



# Blockchain for Real World Applications

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

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

knygoje paaiškinamas daugialypis blokų grandinės technologijos pobūdis ir jos klastojimui atspari ekosistema, skirta realiai veiklai, tokiai kaip švietimas, sveikatos priežiūra, nekilnojamasis turtas, transportas, bankininkystė, verslas, tiekimo grandinės valdymas, elektroninė prekyba ir decentralizuoti finansai, vykdyti. Skaitytojai atras potencialų blokų grandinės technologijos panaudojimą visose svarbiose gyvenimo srityse ir išmoks valdyti sandorių procedūras. Pasakojimas yra aiškus, su puikiu meno kūriniu ir tikrai sužavės skaitytojus. Paprasta sudėtingo dalyko tvarkymas, ši knyga yra kiekvieno mokslininko ir verslininko lobis.

*Indraneel Shankar Dani*  
*buvęs papildomas vyriausiasis sekretorius, parlamento narys, Indija.*

Esame dar vienos didelės revoliucijos, vadinamos BLOCKCHAIN, įkarštyje - paskirstytoje duomenų bazėje, kurioje saugomas vis didėjantis įrašų, vadinamų blokais, sąrašas. Šis inovacijų peizažas reprezentuoja tik 12 elito geekų, kriptografų ir matematikų grupės darbo metų.

Ateityje **blockchain** persmelks visus žmogaus siekius, todėl procesai bus efektyvūs ir protingi. Visuomenėje išnaudojant visą šių proveržių potencialą, viskas pamažu ims vykti kitaip - tarptautiniai pinigų pervedimai bus greitesni ir patikimesni; patikrinimas bus lengvas; tapatybė bus globali, decentralizuota; ir joks asmuo – administratorius, vadovas, pramonininkas, startuolis, darbdavys, paslaugų teikėjas, pedagogas, studentas ar vartotojas neliks nepaliestas. Akivaizdu, kad pasaulis turės priimti šią technologiją išskėstomis rankomis.

Atsižvelgdamas į tai, autorius tvirtai tiki, kad apie blokų grandinę turėtų būti supažindinta kiekviena visuomenės dalis, nesvarbu, ar tai būtų pradedantysis technologas, ar startuolių entuziastas, ar netechninis decentralizuotų programėlių vartotojas. Šis straipsnis, ištrauktas iš knygos **Blockchain for Real World Applications**, kurią parašė **Rishabh Garg** ir išleido **John Wiley & Sons Inc. USA**, suteikia išsamų supratimą apie **blockchain** ekosistemą, architektūrą, Ethereum, Hyperledger ir kriptovaliutas, po to sekė išsami diskusija apie galimus blokų grandinės panaudojimo būdus, tokius kaip kriptografija, kibernetinis saugumas, tapatybės valdymas, įgaliojimų tikrinimas, darbo sertifikavimas, sveikatos priežiūra, nuotolinė sveikatos stebėseną, organų transplantacija, genomika, vaistų tiekimo grandinė, maisto ir civilinės paskirties tiekimas ir kt. Tiesioginės ekrano kopijos ir susijusios kodo ląstelės, pateiktos tarp teksto, padės skaitytojams iš naujo suprasti bankininkystę, verslą, decentralizuotus finansus, prognozavimo rinką, portfelio valdymą, kvadratinį finansavimą, sutelktinį finansavimą, el. prekybą ir kt. metodus.

Turinys suteikia praktinį žingsninį mechanizmą kiekvienam skaitytojui, kad galėtų įdiegti savo turiniu pagrįstą saugojimo sistemą. Mūsų požiūris yra padėti jums valdyti šią revoliucinę technologiją, supažindindami jus su kiekviena jos smulkmena. Naudodami šią naują technologiją galėsite pasiekti blokų grandinės funkcijas taip pat lengvai, kaip ir naudodami paprastą mobiliąją programėlę. Taigi, prisijunkite prie blockchain revoliucijos; išmokti kurti decentralizuotas programas; ir aplenkite savo bendraamžius.



