osigurala valjanost transakcija, koristi se mehanizam otporan na pogreške, a naziva se **mehanizam konsenzusa**. U ovom slučaju, svaki član blockchain mreže dogovara trenutno stanje distribuirane knjige. Za dodavanje novog bloka u lanac, čvor mora izvršiti računalni zadatak, poznat kao **Proof-of-Work**. PoW je oblik konsenzusa koji koristi bitcoin mreža. Puno se energije gubi u ovim operacijama jer PoW zahtijeva od rudara izvođenje enormnih izračuna. **Proof-of-Stake** je manje energetska intenzivna alternativa PoW -u koja od rudara zahtijeva da dokažu da su legitimni vlasnici valute. Ovo se temelji na nelogičnoj premisi da je manja vjerojatnost da će korisnici s više valute napasti mrežu. Predloženo je nekoliko konsenzusnih algoritama za prevladavanje ove slijepe ulice, uključujući **PBFT, DPoS, Peercoin, Ripple, Tendermint itd.**

Kako bi se osigurala učinkovitost, sigurnost i pogodnost, neki su radnici predložili pohlepno teško promatračko podstablo (**GHOST**) pravilo odabira lanca. U ovom sustavu, grane se važu pomoću GHOST-a tako da rudari mogu odabrati najbolju granu koju će slijediti, a ne najduži plan grana [Simpolinski i Zohar, 2013].

## PROVJERA PLAĆANJA U BLOCKCHAIN-U

Postoje dvije moguće vrste potvrde plaćanja: Jednostavna potvrda plaćanja i Potpuna potvrda plaćanja.

Kao dio procesa **jednostavne provjere plaćanja** (SPV), tanki ili lagani klijent može preuzeti zaglavlje bloka, koje je puno lakše od cijelog bloka. Lakše je i korisnije za korisnika spremati samo jednu kopiju zaglavlja bloka iz najdužeg lanca dokaza o radu i dobiti podružnicu Merkle koja povezuje transakciju s blokom. Provjera je pouzdana sve dok pošteni čvorovi kontroliraju mrežu. Ali u trenutku kada napadač preuzme kontrolu nad mrežom, sustav postaje izložen.

Nasuprot tome, **potpuna provjera plaćanja** zahtijeva debeo ili težak novčanik, koji je potpuna kopija blockchaine. Ovi programi novčanika potvrđuju i prenose tuđe trgovine uz upravljanje vlastitim transakcijama korisnika. Kako bi se pružili personalizirani rezultati i odabrao blockchain s najboljim dokazom o radu, sve strane (svi čvorovi) na mreži moraju biti povezani. Stoga, ovisno o povezivosti, može proći nekoliko dana dok se blockchain mreža ne preuzme pomoću aplikacije bitcoin wallet. Čitaj više, [Blockchain for Real World Applications - Rishabh Garg. John Wiley & Sons, Inc. US, 01-388: ISBN - 9781119903734](#).

## KRIPTOVALUTE

**Kriptovalute**, poput Bitcoina, Ethera ili Litecoina, digitalni su tokeni kojima se trguje na blockchainu i koriste se za kupnju proizvoda i usluga. Tehnologiju blokovnog lanca koriste kriptovalute kako bi nadopunile prednosti javne knjige i sofisticiranog kriptografskog sigurnosnog sustava. Tijekom godina te su valute postale nevjerojatno popularne, što je dovelo do postojanja više od 18 000 kriptovaluta diljem svijeta s tržištem vrijednim 3,2 trilijuna dolara. Bitcoin trenutno vrijedi 3.120.210,68 INR.

## SCENARIJE

**Skripte** se smatraju jednim od temeljnih čimbenika u implementaciji sloja poslovne logike na blockchainu. Jednostavno rečeno, bitcoin transakcije su informacije koje odražavaju kretanje bitcoina iz jednog novčanika u drugi. Obično prva transakcija u novom bloku stvara novu valutu, ali je nikada ne troši. Kod ovih transakcija unos ostaje prazan i takav prazan unos naziva se **Coinbase transakcija**. Nagrada stvorena ovom transakcijom također se može distribuirati na jednu ili više adresa novčanika poput tipične bitcoin transakcije. Nakon što se pridonese određeni broj uspješnih blokova, nagrada se prepolovljuje za svaki uspješni blok dodan u blockchain, održavajući bitcoin kao resurs ograničene ponude, otporan na inflaciju.

Budući da Bitcoin nije oblik zakonskog sredstva plaćanja koje izdaje vlada, njegova je popularnost stvorila nove puteve za njegovu razmjenu za fiat novac, kao što su mjenjačnice kriptovaluta, bitcoin debitne kartice, bitcoin bankomati, Metal Pay i peer-to-peer mreža.

U početku se peer-to-peer kriptovaluta poznata kao Bitcoin koristila za redovite transakcije, no Bitcoin se s vremenom promijenio iz penija u sredstvo ulaganja kako je stjecao popularnost i povećavao mu se vrijednost.

Vjerovalo se da blockchain tehnologiji na kojoj je radila nedostaje skalabilnost jer sama po sebi nije bila u stanju upravljati velikim količinama transakcija. Tako je u kolovozu 2017. originalna kriptovaluta Bitcoin se podijelio u dvije različite kriptovalute, **Bitcoin Cash** i **Bitcoin SV**. U studenom 2018. kriptovaluta je doživjela još jedan fork, podijelivši se na **Bitcoin Cash ABC** i **Bitcoin Cash SV (Satoshi Vision)**. Budući da koristi izvorni Bitcoin Cash klijent, Bitcoin Cash ABC sada se naziva Bitcoin Cash.

Programeri mogu koristiti jezike pametnih ugovora kao što je CashScript kako bi omogućili složenije operacije korištenjem Bitcoin Casha nego s Bitcoinom . Bitcoin Cash može biti teška imovina, kao što su nekretnine, zlato ili druga fizička dobra, budući da Bitcoin ima ograničenje od 21 milijun kovanica, što korisnicima omogućuje da zadrže vrijednost u digitalnom obliku jako dugo.

## **ETHEREUM**

Ethereum je varijanta blockchaine koju je kreirao rusko-kanadski programer Vitalik Buterin i njegovi kolege. Ethereum je decentralizirana blockchain platforma koja je izgrađena sa zajedničkom globalnom infrastrukturom. Svaki čvor u mreži pokreće operativni sustav - Ethereum Virtual Machine, koji ima sposobnost razumijevanja i pokretanja programa poznatih kao pametni ugovori. Stoga Ethereum pojačava prednosti bitcoina blockchain omogućujući programerima pisanje koda koji emulira temeljnu funkcionalnost decentralizirane aplikacije ili dApp-a .