**Rishabh Garg** | **BITS Indie** | Scholars Park įkūrėjas ir generalinis direktorius darbo duomenų mokslų srityje Indijos technologijos institute Naujajame Delyje; prekės ženklo partneris su Cuvette; SDE su ServiceNow, Swiggy ir Ethan AI. Bafalo universitete, NY, jis įgijo Blockchain specializaciją; Taikomoji duomenų mokslas su Python iš Mičigano universiteto, JAV; ir investicijų valdymas iš Ženevos universiteto, Šveicarija (per MOOC).

Jis parašė knygą **Blockchain for Real World Applications** (John Wiley & Sons Inc. US) ir kitą knygą **Self Sovereign Identities**, kuri buvo išleista šešiomis tarptautinėmis kalbomis Vokietijoje, Prancūzijoje, Italijoje, Moldovoje, Ispanijoje ir Portugalijoje. Jis yra IEEE Internet of Things žurnalo teisėjas ir programos komiteto narys, dalyvaujantis tarptautinių konferencijų, kurias AIRCC organizuoja Toronte (Kanada), Youngs (Australija) ir Londone (JK), apžvalgininkas.

Rishabh yra apdovanotas **Indijos prezidento** Nacionaliniu apdovanojimu už išskirtinius pasiekimus inovacijų srityje ir Indijos **ministro pirmininko** Nacionalinį CSIR inovacijų apdovanojimą.

## Bloko Grandinė: Neteisianti Revoliucija

Buhalterija buvo civilizacijos kertinis akmuo nuo Babilonijos eros, nes vertės mainams reikėjo dviejų nepažįstamųjų pasitikėti vienas kito sąskaitomis. Mums vis dar reikia integruotos sistemos, kuri galėtų registruoti visus mūsų sandorius, išlaikyti organizuotą visuomenę ir palaikyti visuomenės pasitikėjimą [Garg, 2023]. Skaityti daugiau, [Blockchain for Real World Applications - Rishabh Garg. John Wiley & Sons, Inc. US, 01-388: ISBN - 9781119903734](#).

Techninė **Distributed Ledger Technology** (DLT) architektūra ir protokolai leidžia vienu metu pasiekti, patikrinti ir negrįžtamai atnaujinti duomenis tinkle, apimančiame kelis mazgus ar vietas. Blockchain yra viena iš daugelio formų, tokių kaip **DAG**, **Hashgraph**, **Holochain** ir **Tempo** (Radix). Blockchain yra neišvengiama revoliucija ir visiškai naujas programų kūrimo protokolas. Kaip ir internetas prieš ketvirtį amžiaus, blockchain programos ateinančiais metais gali persmelkti mūsų kasdienį gyvenimą [Garg, 2022].

Blockchain iš esmės yra skaitmeninė knyga, kuri seka operacijas. Sandoriai gali reikšti bet ką – grynuosius pinigus, skaitmenines valiutas, akcijas ar bet kokią kitą turtą. „Blockchain“ gali patenkinti daugybę terminų ir sąlygų, susijusių su šio turto įsigijimu ar atsiskaitymu per vadinamąsias išmaniąsias sutartis.

Tai, kaip operacijos įrašomos keliuose kompiuteriuose decentralizuotame tinkle, išskiria blokų grandinę nuo paprastos knygos. Pasiekus sutarimą, kiekvienas tinklo mazgas kartu atnaujina savo knygos kopiją. Nesant bendro sutarimo, likusi tinklo dalis akimirksniu nustoja bandyti pridėti arba pašalinti mazgą.

„Blockchain“ naudoja trigubo įrašo apskaitą, kai vienas įrašas daromas kredito pusėje, kitas – debeto pusėje, o trečias – nekintamoje bendroje knygoje – valdoma pažangių matematinių algoritmų ir nepralaidžios kriptografijos. Skaityti daugiau, [Blockchain for Real World Applications - Rishabh Garg. John Wiley & Sons, Inc. US, 01-388: ISBN - 9781119903734](#).

Blockchain yra blokų serija, sudaranti išsamų operacijų, perduodamų ir atkartojamų tinkle kaip skaitmeninė viešoji knyga, sąrašą. Blockchain ekosistemą sudaro **mazgai** - vartotojai arba

kompiuteriai – kurie palaiko pilną įrašo ar knygos kopiją, o **bloškai** yra duomenų formatai, naudojami operacijų įrašams saugoti ir perduoti juos tarp visų tinklo mazgų [Garg, 2021].

Stuartas Haberis ir W Scottas Stornetta [1991] pirmieji pristatė blokų grandinės koncepciją. Tačiau Satoshi Nakamoto, slapyvardžiu slėpintis asmuo, jį išpopuliarino 2008 m., kad jis galėtų būti viešas bitkoinų operacijų žurnalas. Programuojamos išmaniosios sutartys, konstitucinis dizainas ir blockchain konsensuso protokolas buvo pagrindinės naujovių sritys per pastarąjį pusantro dešimtmečio.

## **BLOCKCHAIN LAIKAS**

Per pastaruosius 15 metų buvo daug naujovių blokų grandinės konsensuso technologijose, programuojamose išmaniosiose sutartyse ir patikėjimo architektūroje.

### **BLOCKCHAIN 1.0**

Blockchain 1.0 buvo naudojama kaip skaitmeninė valiuta didelės apimties prekybai, nedidelės vertės sandoriams, Forex, lošimams ir pinigų plovimui. Blockchain technologijos naudojimas skaitmeninei valiutai turi daug privalumų, tačiau pagrindinis jos pranašumas yra tai, kad ji suteikia saugią ir saugią turto pervedimo platformą be tarpininkų ar sandorio šalių. Dabar yra daugiau nei 4500 skirtingų kriptovaliutų rūšių. Populiariausi yra Bitcoin (2009), Litecoin (2011), Namecoin (2011), Dogecoin (2013) ir Peercoin, kurių bendra rinkos kapitalizacija yra 295 milijardai JAV dolerių (2012).

### **BLOCKCHAIN 2.0**

Blockchain 2.0 programų išplėtimas įgalino išmaniąsias sutartis, decentralizuotas programas (dApps) ir decentralizuotas autonomines organizacijas (DAO). Jis atliko pagrindinį vaidmenį konkrečiose finansų srityse – bankininkystėje, vertybinių popierių prekyboje, kreditų sistemose, tiekimo grandinės finansavime, mokėjimų tarpuskaitoje, kovoje su padirbinėjimu, savitarpio draudimu ir sutrikdė tradicines valiutas bei mokėjimo būdus. Tai palengvino išmaniųjų sutarčių įgyvendinimą naudojant kai kurias programuojamas sutarčių kalbas, įskaitant Ethereum, Codius ir Hyperledger.

### **BLOCKCHAIN 3.0**

Be valiutos ir finansų, Blockchain 3.0 sugebėjo įtvirtinti dominavimą tokiose srityse kaip švietimas, sveikata, mokslas, transportas ir logistika. Tai apima sudėtingesnę išmaniosios sutarties tipą, siekiant sukurti decentralizuotą organizacinį vienetą, kuris sukuria savo taisykles ir suteikia didelę autonomiją.

### **BLOCKCHAIN 4.0**

Blockchain 4.0 vystosi į verslui palankią ekosistemą masėms. Tai blokų grandinės sintezė su pažangiausiomis ateities technologijų galimybėmis, tokiomis kaip daiktų internetas, debesų kompiuterija, dirbtinis intelektas ir robotika. Išnagrinėjus virtualių blokų grandinių potencialą

vienoje blokų grandinėje, sistema gali užsidirbti nevaržomo mastelio. Blockchain 4.0 reiškia idėjas ir sprendimus, kurie racionalizuoja technologijas verslo poreikiams, ypač pramonei 4.0 ir prekybai. Blockchain technologija gali būti naudojama siekiant pagerinti įvairius procesus, įskaitant tiekimo grandinės valdymą, įmonės darbo eigą, finansines operacijas, daiktų interneto duomenų rinkimą, sveikatos stebėjimą, turto valdymą ir kredito sistemas.

Taigi, blockchain 4.0 žada skaitmeninę architektūrą, kuri apjungia automatizavimą, atskaitomybę ir privatumo apsaugą, kad būtų sukurta be trikdžių realioje pasaulyje [Garg, 2021; 2023].