## **PAMETNI UGOVORI**

Pametni ugovor je aplikacijski kod pohranjen na određenoj adresi (adresa ugovora) na blockchainu. Aplikacije mogu implementirati rad pametnih ugovora, mijenjati njihova stanja i pokretati transakcije. Za izradu takvih ugovora koristi se specijalizirani programski jezik, kao što je Solidity ili Viper. Izjave poput "ako...onda" često se koriste za izvršenje ugovora. Čitaj više, [Blockchain for Real World Applications - Rishabh Garg. John Wiley & Sons, Inc. US, 01-388: ISBN - 9781119903734.](#)

## **HYPERLEDGER**

Hyperledger je globalni zajednički rad otvorenog koda koji pruža okvir, standarde, smjernice i alate potrebne za korištenje u raznim industrijama. Pozdravlja svakog člana zajednice sa znanjem programiranja ili interesom za doprinos razvoju izvornog koda. Kod može pregledavati, stvarati, modificirati ili distribuirati bilo koji programer na svijetu.

Samo oni subjekti ili pojedinci koji imaju autorizacijski certifikat mogu provjeravati transakcije na Hyperledger mreži. Tvrtke poput privatnih ili B2B koje ne žele svoje osobne podatke na

javnom blockchainu mogu koristiti ovu dopuštenu i ograničenu pristupnu blockchain mrežu – Ethereum Hyperledger .

## **DECENTRALIZIRANE APLIKACIJE**

U centraliziranom sustavu, aplikacijski softver može biti postavljen na jednu ili više središnjih lokacija, ovisno o veličini instalirane baze klijenata. Međutim, u decentraliziranom sustavu pametni se ugovori koriste kako bi se aplikacijskom softveru omogućilo neovisno pokretanje na peer-to-peer blockchain mreži, umjesto na jednom stroju. **Decentralizirana aplikacija** (dApp) čini front-end, blockchain back-end i middleware - softver koji povezuje to dvoje.

Iako dApps obećavaju da će riješiti mnoge glavne probleme s tradicionalnim aplikacijama, oni također imaju brojne nedostatke, kao što su zahtjevi za održavanjem, značajni troškovi performansi, zagušenje mreže itd.

## **BRIGA O IDENTITETU**

Identitet je središnji dio svih ljudskih aktivnosti. Valjani identitet preduvjet je za upis u školu, prijavu za posao, upravljanje bankovnim računom, dobivanje putovnice, potpisivanje ugovora ili pristup financijskom sustavu [Garg, 2019]. Međutim, više od milijardu pojedinaca, uključujući 21 milijun izbjeglica, još uvijek nema pravni identitet. To je zbog skrivenih troškova, intervencija posrednika i zamornih procesa.

## **IDENTITETI ŠIROM SVIJETA**

Ljudi diljem svijeta imaju različite oblike identiteta, kao što su putovnica za međunarodna putovanja, vozačka dozvola za upravljanje vozilom, biračka kartica za izbore, broj socijalnog osiguranja za vođenje evidencije o plaćama ili samozapošljavanju, itd. [Garg , 2020]. Povijest identifikacijskog sustava vjerojatno počinje 1803. godine, kada je Napoleon Bonaparte predstavio prvi identifikacijski sustav na svijetu.

Francuska vlada uvela je osobnu iskaznicu za radnike s ciljem da je koristi kao alat za transformaciju neograničenog društva Francuske Republike u dobro organiziranu policijsku državu kako radnici ne bi mogli migrirati na bolje poslove i veće plaće bez dopuštenja poslodavca. . Napoleonov ID plan bio je parabola za trgovinu ljudima i ropstvo u Rusiji ili istočnoj Europi, ali nije mogao napredovati zbog nedostatka radne snage i pojave organizacija za samopomoć tijekom svjetskih ratova [Lyon, 1994].

Do 20. stoljeća Njemačka je postala visoko demokratska, tolerantna i liberalna nacija sa sustavima socijalne skrbi, socijalnim osiguranjem i nacionalnim zdravstvenim službama. U takvom okruženju nacisti su bili opsjednuti ekonomskom vrijednošću radnika, zadržavanjem plaća, uklanjanjem štrajkaša i invalida. Nacisti su uveli radnu knjižicu za bilježenje radnog staža svakog zaposlenika, uključujući razdoblja otpuštanja i kršenja ugovora o radu. Njegov prikriveni motiv bio je identificirati štrajkaše, slabe, sramežljive, neraspoložene, seksualno promiskuitetne,



tajne prostitutke i podproletarijat. Naredba je odbijena tek 1941-42, kada se rat okrenuo protiv Njemačke [Gotz i Roth, 2004].

Kina je proširila nacističku radnu bilježnicu prilagodivši je u sustav nazvan dang -an dossier, koji je omogućavao prikupljanje osobnih dosjea iz školskih dana. Radnici nisu mogli započeti novo zanimanje sve dok im bivši poslodavac nije poslao dosje. Ovaj novi sustav bio je potpuno drugačiji od povijesnog sustava, Dang-e, koji je bio namijenjen za nadzor plemića.

Osim toga, u Kini je postojao takozvani domaći sustav registracije koji je sprječavao kineske radnike da se presele u drugo područje bez dopuštenja. U 1990-ima danganski sustav počeo se raspadati pod utjecajem sila koje proizlaze iz globalizacije. Strane tvrtke koje su ulazile u Kinu nisu vodile dang- an evidenciju i zapošljavale su ruralne migrante bez dang-an dosjea.

Suvremeno doba osobnih iskaznica počelo je s Drugim svjetskim ratom. Godine 1938. Ujedinjeno Kraljevstvo donijelo je Zakon o nacionalnom registru, prema kojem su svi stanovnici morali imati osobnu iskaznicu [Whitley i Hosein, 2009]. Godine 1940 francuska vlada iz Vichyja uspostavila je sustav osobnih iskaznica s Grčkom i Poljskom, koji je više-manje zadržan do danas. Izuzimajući nekoliko iznimaka, jedva da je ijedna država u svijetu s običajnim pravom usvojila mirnodopski sustav identifikacije.

Usvajanje osobnih iskaznica u Aziji odrazilo se na procvat nakon Drugog svjetskog rata. Vlada Hong Konga uvela je osobnu iskaznicu 1949 kako bi spriječila useljavanje iz kontinentalne Kine i ojačala svoj suverenitet. Tajvan 1949, Južna Koreja i Singapur 1960-ih slijedili su taj primjer pod izgovorom ekonomske transformacije.

## **SUVREMENI IDENTITETI**

U Sjedinjenim Američkim Državama, deveteroznamenasti broj socijalnog osiguranja (SSN) izdaje se svim građanima SAD-a, stalnim i privremenim stanovnicima starijim od 18 godina. Iako je prvotno bio namijenjen za identifikaciju pojedinaca u svrhe socijalnog osiguranja, sada je također koristi se za praćenje pojedinaca u svrhu oporezivanja. U praksi je postao de facto nacionalni identifikacijski broj zbog svoje široke primjene, poput otvaranja bankovnog računa ili podnošenja zahtjeva za vozačku dozvolu.

Broj socijalnog osiguranja uveden je u Kanadi, ali je okončan 2004. uvođenjem zaštite osobnih podataka i elektroničkog dokumenta kao pravih osobnih brojeva.