## BLOCKCHAIN ARCHITEKTŪRA

Blockchain patikrina operacijų pagrįstumą naudodama asimetrinę kriptografijos techniką. Čia matematinis procesas, žinomas kaip **maišos funkcija**, naudojamas bet kokiems duomenims konvertuoti į raidinių ir skaitmeninių reikšmių eilutę. Tai procesas, vadinamas **šifravimu**, kuris sušifruoja skaitomą tekstą, kurį gali perskaityti tik slaptaį kodą arba iššifravimo raktą turintis asmuo. Yra dvi pagrindinės šifravimo formos – **asimetrinis šifravimas** (viešasis raktas) ir **simetrinis šifravimas**. Simetrinis šifravimas turi tik vieną privatą (slaptą) raktą ir jį naudoja visos bendraujančios šalys tiek šifravimui, tiek iššifravimui.

Čia lauko maiša ir užšifruoti operacijų duomenys veikia kaip skaitmeninis parašas. Originali duomenų kopija ir saugi duomenų maiša išsiunčiama gavėjui. Gavėjas apskaičiuoja naują maišą naudodamas pirminius duomenis, gautus iššifravus saugią maišą. Jei abu yra vienodi, tai reiškia, kad gauti duomenys nebuvo pakeisti.

## DECENTRALIZUOTAS IDENTIFIKATAS

**Decentralizuoti ID** įgalina lygiaverčius ryšius tarp dviejų šalių, kurios yra pasauliniu mastu unikalios, atkaklios ir pseudoanoniminės. DID suteikia tapatybės savininko kontrolę ir tapatybių suverenitetą, nes jie nepriklauso nuo centralizuotų registru, institucijų ar tapatybės tiekėjų. Kadangi žmogus gali turėti kelis DID, juos stebėti visoje savo veikloje yra sunkiau. Skaityti daugiau, *Blockchain for Real World Applications - Rishabh Garg. John Wiley & Sons, Inc. US, 01-388: ISBN - 9781119903734*.

## BLOKINĖS EKOSISTEMA

Blockchain ekosistema yra vartotojų tinklas, besidalinantis mazgais bendrai verslo veiklai ir tikslui. Kiekviename blokų grandinės bloke yra apie 1 MB duomenų. Užpildžius pirmojo bloko 1 MB duomenų talpą, informacija šiame bloke saugoma chronologiškai, o po to kartojama antrajame bloke [Garg, 2021].

Kiekvienas blokas gauna skirtingą maišą, tiksliai atitinkančią tame bloke esančią duomenų eilutę, kad visi šie blokai būtų sujungti į vieną seką. Blokas gauna naują maišą, jei jame yra net nedidelis pakeitimas. Sistema remiasi decentralizuotomis duomenų bazėmis, kad galėtų kontroliuoti duomenų atsiradimą tarp subjektų per P2P (peer-to-peer) tinklą, kur sutarimo metodai užtikrina replikaciją tinklo mazguose.

Atskiri mazgai sudaro blokų grandinės ekosistemą ir kiekvienas turi savo knygos kopiją. Mazgai bendrauja tarpusavyje, kad susitartų dėl knygos įrašo, todėl centrinei institucijai ar bet kuriai trečiajai šaliai nereikia koordinuoti ar tikrinti. Be pateiktų duomenų perdavimo ir tikrinimo blokų grandinėje, mazgai taip pat padeda įvesti naujus duomenis. Operacijų įrašymas naujame bloke ir jų įtraukimas į esamą grandinę vadinamas **kasyba** ir įvyksta, kai visi mazgai pasiekia konsensumą. Blokų grandinėje kiekvienas blokas turi savo nonce ir maišą, prieš kurią grandinėje yra bloko maiša.

Kriptografinė maišos funkcija generuoja maišą blokų grandinėje, kuri kiekvieną įvesties eilutę paverčia 64 skaitmenų išvesties eilute. Ne visos maišos galioja. Bloko maiša turi prasidėti bent dešimčia iš eilės einančių nulių, kad būtų galima priskirti blokų grandinę. Kiekvienas blokas gauna **nonce**, kuris yra nedidelis unikalių duomenų kiekis. Kalnakasiai turi nuolat užsiimti kasyba, ty nuolatos modifikuoti ir maišyti bloko duomenis ieškant veikiančios maišos. Norėdami rasti tinkamą parašą (išėjimą), kalnakasiai turi nuolat keisti bloko struktūrą (vieną kartą) ir sunaudoti daug elektros energijos. Kuo daugiau skaičiavimo galios jie turi, tuo greičiau apdoroja įvairias blokų kompozicijas, kad surastų gerą maišą.

## VIEŠA IR PRIVATI BLOKŲ GRINDINĖ

Yra trys pagrindiniai blokų grandinių tipai : viešosios, privačios ir konsorciumo grandinės. Bet kuris vartotojas, norintis atlikti tinklo operacijas, gali tai padaryti **viešojoje blokų grandinėje** be jokių apribojimų. Kita vertus, **privačiose blokų grandinėse** konsensuso procese gali dalyvauti tik tam tikros organizacijos mazgai. Todėl ji taip pat žinoma kaip leistina blokų grandinė. **Consortium blockchain** yra pusiau privatus panašiai mastančių įmonių tinklas, skirtas produktyvumui, atskaitomybei ir skaidrumui didinti.

## BLOKCHINĖS KONSENSUSAS

Siekiant sutarimo dėl blokų grandinės būsenos ir užtikrinti operacijų pagrįstumą, naudojamas gedimams atsparus mechanizmas, vadinamas **konsensuso mechanizmu**. Čia kiekvienas blokų grandinės tinklo narys susitaria dėl dabartinės paskirstytos knygos būsenos. Norėdami pridėti naują bloką prie grandinės, mazgas turi atlikti skaičiavimo užduotį, žinomą kaip **darbo įrodymas**. PoW yra sutarimo forma, kurią naudoja bitkoinų tinklas. Šioms operacijoms eikvojama daug energijos, nes PoW reikalauja, kad kalnakasiai atliktų didžiulius skaičiavimus. **Proof-of-Stake** yra mažiau energijos sunaudojanti, PoW alternatyva, pagal kurią kalnakasiai turi įrodyti, kad jie yra teisėti valiutos savininkai. Tai pagrįsta nelogiška prielaida, kad vartotojai, turintys daugiau valiutos, yra mažiau linkę atakuoti tinklą. Siekiant įveikti šią aklavietę, buvo pasiūlyti keli konsensuso algoritmai, įskaitant **PBFT, DPoS, Peercoin, Ripple, Tendermint** ir kt.

Siekdami užtikrinti efektyvumą, saugą ir patogumą, kai kurie darbuotojai pasiūlė gobšų sunkaus stebėjimo pomeđį. (**GHOST**) grandinės pasirinkimo taisyklė. Šioje sistemoje šakas sveria

GHOST, kad kalnakasiai galėtų pasirinkti tinkamiausią šaką, o ne ilgiausią šakos planą [Simpolinski ir Zohar, 2013].

## MOKĖJIMO PATIKRINIMAS BLOCKCHAIN

Yra du galimi mokėjimo patvirtinimų tipai: paprastas mokėjimo patvirtinimas ir visiškas mokėjimo patvirtinimas.

Vykdydamas **paprasto mokėjimo patvirtinimo** (SPV) procesą, plonas arba lengvas klientas gali atsisiųsti bloko antraštę, kuri yra daug lengvesnė nei viso bloko. Vartotojui lengviau ir naudingiau išsaugoti tik vieną bloko antraštės kopiją iš ilgiausio patikrinimo grandinės ir gauti Merkle filialą, susiejantį operaciją su bloku. Tikrinimas yra patikimas tol, kol sąžiningi mazgai valdo tinklą. Tačiau tuo metu, kai užpuolikas perima tinklo valdymą, sistema tampa atskleista.

Priešingai, **pilnam mokėjimo patvirtinimui** reikalinga stora arba sunki piniginė, kuri yra visa bloko grandinės kopija. Šios piniginės programos patvirtina ir perduoda kitų žmonių sandorius, be to, valdo paties vartotojo operacijas. Norint pateikti suasmenintus rezultatus ir pasirinkti blokų grandinę su aukščiausiu darbo įrodymu, visos tinklo šalys (visi mazgai) turi būti prijungti. Taigi, priklausomai nuo ryšio, gali prireikti kelių dienų, kol „blockchain“ tinklas bus atsiųstas naudojant bitcoin piniginės programą. Skaityti daugiau, [\*Blockchain for Real World Applications - Rishabh Garg. John Wiley & Sons, Inc. US, 01-388: ISBN - 9781119903734.\*](#)

## KRIPTOVALIUTOS

**Kripto valiutos**, tokios kaip Bitcoin, Ether arba Litecoin, yra skaitmeniniai žetonai, kuriais prekiaujama blokų grandinėje ir kurie naudojami perkant produktus ir paslaugas. Blockchain technologiją krypto valiutos naudoja siekdamos papildyti viešosios knygos ir sudėtingos kriptografinės apsaugos sistemos pranašumus. Bėgant metams šios valiutos tapo neįtikėtinai populiarios, todėl visame pasaulyje egzistuoja daugiau nei 18 000 krypto valiutų, kurių rinkos vertė siekia 3,2 trilijonus USD. Šiuo metu bitcoino vertė yra 3 120 210,68 INR.