U Kolumbiji, svaka osoba tijekom djetinjstva dobiva osnovnu identifikacijsku iskaznicu koja se zove Tarjeta de Identidad koja uključuje datum rođenja i mali serijski broj. Svaki građanin nakon navršenih 18 godina ponovno dobiva iskaznicu državljanstva (Cedula de Ciudadanía), koja je neophodna u svim javnim i privatnim stvarima.

U Meksiku se identifikacijski broj zove Clave Única de Registro de Población (CURP). Iako razne druge osobne iskaznice, kao što je broj socijalnog osiguranja, koji dodjeljuje Instituto Mexicano del Seguro Social i Registro Federal del Contribuyente (RFC) koje dodjeljuje

Ministarstvo financija također su u modi, ali izborna kartica, Credencial de Elector ili Credencialdel INE, koju izdaje Instituto Nacional Electoral dodijeljeno je najveće priznanje.

Nacionalna osobna iskaznica, Documento Nacional de Identidad (DNI) izdaje Registro Nacional de las Personas u trenutku rođenja u Argentini, osim za useljenike koji dobivaju brojeve koji počinju s 92.000.000. Ovaj ID potreban je za podnošenje zahtjeva za kredit, otvaranje bankovnog računa i ostvarivanje prava franšize. Budući da su roditelji dužni prijaviti svoju djecu, siromašni, a posebno siročad, izostavljeni su.

Brazil ima dva sustava – prvi, Registro Geral (RG) koji je broj koji dodjeljuju države i neke organizacije kao što su oružane snage kao ovlaštenu nacionalnu iskaznicu. Budući da se oni dodjeljuju na državnoj razini, moguće je imati isti RG broj za dva građanina u različitim državama

Drugi sustav, Cadastro de Pessoas Físicas (CPF), federalni je i jedinstven, ali je izvorno stvoren za potrebe oporezivanja. U Brazilu su jedan ili oba broja potrebni za određene uobičajene zadatke, poput otvaranja bankovnog računa ili dobivanja vozačke dozvole.

Unutar Europskog gospodarskog prostora i Švicarske, Europska kartica zdravstvenog osiguranja izdaje se u svrhu zdravstvene zaštite. Ova kartica navodi kod koji se naziva identifikacijski broj. U Finskoj je osobni identifikacijski kod, henkilotunnas (HETU ili švedski – Personbeteckning) u modi od 1964. i koristi se za identifikaciju građana za državne i korporativne transakcije.

U Francuskoj se kod INSEE koji je nastao tijekom Vichyjevog režima koristi za identifikaciju, socijalno osiguranje, zapošljavanje i oporezivanje. U Njemačkoj su od 2007. samo decentraliziranu bazu podataka održavala društva za socijalno osiguranje, koja su dodijelila broj socijalnog osiguranja gotovo svakoj osobi. Nakon 2008. prijašnji brojevi poreznih datoteka zamijenjeni su novim identifikacijskim brojevima poreznih obveznika, Steuerliche Identifikacijski broj ili Steuer-IdNr. Fizičke osobe koje su istovremeno zaposlene i samostalne djelatnosti mogu dobiti dva matična broja poreznog obveznika. Odgovarajući broj za organizacije izdaje Savezni središnji porezni ured, a zove se Wirtschafts-Identifikationsnummer.

U Italiji se financijski kod (Codicefiscale) izdaje u formatu SSSNNYYMDDZZZZX u trenutku rođenja. SSS su prva tri suglasnika u prezimenu (ako nema dovoljno suglasnika prvi samoglasnik, koristi se X); NNN je prvo ime, od kojeg se koriste prvi, treći i četvrti suglasnik; YY su zadnje dvije znamenke godine rođenja, M je slovo pridruženo mjesecu rođenja, DD su zadnja dva slova rođenja; ZZZZ je specifični pozivni broj za općinu u kojoj je osoba rođena; X je znak parnosti koji se izračunava zbrajanjem slova na parnim i neparnim pozicijama. Slova mjeseca koriste se abecednim redom, ali se koriste samo slova od A do E, H, L, M, P, R do T (dakle, siječanj je A, a listopad R); Da bi se razlikovali spolovi, 40 se dodaje danu rođenja za žene; a za strance se umjesto općinskog koda koristi šifra za cijelu zemlju.

Gambija i Nigerija dodjeljuju 11-znamenasti identifikacijski broj svojim građanima koji se nazivaju nacionalni identifikacijski brojevi [NIMC, 2022].

Nacionalni identifikacijski broj u Zimbabveu je alfanumerički kod od jedanaest znakova kojim upravlja Ured glavnog registrara. Ima dvoznamenkasti prefiks koji označava okrug u kojem podnositelj zahtjeva prebiva; sljedećih šest znamenki predstavlja jedinstveni osobni kod podnositelja zahtjeva; a posljednje 2 znamenke su prefiks matičnog broja izvornih roditelja.

U Narodnoj Republici Kini osobna iskaznica od 18 znamenki u formatu RRRRRRRYYY-MMDDSSSC obavezna je za sve građane starije od 16 godina. RRRRRR je standardni kod za administrativnu podjelu okruga ili grada u kojem je vlasnik rođen; GGGGMMDD je datum rođenja nositelja; a SSS je sekvencijalni kod za razlikovanje ljudi s istim datumom rođenja i mjestom rođenja [Shaw, 1996; Perry, 1997]. Sekvencijalni kod je neparan za muškarce i paran za žene.

Indonezija je izbacila 16-znamenkasti RFID karticu s elektroničkim potpisom, skeniranjem šarenice, skeniranjem otiska prsta deset prstiju i putovnicom visoke rezolucije pod nazivom e-KTP (Electronic Kartu Tanda Penduduk) od 2012. Ovaj program je osmišljen na temelju UIDAI Indije.

Indija već desetljećima nastoji pružiti službeni identitet svim svojim građanima. Do sada su bezbrojne osobne iskaznice objavljene i poništene, što je dovelo do stanja fluktuacije i zbunjenosti među građanima [Garg, 2017]. Ograničenje postojećih ID-ova je to što služe samo u različite i ograničene svrhe. Nadalje, nije neuobičajeno pronaći odstupanja u profilu građanina među različitim repozitorijima, što uzrokuje zabunu i pogreške [Garg, 2018; 2019].

Ideju o biometrijski omogućenom jedinstvenom identifikacijskom broju (UID), ili Aadhaar, predložio je Odjel za informacijsku tehnologiju, Vlada Indije, s ciljem pružanja autentičnog identiteta svakom stanovniku Indije. Više od jedne milijarde građana uključeno je u shemu, na koju je dosad potrošeno procjenjuje se da je 130 milijardi INR (UIDAI, 2022). To je najveći svjetski biometrijski identifikacijski sustav koji ima za cilj pružiti identifikaciju svakom takvom stanovniku koji nema individualni identitet.



# Jedan Svijet - Jedan Identitet

RISHABH GARG - BITS INDIA

Kao odgovor, **Garg [2016 – 2023]** predstavio je ideju One World – One Identity, koja je usamljena alternativa višestrukim osobnim iskaznicama. Ovim globalno jedinstvenim višenamjenskim digitalnim identifikacijskim brojem može se upravljati uz pomoć najsuvremenije blockchain tehnologije.