## STRAIPTAI

**Scenarijai** laikomi vienu iš pagrindinių aspektų diegiant verslo logikos sluoksnį blokų grandinėje. Paprasčiau tariant, bitkoinų operacijos yra informacija, atspindinti bitkoinų judėjimą iš vienos piniginės į kitą. Paprastai pirmas sandoris naujame bloke sukuria naują valiutą, bet niekada jos neišleidžia. Šiose operacijose įvestis paliekama tuščia ir tokia tuščia įvestis vadinama **Coinbase operacija**. Šios operacijos sukurtas atlygis taip pat gali būti paskirstytas vienam ar daugiau piniginės adresų, kaip įprasta bitkoinų operacija. Įdėjus tam tikrą sėkmingų blokų skaičių, atlygis sumažinamas perpus už kiekvieną sėkmingą bloką, pridėtą prie blokų grandinės, išlaikant bitkoiną kaip ribotą atsargą, atsparų infliacijai.

Kadangi Bitcoin nėra vyriausybės išleista teisėta mokėjimo priemonė, dėl jo populiarumo atsirado naujų galimybių jį keisti į fiat pinigus, pvz., krypto valiutų keitykla, bitkoinų debeto kortelės, bitkoinų bankomatai, Metal Pay ir lygiavertis tinklas.

Iš pradžių peer-to-peer kriptovaliuta, žinoma kaip Bitcoin, buvo naudojama įprastoms operacijoms, tačiau laikui bėgant Bitcoin tapo investicine priemone, nes išpopuliarėjo ir išaugo vertė.

Buvo manoma, kad blockchain technologija, kurioje ji veikė, stokoja mastelio, nes ji iš esmės negalėjo valdyti didelės apimties operacijų. Taigi 2017 m. rugpjūčio mėn. originali kriptovaliuta Bitcoin suskilo į dvi skirtingas kriptovaliutas – **Bitcoin Cash** ir **Bitcoin SV**. 2018 m. lapkritį kriptovaliuta patyrė dar vieną šakę, padalytą į **Bitcoin Cash ABC** ir **Bitcoin Cash SV (Satoshi Vision)**. Kadangi jame naudojamas originalus Bitcoin Cash klientas, Bitcoin Cash ABC dabar vadinamas Bitcoin Cash.

Kūrėjai gali naudoti išmaniąsias sutarčių kalbas, tokias kaip CashScript, kad įgalintų sudėtingesnes operacijas naudodami Bitcoin Cash nei su Bitcoin. Bitcoin Cash gali būti sunkus turtas, pavyzdžiui, nekilnojamasis turtas, auksas ar kitos fizinės prekės, nes Bitcoin turi 21 milijono monetų ribą, leidžiančią vartotojams labai ilgą laiką išlaikyti vertę skaitmenine forma.

## ETERIJAS

Ethereum yra blockchain variantas, kurį sukūrė Rusijos ir Kanados programuotojas Vitalikas Buterinas ir jo kolegos. Ethereum yra decentralizuota „blockchain“ platforma, sukurta naudojant bendrą pasaulinę infrastruktūrą. Kiekviename tinklo mazge veikia operacinė sistema – Ethereum virtualioji mašina, kuri gali suprasti ir paleisti programas, žinomas kaip išmaniosios sutartys. Taigi, Ethereum sustiprina bitkoino pranašumus blokų grandinė, leidžianti programuotojams rašyti kodą, kuris imituoja pagrindines decentralizuotos programos arba dApp funkcijas.