Svakoj osobi koja živi na Zemlji može se dodijeliti 20-znamenasti identitet na određeni datum. To će omogućiti pojedincima da pohrane svoje vjerodajnice za prijavu i osobne podatke u novčanik ili aplikaciju poznatu kao IPFS [**Garg, 2021**]. Za dijeljenje datoteka, IPFS će koristiti decentralizirani, distribuirani peer-to-peer (P2P) mrežni model koji se može proširiti na više računala ili čvorova. Datoteke se mogu podijeliti u segmente i čuvati u mreži čvorova koji ih prate koristeći njihov hash. Izvorna datoteka može se rekonstruirati kada se cijela datoteka sastavi, na temelju hash vrijednosti svake komponente.

Za razliku od tradicionalnih protokola protokola ili centraliziranih imenskih prostora tradicionalnih Hyper-Text Transfer Protocol (HTTP), IPFS je sustav za pohranu temeljen na lokaciji. Kada se sustav za pohranu temelji na lokaciji, on prati hostove pomoću IP adrese ili druge logičke sheme adresiranja preslikane na poznato ime. Ako host promijeni svoje ime ili adresu, potrebno je ažurirati i tablicu usluge naziva.

Identifikator sadržaja potreban je u pohranjivanju adresa temeljenom na sadržaju kako bi se odredila točna lokacija datoteke. Umjesto logičke adrese, ovdje se podacima pristupa na temelju njihovog kriptografskog hasha, koji djeluje kao otisak digitalne datoteke. Mreža uvijek vraća isti sadržaj na temelju hasha, bez obzira na to tko i gdje je učitao datoteku. IPFS je decentralizirani način pohranjivanja datoteka, pri čemu se za upravljanje identitetom izvorni dokument može spremati na IPFS, dok se metapodaci ili hash njegovog sadržaja mogu pohraniti na blockchain poslužitelj.

Dodatni sloj sigurnosti također se može dodati biometrijskim rješenjima, kao što je otisak palca na pametnom telefonu, otisak prsta, geometrija šake, prepoznavanje glasa ili lica, termalno mapiranje, uzorci očiju – skeniranje mrežnice, skeniranje šarenice ili bilo koji drugi biometrijski protokol verifikacije. Biometrijski podaci mogu se spremati i obrađivati pomoću poslužitelja baze podataka, fizičkih tokena, šifriranih tokena ili oboje. Sigurni sustavi često pohranjuju biometrijske predloške na uređaju ili lokalno kako bi omogućili provjeru identiteta bez prijenosa osjetljivih biometrijskih podataka na drugi poslužitelj ili lokaciju na internetu.

Iako se interni mehanizam za biometrijsku autentifikaciju oslanja na tehnologiju, s korisnikove je točke gledišta nevjerovatno jednostavan i brz. Lakše je staviti prst na skener nego utipkati dugu lozinku s nekoliko posebnih znakova za trenutačno otključavanje računala. Većina biometrijskih metoda provjere autentičnosti koristi se samo s fizičkim aplikacijama; ne smijete prenositi ili



komunicirati biološke metrike online. Biometrijske podatke kao što su otisci prstiju, skeniranje šarenice, obrasci lica i drugi teško je rekonstruirati s trenutnom tehnologijom. Šansa da vaš otisak prsta odgovara tuđem je jedan prema 64 milijarde. Čitaj više, [Blockchain for Real World Applications - Rishabh Garg. John Wiley & Sons, Inc. US, 01-388: ISBN - 9781119903734](#).

Nedavno je otkriveno da se korištenjem blockchaina tradicionalni sastavni blokovi bilo kojeg modela dubokog učenja mogu pretvoriti u siguran sustav. To je arhitektura biometrijskog prepoznavanja koja koristi blockchain tehnologiju za pružanje pristupa otpornog na greške u distribuiranom okruženju. Štiti i model dubinskog učenja i biometrijski predložak i upozorava cijeli sustav kada se neovlašteno mijenja određena komponenta. Također olakšava prepoznavanje potencijalnih smetnji.

Biometrijski identifikacijski sustavi, koji kombiniraju biometriju i blockchain tehnologiju, mogu se koristiti za poboljšanje sigurnosti, postizanje konsenzusa u nestabilnim okruženjima i donošenje revizijskih odluka. Putem osobnog uređaja kao što je pametni telefon, korisnici mogu podijeliti svoj digitalni ID s pružateljem usluge čak i ako nisu fizički prisutni i još uvijek mogu pristupiti osnovnim uslugama bez ugrožavanja svoje privatnosti.

Bez izričitog dopuštenja korisnika, nijedna transakcija neće se izvršiti putem njegovih podataka. Dopuštajući korisniku da upravlja svojim osobnim podacima, sustav će biti interoperabilniji, korisnik će moći slobodno pristupiti podacima na više platformi i neće biti prisiljen koristiti samo jednu.

Budući da nema geografskih ograničenja za korištenje blockchain identiteta, korisnici mogu pristupiti i potvrditi svoj identitet iz bilo kojeg kutka svijeta. Blockchain će eliminirati potrebu za višestrukim korisničkim imenima i lozinkama omogućujući korisnicima da uživaju u samostalnom i šifriranom digitalnom identitetu.

Kartica s jedinstvenim brojem pohranjuje sve fizičke podatke građanina, bilo osobne, biometrijske, obrazovne, izvanškolske, strukovne, medicinske, pravne ili financijske, u zasebne silose, na potpuno šifriran način. Na taj će se način **One World - One Identity** pokazati učinkovitim u boljem obrazovanju, bankarstvu, investicijama, zdravstvu, shemama javne distribucije i drugim uslugama [Garg 2017].

## ŠIFRIRANJE

Enkripcija komunikacije omogućuje čitanje relevantnog sadržaja samo pravom pošiljatelju i namjeravanom primatelju poruke. Postoje tri glavne kategorije kriptografije – kriptografija s asimetričnim ključem, kriptografija s hash funkcijom i kriptografija sa simetričnim ključem.

Bilo je nekoliko prekretnica u povijesti kriptografije koje su postavile temelje suvremenih algoritama. Izraz "šifra" izvorno se odnosio na opću ideju za prijenos tajnih poruka koja je uključivala slova kao temeljnu komponentu. Jednostavna supstitucijska šifra, Cezarova šifra, Hillova šifra, Playfair šifra, Vigenereova šifra, transpozicijska šifra itd. neki su od poznatih

primjera. Playfair šifra u C-u može sigurno prenositi između svog izvora i odredišta bez curenja informacija pomoću enkripcije-dešifriranja.

Hilova šifra je poligrafska supstitucijska šifra temeljena na linearnoj algebri koju je utemeljio Lester S. Hill 1929. Može lako formirati koherentnu šifru kada se koristi s digrafima (blokovi od dva slova), trigrafima (blokovi od tri slova) ili bilo koje druge blokove više veličina. Također se može implementirati mnogo više kriptografskih algoritama, uključujući RSA algoritam, aritmetičku biblioteku višestruke preciznosti, GNU aritmetičku biblioteku višestruke preciznosti, kineski teorem podsjetnika i hash SHA-512 u Javi. Čitaj više, [Blockchain for Real World Applications - Rishabh Garg, John Wiley & Sons, Inc. US, 01-388: ISBN - 9781119903734](#).

## **KIBERSIGURNOST**

Cyber sigurnost štiti sustave i mreže od online prijetnji. Krajolik kibernetičkih napada posljednjih se godina brzo proširio. Napadači koriste zlonamjerni softver poput trojanaca, rootkita i virusa koji su poznati kao napadi distribuiranog uskraćivanja usluge (DDoS), napadi Čovjek u sredini (MITM), napadi krađe identiteta i napadi ransomwarea. Poduzeća diljem svijeta prihvatila su blockchain, koji se pojavio kao potencijalni alat za ublažavanje kibernetičke sigurnosti .

## **OBRAZOVANJE I ZAPOŠLJAVANJE**

Milijuni kandidata diljem svijeta predaju svoje akademske vjerodajnice svake godine u nadi da će ih regrutirati institucije visokog obrazovanja ili angažirati korporativne kuće. Velik broj kandidata preuveličava svoje obrazovanje prilikom svakog zapošljavanja.

Kako bi se očuvala autentičnost dokumenta, nositelj vjerodajnice može zadržati sve svoje vjerodajnice u svom Pi novčaniku i dijeliti ih s validatorima u šifriranom načinu pomoću Ethereum blockchaina. U skladu s Gargom [2021b] hash generiran nakon učitavanja vjerodajnica u IPFS može imati dva sloja enkripcije. Studentov javni ključ može se koristiti za izradu prvog sloja enkripcije, a potom privatni ključ izdavatelja može se koristiti za implementaciju drugog i trećeg sloja enkripcije (autorizacija). Bit će dekriptiran pomoću javnog ključa izdavatelja za provjeru dijeljene vjerodajnice. Proizvedeni šifrirani hash može se usporediti s onim pohranjenim u bazi podataka izdavatelja. Ako se oba podudaraju, vjerodajnica se može smatrati valjanom.

Često se u studentskoj svjedodžbi o uspjehu ne spominje nastavni plan i program ili metode podučavanja. Sprječava studenta da prenese svoje akademske bodove ili postignuća u učenju s jedne institucije na drugu. Potpuna evidencija kurikuluma, poučavanja, učenja i ocjenjivanja može se održavati davanjem pristupa svakom učeniku nadzornoj ploči za ocjenjivanje [Garg, 2021]. Poslodavci će moći odabrati najboljeg kandidata, ispitati njegovu prošlost i procijeniti popratne dokumente pod uvjetom da se kandidatova postignuća bilježe u svakoj fazi njegove/njezine akademske karijere na robusnoj platformi kao što je Blockchain. Kao takav, blockchain se može pokazati korisnim alatom za provođenje pozadinskih provjera kandidata te

uštedjeti vrijeme, novac i ljudske resurse. Čitaj više, [Blockchain for Real World Applications - Rishabh Garg. John Wiley & Sons, Inc. US, 01-388: ISBN - 9781119903734.](#)

## **ZDRAVSTVO**

Zdravstvene ustanove diljem svijeta bore se s problemima kao što su kašnjenja u kršenju podataka, izvor medicinskih potreština i zahtjevi za povratom za lijekove na recept. Blockchain nudi širok raspon primjena i prednosti u zdravstvu. Pomaže u upravljanju lancima opskrbe lijekovima, štiti prijenos medicinske dokumentacije pacijenata i pruža zdravstvenim istraživačima pristup biološkim i genetskim kodovima.

Korištenjem blockchaina, svi medicinski podaci o pacijentu, uključujući recepte, bilješke i laboratorijske rezultate, mogu biti dostupni u jednom prikazu. Svaki dio informacije može se pretvoriti u zasebnu hash funkciju. Svaka hash funkcija je zasebna i može se dijeliti samo uz dopuštenje vlasnika podataka. Dodatno, koristeći blockchain, moguće je pratiti artikl od točke njegove proizvodnje kroz svaku fazu opskrbnog lanca, dajući kupcu potpunu vidljivost i transparentnost nad proizvodima koje će kupiti. Korištenje tehnologije može ubrzati rješavanje zahtjeva za poslovne partnere i osiguravajuća društva, omogućiti policiji da istraži bilo koju sumnjivu aktivnost poput trgovine drogom ili gomilanja tijekom velikih hitnih situacija poput pandemije te povezati donatore organa, primatelje organa i zdravstvene ustanove kako bi se olakšalo presađivanje organa.

## **GENOMIKA**

Beskonačan broj genetskih podataka može se sigurno pohraniti na blockchain. Pretvara se u tržište na kojem pojedinci mogu trgovati svojim genetskim podacima. Teži stvaranju sveobuhvatnih baza podataka i pružanju vitalnih informacija znanstvenicima brže nego ikad prije. Za razliku od sadašnjih sustava, ako vlasnici podataka mogu uspostaviti kontakt s kupcima podataka izravno bez korištenja posredničkog poslovanja, troškovi analize mogu se smanjiti, a vlasnici podataka mogu ostvariti veću zaradu. Čitaj više, [Blockchain for Real World Applications - Rishabh Garg. John Wiley & Sons, Inc. US, 01-388: ISBN - 9781119903734.](#)

## **LANAC NABAVE**

Svakodnevno se proizvode i distribuiraju milijarde robe široke potrošnje kroz složene opskrbe lance koji dopiru do svakog kutka svijeta. Međutim, podaci o podrijetlu, proizvodnji i korištenju ovih proizvoda tijekom njihova životnog ciklusa ostaju nejasni. Svaki proizvod prolazi kroz razgranatu mrežu dobavljača, trgovaca, distributera, prijevoznika, skladišta i drugih objekata prije nego što se proda krajnjem kupcu, ali gotovo uvijek ostaju misterij tijekom ovog složenog putovanja.

Kao rezultat toga, kritična poslovna prepreka koja sprječava većinu organizacija da saznaju bilo što o svojim dobavljačima druge i treće razine je vidljivost opskrbnog lanca. Transparentnost i



vidljivost kroz različite kanale cijelog opskrbnog lanca može olakšati kretanje robe od sirovina do proizvodnje gotovih proizvoda, testiranja i distribucije.

Bolji rezultati mogu se očekivati od primjene blockchain tehnologije u opskrbnom lancu. Lanac opskrbe može koristiti zajedničku javnu knjigu temeljenu na konsenzusu za praćenje procesa podrijetla i proizvodnje proizvoda. U upravljanju opskrbnim lancem, životni ciklus, certifikacija i dokumentacija proizvoda mogu biti odmah dostupni svim stranama putem blockchainta. Od proizvođača do skladištenja, putovanja, distribucije i prodaje, proizvodi se mogu pratiti.