## PROTINGOS SUTARTYS

Išmanioji sutartis yra programos kodas, saugomas konkrečiu adresu (sutarties adresu) blokų grandinėje. Programos gali įdiegti išmaniųjų sutarčių veikimą, modifikuoti jų būsenas ir inicijuoti operacijas. Tokioms sutartims kurti naudojama specializuota programavimo kalba, tokia kaip Solidity arba Viper. Vykdam sutartis dažnai naudojami tokie teiginiai kaip „jei... tada“. Skaityti daugiau, [\*Blockchain for Real World Applications - Rishabh Garg, John Wiley & Sons, Inc. US, 01-388: ISBN - 9781119903734\*](#).

## HYPERLEDGER

Hyperledger yra pasaulinė atvirojo kodo bendradarbiavimo priemonė, kuri suteikia pagrindą, standartus, gaires ir įrankius, reikalingus naudoti įvairiose pramonės šakose. Jis sveikina bet kurį bendruomenės narį, turintį programavimo žinių ar besidominčių, prisidėti prie šaltinio kodo kūrimo. Kodą gali peržiūrėti, sukurti, modifikuoti ar platinti bet kuris pasaulio programuotojas.

Tik tie subjektai ar asmenys, kurie turi autorizacijos sertifikatą, gali tikrinti operacijas Hyperledger tinkle. Įmonės, pvz., privačios arba B2B, nenorinčios savo asmeninės informacijos viešoje blokų grandinėje, gali naudoti šį leistiną ir ribotos prieigos blokų grandinės tinklą – Ethereum, Hyperledger.

## DECENTRALIZUOTOS PROGRAMOS

Centralizuotoje sistemoje taikomoji programinė įranga gali būti patalpinta vienoje ar keliuose centrinėse vietose, atsižvelgiant į įdiegtos klientų bazės dydį. Tačiau decentralizuotoje sistemoje išmaniosios sutartys naudojamos tam, kad taikomoji programinė įranga galėtų veikti nepriklausomai lygiaverčio blokų grandinės tinkle, o ne viename kompiuteryje. **Decentralizuota programa** (dApp) sudaro priekinę dalį, blokų grandinės užpakalinę dalį ir tarpinę programinę įrangą – programinę įrangą, jungiančią jas abi.

Nors dApps žada išspręsti daugelį pagrindinių problemų, susijusių su tradicinėmis programomis, jos taip pat turi nemažai trūkumų, tokių kaip priežiūros reikalavimai, didelės našumo išlaidos, tinklo perkrova ir kt.

## TAPATYBĖS NURODYMAI

Tapatybė yra pagrindinė visos žmogaus veiklos dalis. Galiojanti tapatybė yra būtina sąlyga norint stoti į mokyklą, pateikti prašymus įsidarbinti, turėti banko sąskaitą, gauti pasą, pasirašyti sutartis ar patekti į finansų sistemą [Garg, 2019]. Tačiau daugiau nei milijardas asmenų, įskaitant 21 milijoną pabėgėlių, vis dar neturi teisinės tapatybės. Taip yra dėl paslėptų išlaidų, tarpininkų įsikišimo ir varginančių procesų.

## TAPATYBĖS VISAME PASAULYJE

Žmonės visame pasaulyje turi įvairių tapatybės formų, pavyzdžiui, pasą tarptautinei kelionei, vairuotojo pažymėjimą vairuoti transporto priemonę, rinkėjo kortelę rinkimuose, socialinio draudimo numerį, leidžiantį registruoti atlyginimą ar savarankišką veiklą ir kt. [Garg, 2020]. Identifikavimo sistemos istorija tikriausiai prasideda 1803 m., kai Napoleonas Bonapartas pristatė pirmąją identifikavimo sistemą pasaulyje.

Prancūzijos vyriausybė įvedė darbuotojų tapatybės kortelę, siekdama panaudoti ją kaip įrankį nevaržomai Prancūzijos Respublikos visuomenei paversti gerai organizuotą policinę valstybę, kad darbuotojai negalėtų migruoti į geresnes darbo vietas ir didesnius atlyginimus be darbdavio leidimo. Napoleono ID planas buvo palyginimas apie prekybą žmonėmis ir vergiją Rusijoje ar Rytų Europoje, tačiau jis negalėjo klestėti dėl darbo jėgos trūkumo ir savipagalbos organizacijų atsiradimo per pasaulinius karus [Lyon, 1994].