## **ZALIHA HRANE**

Velik dio hrane koju konzumiramo proizvodi se kroz zamršen globalni lanac opskrbe, što također povećava rizik od krivotvorenja, neovlaštenog mijenjanja, lažnog predstavljanja i namjerne zamjene. Globalni prehrambeni sektor svake godine gubi milijarde dolara zbog krađe hrane. Mlijeko, čaj, kava, voćni sok, maslinovo ulje, javorov sirup, školjke, med i mnoge druge namirnice uključene su u većinu kategorija hrane. Prosječna osoba ne može zamisliti svoj dan bez ovih namirnica.

Kako se globalni lanac opskrbe širi, sigurnost hrane postaje glavna briga i za potrošače i za regulatore. Prema Svjetskoj zdravstvenoj organizaciji, jedna od deset osoba pogođena je trovanjem hranom, što rezultira 33 milijuna godina zdravog života i 420 000 smrtnih slučajeva svake godine [Izješće WHO-a, 2019]. Uz to, bolesti izazvane hranom svake godine odnose živote 125 000 djece mlađe od pet godina. I ovdje je blockchain pouzdana alternativa koja može očuvati sljedivost nepromjenjivih dokumenata. Korištenjem blockchainta moguće je pratiti prehrambene proizvode na svim razinama, od farme do supertrgovina.

Blockchain također brzo uspostavlja svoju dominaciju u drugim industrijama osim upravljanja lancem opskrbe hranom. Iako većina vrhunskih tvrtki ima vrhunsku digitalnu infrastrukturu, uključujući softver za upravljanje lancem opskrbe (SCM) i planiranje resursa poduzeća (ERP), sustav još uvijek pokazuje analogne nedostatke kada se proizvodi prate od povezane proizvodne opreme (podrijetlo) do digitalne dostave obavijesti i RFID skeniranje. Čak ni najnapredniji strojevi ne mogu točno izračunati koliko će proizvod trajati. Tvrtke mogu koristiti blockchain tehnologiju za održavanje nepromjenjive digitalne knjige svih transakcija i kretanja u stvarnom vremenu za svakog člana mreže opskrbnog lanca. Čitaj više, [Blockchain for Real World Applications - Rishabh Garg. John Wiley & Sons, Inc. US, 01-388: ISBN - 9781119903734](#).

## **NEKRETNINA**

Od pamtivijeka su nekretnine bile pouzdana opcija ulaganja za bogate. Samo mali broj sredstava osigurava isti iznos rasta kapitala. Unatoč svemu tome, postoje mnoga ograničenja na globalnom krajoliku, poput pristupa potencijalnim sponzorima, financijerima i upraviteljima fondova; državljanstvo zemlje; priznavanje poslovnog nastana kupca, međunarodnih bankovnih računa, kreditnih rezultata, odgovarajućih sredstava, itd. Osim toga, svaki vlasnik nekretnine nepotrebno

troši ogromnu količinu novca na uknjižbu vlasništva, oslobađanje založnog prava i prijenos vlasništva u općinsku evidenciju kako bi osigurao svoja ulaganja.

Blockchain nudi svim igračima istu verziju istine o vlasništvu nad zemljom. Kao rezultat toga, postupci koji su često povezani s nekretninama, poput dvostruke prodaje, lažnih upisnika i zadiranja, mogu se eliminirati. Pametni ugovori mogu se koristiti za reguliranje transakcija nekretnina, uz smanjenje papirologije, posrednika i procjenitelja nekretnina.

## **IZBORNI PROCES**

Primarni cilj svake izborne vlasti je provedba izbora na pošten, pouzdan i transparentan način. Kako bi postigla ovaj cilj, birokracija bezobzirno troši milijarde dolara i baca milijune državnih službenika na izborne dužnosti. Blockchain tehnologija može biti učinkovita u tome da postupak glasovanja učini jednostavnim, glatkim i transparentnim.

To može pomoći ljudima da glasaju koji često ne iskoriste svoje pravo glasa, možda zato što žive u udaljenim područjima, nemaju pristup biračkim mjestima ili su potpuno nesposobni. Budući da koristi distribuiranu knjigu, glasači mogu glasati s bilo kojeg mjesta u svijetu bez žrtvovanja privatnosti. Olakšava glasačima da glasaju na dan izbora sjedeći kod kuće, bez stajanja u redu ili prolaska kroz pretjerane formalnosti.

Kada svaki građanin ima decentralizirani identitet, također poznat kao samo-suvereni identitet, distribuirana knjiga se može koristiti za bilježenje svih važnih događaja u njihovim životima. Građanima se može dopustiti sudjelovanje u izbornom procesu na temelju njihovih podataka, uključujući njihovo uobičajeno mjesto stanovanja (izborna jedinica u kojoj imaju pravo glasovanja), datum rođenja (kada navršše zakonsku dob za glasanje) i pod drugim uvjetima (ako ijedan). Birač može glasovati preko svog ID-a za prijavu, ali ne može ponovno koristiti isti decentralizirani identifikacijski broj na temelju kojeg je glasovao tijekom navedenih izbora. Odvajanjem glasova svake izborne jedinice pomoću softvera drugog dana glasanja, blockchain će zbrojiti glasove dane u korist svakog kandidata kroz različite čvorove.

Ipak, tajna je da svaki građanin zna da se oko procesa glasovanja i izbornih rezultata odvijaju mnoge neprijateljske i nezakonite aktivnosti. Nigdje u svijetu izborni proces nije potpun bez otimanja kabina, zamjene glasačke opreme na biračkim mjestima ili lažnih tvrdnji o glasanju. Vlade mogu biti oprezne s provedbom izbora temeljenih na blockchainu jer su to procesi koji se mogu u potpunosti provjeriti i koji političkim strankama ograničavaju mogućnosti manipulacije. Čitaj više, [\*Blockchain for Real World Applications - Rishabh Garg. John Wiley & Sons, Inc. US, 01-388: ISBN - 9781119903734.\*](#)

## **BANKARSTVO I FINACIJE**

Svrha stvaranja bankarskih institucija vjerojatno je bila omogućiti sve vrste trgovine i poslovanja okupljanjem ljudi. Blockchain udaljenim nepouzdanim stranama u bankarskom i financijskom sektoru olakšava postizanje konsenzusa o stanju baze podataka, bez pomoći vratara. Korisnici će

moći birati s kim i koliko žele dijeliti svoj identitet. Na blockchainu samo jednom trebaju unijeti svoj identitet. Ako pružatelji usluga koriste blockchain, nema potrebe da bilo koji korisnik ponavlja svoju registraciju.

Slično pouzdanom knjigovodi, upravlja svim financijskim transakcijama uključujući plaćanja, sustave namire, prikupljanje sredstava, upravljanje vrijednosnim papirima, zajmove, kredite i financiranje trgovine. U pogledu provjere identiteta, plaćanja, isplata, nagodbi, kredita i zajmova, prijenosa imovine, prijenosa između ravnopravnih korisnika, hedge fondova, sigurnosti i odgovornosti, uspio je nadmašiti tradicionalne sustave.

To može dramatično smanjiti naknade za transakcije, smanjenjem režijskih troškova koji nastaju prilikom ručnog postavljanja, izvršavanja i razmjene sredstava. Uklanjanje posrednika učinilo je procese, kao što su prekogranična plaćanja, trgovina i obračuni, bržima, pouzdanijima i jeftinijima.

## **FINANCIRANJE TRGOVINE**

Prijenos informacija, prijenos sredstava i proces plaćanja uvelike se oslanjaju na papirnatu poslovne operacije u financiranju trgovine. Ti bi ugovori mogli biti bolje objašnjeni u programskom jeziku Python nego pravnim kako bi ih trgovci mogli razumjeti. Stoga blockchain i pametni ugovori poslovnim ulagačima pružaju sigurno, otvoreno, transparentno, revizijsko i automatizirano transakcijsko okruženje. Ima potencijal transformirati financiranje trgovine pojednostavljuvanjem operacija pametnih ugovora, korporativnog planiranja resursa, munjevite mreže, procesa prije i nakon trgovanja, računa i revizija, programa vjernosti itd.

## **DECENTRALIZIRANE FINACIJE**

Decentralizirane financije (DeFi) financijska je tehnologija u nastajanju izgrađena na blockchainu. Prilično se razlikuje od drugih financijskih mreža jer je otvoren i programibilan. Pametni ugovori i uvjeti koji ih podupiru omogućuju mu automatski rad bez središnjeg autoriteta. Programerima omogućuje stvaranje novih modela plaćanja, ulaganja, kreditiranja, trgovine i razmjene neovisno o bankama i drugim institucijama.

U centraliziranim financijama, banka, financijska institucija ili tvrtka koja jamči transakciju posjeduje vaš novac. Uzimaju veliku dividendu od vašeg novca jer imaju veliku financijsku slobodu. U DeFi-ju, pametni ugovor djeluje kao transakcijska zamjena za financijsku instituciju. Nakon što počnu raditi, samo pametni ugovori su usklađeni. Ovi se ugovori ne mogu mijenjati jer su uvijek dizajnirani za automatizaciju.

Decentralizirani financijski protokoli omogućili su potrošačima diljem svijeta pristup širokom rasponu novih gospodarskih prilika. Pokriveno je upravljanje imovinom, tokenizacija, izvedenice tokena, decentralizirana autonomija, analiza podataka i vrednovanje, plaćanja, pozajmljivanje i pozajmljivanje, osiguranje, trgovanje maržom, tržišta, igre na sreću i uzgoj prinosa. Čitaj više, [Blockchain for Real World Applications - Rishabh Garg. John Wiley & Sons, Inc. US, 01-388: ISBN - 9781119903734.](#)

## **ETHEREUM KAO DEFI PLATFORMA**

Ethereum je inovativan ekonomski sustav vođen algoritmima kojeg pokreću povjerenje, prilike i financijski pristup. Može se iskoristiti za slanje novca, korištenje programabilne valute, pozajmljivanje ili posuđivanje novca, sudjelovanje u lutriji bez gubitka, trgovanje tokenima, kvadratno trgovanje, prikupljanje sredstava, grupno financiranje, upravljanje portfeljem itd. Osim toga, tržišta predviđanja također mogu imati koristi od Ethereum blockchaine na nekoliko načina - povećanjem pristupa, otporom cenzuri i uklanjanjem posrednika.

## **DISTRIBUIRANI RESURSI I IOT**

Blockchain pruža sigurniju pohranu podataka i upravljanje sa značajnim prednostima, nudeći jedinstvenu, interoperabilnu i zaštićenu arhitekturu za vlade, tvrtke, potrošače i IoT sustave upravljanja. Obavlja funkcije srednjeg i pozadinskog ureda na isti način na koji ih obavljaju internet i web front, automatizira zadatke za povećanje produktivnosti i otvara nove poslovne mogućnosti.

Povezivanje IoT sustava s blockchainom osigurava učinkovitost i sigurnost podataka IoT aplikacija. Algoritam se može kombinirati s novom tehnikom odabira voditelja kako bi se olakšalo korištenje blockchaine na IoT krajnjim uređajima s ograničenom dostupnošću resursa. IoT podaci koji se čuvaju u zajedničkoj knjizi lanca blokova omogućuju svim stranama praćenje podrijetla komponenti tijekom životnog ciklusa proizvoda. Sada je sigurno, jednostavno i ekonomično dijeliti sve relevantne informacije s regulatornim tijelima, pošiljateljima i proizvođačima. Čitaj više, [Blockchain for Real World Applications - Rishabh Garg, John Wiley & Sons, Inc. US, 01-388: ISBN - 9781119903734](#).

## **E-UPRAVA**

Unatoč činjenici da su mnogi geekovi pokušali riješiti sigurnosna pitanja u sustavima e-uprave, sigurnosni okviri i modeli uglavnom ne ispunjavaju sigurnosne zahtjeve. Budući da je nemoguće zanemariti nedostatak povjerenja u internetske transakcije i neovlašteni pristup insajdera sustavu, čini se da je implementacija blockchain tehnologije jedini način za rješavanje ovih nedostataka. To obećava učinkovitiju, sigurniju i sigurniju javnu uslugu.

Stotine blockchain inicijativa pokrenute su u više od trideset zemalja u proteklih četiri do pet godina kako bi zamijenile državne sustave. Estonija je usvojila ID s omogućenim blockchainom za provjeru identiteta građana. Blockchain tehnologija koristi se za izgradnju elektroničkih sustava glasovanja u Australiji i Ukrajini. U SAD-u se koristi za sigurno dijeljenje medicinskih podataka, au Ujedinjenom Kraljevstvu za poboljšanje javnih usluga. U Gruziji i Hondurasu zemljišni upis se vodi pomoću tehnologije distribuirane knjige. U bliskoj budućnosti, Kina sanja o izgradnji blockchain grada.

Automatizirani blockchain sustavi mogu omogućiti vladinim agencijama da djeluju učinkovitije, smanjujući trud, vrijeme i troškove koji su obično potrebni za ručno upravljanje pristupom njihovim mrežama. Osim toga, također može olakšati:

- održavanje pojedinosti o tijelu koje izdaje i provjerava;
- osiguranje dokumenata od neovlaštenog mijenjanja;
- stavljanje svih relevantnih informacija na raspolaganje tijelima putem javnog ključa;
- pristup osobnim podacima ili izvornim dokumentima bilo kada i bilo gdje putem privatnih ključeva korisnika;
- smanjenje prijevара, utaje poreza i nesavjesnog postupanja; i
- jačanje gospodarstva zemlje [Garg, 2020].

Čitaj više, [Blockchain for Real World Applications - Rishabh Garg. John Wiley & Sons, Inc. US, 01-388: ISBN - 9781119903734.](#)

## **DECENTRALIZIRAN STREAMING**

Video zapisi mogu biti zabavni, poučni i osnažujući. Međutim, emiteri koji prenose video na Internet moraju ga prvo transkodirati. Zauzima do 80% cjelokupne internetske širine pojasa, zbog čega je video streaming vrlo skup. Potrebna je video infrastruktura za pružanje skalabilnijih i troškovno učinkovitijih rješenja, a da bi se to ispunilo, tehnologije kao što je blockchain mogu programerima aplikacija na tržištu video transkodiranja omogućiti pristup širem rasponu distribuiranih procesora, koji su dostupni, sigurni i isplativi.

## **DVOJNO RUDARENJE**

Dvostruko rudarenje je praksa izvođenja različitih operacija na istoj opremi. Fraza se prvi put pojavila u kontekstu PoW rudarenja, gdje je opisivala istovremeno rudarenje više kriptovaluta korištenjem jednog GPU-a za pokretanje PoW algoritma za raspršivanje. Dvostruko rudarenje - korištenje GPU-a za rudarenje kriptovaluta poput Ethereuma, kao i njegovo korištenje za transkodiranje videa kao video rudara na vašoj vlastitoj mreži - još uvijek može biti moguće za video streaming. Jedna od prednosti korištenja transkodiranja kao dodatne aktivnosti dualnom rudarenju je ta što koristi manje GPU jezgri od drugih mogućih radnih opterećenja jer GPU hardverski koderi i dekoderi obavljaju većinu posla.

## **MREŽA KOJA SE SVE ŠIRI**

Blockchain mreža koja se stalno širi pokriva mnoge aspekte stvarnog svijeta, uključujući upravljanje ljudskim resursima, provedbu zakona, javnu pomoć, isporuku socijalne pomoći, poštanske usluge, račune i plaćanja, oporezivanje, lijekove, cijepljenje i zdravlje zajednice, nagodbu medicinskih zahtjeva, osiguranje, otpremu, teretni promet, javni prijevoz, putovanja i mobilnost, poziv za vožnju, zračni promet, internet stvari, informacije i komunikacije, slanje poruka, ugostiteljstvo, zabava, kockanje, hrana i piće, ribarstvo, stočarstvo, poljoprivreda i

prirodni resursi, infrastruktura i energija, proizvodnja, nekretnine, gradnja, vozila, oporuke i nasljedstva.

## U SUŠTINI

Blockchain ne obećava da će korisnika preko noći učiniti milijarderom niti nudi mehanizam za zaštitu njihovih finansijskih transakcija od politički inspiriranih vlada. Međutim, ono što je dokazano točno jest da nudi novi pristup strukturiranju administrativnih i gospodarskih organizacija, dok značajno smanjuje troškove povjerenja putem radikalnog, decentraliziranog pristupa glavnoj knjizi.

Čitaj više, [Blockchain for Real World Applications - Rishabh Garg. John Wiley & Sons, Inc. US, 01-388: ISBN - 9781119903734.](#)

## REFERENCE

- Rishabh Garg, 2016. [Generic Information Tracker](#). 2nd India International Science Festival, New Delhi India.
- Rishabh Garg, 2017. [Hi-Tech ID with Digital Tracking System](#), National Conference on Application of ICT for Built Environment.
- Rishabh Garg, 2018. [Digital ID with Electronic Surveillance System](#). Innovation registered with National Innovation Foundation, Autonomous Body of Department of Science & Technology, Government of India.
- Rishabh Garg, 2018. [Multipurpose ID: A Digital Identity to 1.34 Billion Indians](#). Ideate for India – Creative Solutions using Technology. National e-Governance Division, Ministry of Electronics & Information Technology, Government of India.
- Rishabh Garg, 2019. [Multipurpose ID: One Nation - One Identity](#), Annual Convention – Indian Society for Technical Education (ISTE). National Conference on Recent Advances in Energy, Science & Technology (39).
- Rishabh Garg, 2020. [Digital Identity and Access Management through Distributed Ledger Technology](#). Research Project, Department of Higher Education, Government of MP.
- Rishabh Garg, 2021. [Blockchain based Decentralized Applications for Multiple Administrative Domain Networking](#). BITS – Pilani, KK Birla Goa Campus India, 01-69.
- Rishabh Garg, 2021. [Blockchain based Identity Solutions](#). International Journal of Computer Science & Information Technology (In Press).
- Rishabh Garg, 2021. [Blockchain Ecosystem for Education and Employment Verification](#). 13th International Conference on Network & Communication Security, Toronto Canada.
- Rishabh Garg, 2021. [Digital Identity Leveraging Blockchain](#). Barnes & Noble, Basking Ridge, New Jersey US, 01-124.
- Rishabh Garg, 2021. [Distributed Framework for Real World Applications](#). Barnes & Noble, Basking Ridge, New Jersey US, 01-126.
- Rishabh Garg, 2021. [Global Identity through Blockchain](#). International Webinar on Blockchain. Scholars Park, India, 01-60.
- Rishabh Garg, 2021. [Samostoqtel'nye lichnosti: Cifrowaq identifikaciq s ispol'zovaniem blokchejna](#). Scienca Scripts, Russia, 01-108.
- Rishabh Garg, 2021. [Identidades auto-soberanas](#). Ediciones Nuestro Conocimiento, Spain, 01-104.

- Rishabh Garg, 2021. [Identidades de Soberania Própria](#). Edições Nosso Conhecimento, Portuguese, 01-104.
- Rishabh Garg, 2021. [Identità auto sovrane](#). Edizioni Sapienza, Italy, 01-104.
- Rishabh Garg, 2021. [Identités auto-souveraines](#). Editions Notre Savoir, France, 01-104.
- Rishabh Garg, 2021. [Interplanetary File System for Document Storage and e-Verification](#). 2nd International Conference on Software Engineering, Security & Blockchain, Sydney Australia.
- Rishabh Garg, 2021. [Self Sovereign Identities](#). Lambert Academic Publishing, Germany, 01-78.
- Rishabh Garg, 2021. [Souveräne Identitäten](#). Verlag Unser Wissen, Germany, 01-104.
- Rishabh Garg R, 2022. [A Technological Approach to Address Deficiencies in UID \(Aadhaar\)](#). 3rd International Conference on Big Data, Blockchain and Security, Copenhagen Denmark.
- Rishabh Garg, 2022. [Decentralized Transaction Mechanism based on Smart Contracts](#). 3rd International Conference on Blockchain and IoT, Sydney Australia.
- Rishabh Garg, 2022. [Distributed Ecosystem for Identity Management](#). Journal of Blockchain Research. 1(1): 51-63.
- Rishabh Garg, 2022. [Ethereum based Smart Contracts for Trade and Finance](#). International Conference on Blockchain and Smart Contracts, Bangkok Thailand. International Journal of Economics and Management Engineering, 16 (11): 619-629.
- Rishabh Garg, 2023. [Blockchain for Real World Applications](#). John Wiley & Sons, Inc. US, 01-388.
- Gotz A and Roth KH, 2004. The Nazi Census Identification and Control in the Third Reich Temple University Press, Philadelphia, 43.
- Lyons M, 1994. Napoleon Bonaparte and the legacy of the French Revolution, Macmillan Houndmills, Basingstoke, Hampshire, 119.
- Sompolinsky Y and Zohar A, 2013. Accelerating Bitcoins Transaction Processing. Fast Money Grows on Trees, Not Chains. IACR Cryptology e-Print Archive, 881.