Iki XX amžiaus Vokietija tapo labai demokratiška, tolerantiška ir liberalia tauta su gerovės sistemomis, socialiniu draudimu ir nacionalinėmis sveikatos priežiūros paslaugomis. Tokioje aplinkoje naciai buvo apsėsti darbuotojų ekonominės vertės, išskaičiuoti atlyginimus, pašalinti streikuotojus ir neįgaliuosius. Naciai įvedė darbo knygą, kurioje įrašoma kiekvieno darbuotojo darbo istorija, įskaitant atleidimo laikotarpius ir darbo sutarčių pažeidimus. Jo užmaskuotas motyvas buvo nustatyti streikuojančius, silpnuosius, drovius darbui, neblaivias, seksualiai ištvirkusias, slaptas prostitutes ir subproletariatą. Įsakymas buvo atmestas tik 1941-42 m., kai karas atsisuko prieš Vokietiją [Gotz and Roth, 2004].



Kinija išplėtė nacių darbo knygą, pritaikydama ją į sistemą, vadinamą dangan dossier, kuri numatė asmeninių įrašų iš mokyklos laikų rinkimą. Darbuotojai negalėjo pradėti naujo pašaukimo, kol buvęs darbdavys neišsiuntė jų dokumentų rinkinio. Ši nauja sistema visiškai skyrėsi nuo istorinės sistemos Dang-e, kuri buvo skirta didikams prižiūrėti.

Be to, Kinijoje egzistavo vadinamoji vidaus registracijos sistema, kuri neleido Kinijos darbuotojams be leidimo persikelti į kitą vietą. Dešimtajame dešimtmetyje dangų sistema pradėjo irti dėl globalizacijos kylančių jėgų. Užsienio įmonės, atvykstančios į Kiniją, nevedė įrašų ir įdarbino migrantus iš kaimo be dokumentų.

Šiuolaikinė asmens tapatybės kortelių era prasidėjo nuo Antrojo pasaulinio karo. 1938 m. Jungtinė Karalystė priėmė Nacionalinio registro įstatymą, pagal kurį visi gyventojai privalo turėti asmens tapatybės kortelę [Whitley ir Hosein, 2009]. 1940 m. Prancūzijos Viši vyriausybė sukūrė ID sistemą su Graikija ir Lenkija, kuri daugiau ar mažiau išliko iki šiol. Išskyrus keletą išimčių, vargu ar kuri nors pasaulio šalis, kurioje galioja bendroji teisė, yra priėmusi taikos meto identifikavimo sistemą.

Asmens tapatybės kortelių priėmimas Azijoje atsispindėjo bume po Antrojo pasaulinio karo. Honkongo vyriausybė įvedė asmens tapatybės kortelę 1949 m., siekdama užkirsti kelią imigracijai iš žemyninės Kinijos ir sustiprinti jos suverenitetą. Taivanas 1949 m., Pietų Korėja ir Singapūras septintajame dešimtmetyje pasekė pavyzdžiu, pretekstu ekonominei pertvarkai.

## **ŠIUOLAIKINĖS TAPATYBĖS**

Jungtinėse Valstijose devynių skaitmenų socialinio draudimo numeris (SSN) išduodamas visiems JAV piliečiams, nuolatiniais gyventojams ir laikiniejiems gyventojams, vyresniems nei 18 metų. Nors iš pradžių jis buvo skirtas identifikuoti asmenis socialinės apsaugos tikslais, dabar jis taip pat yra naudojamas asmenims sekti mokesčių tikslais. Praktiškai jis tapo de facto nacionaliniu identifikavimo numeriu dėl plataus pritaikymo spektro, pavyzdžiui, banko sąskaitos atidarymo ar prašymo išduoti vairuotojo pažymėjimą.

Socialinio draudimo numeris buvo įvestas Kanadoje, bet baigėsi 2004 m., kai buvo įvestas asmeninės informacijos apsauga ir elektroninis dokumentas kaip tikri ID numeriai.

Kolumbijoje kiekvienam asmeniui vaikystėje išduodama pagrindinė asmens tapatybės kortelė, vadinama Tarjeta de Identidad, kurioje yra gimimo data ir mažas serijos numeris. Kiekvienam piliečiui sulaukus 18 metų pakartotinai išduodama pilietybės kortelė (Cedula de Ciudadanía), kuri yra būtina visais viešaisiais ir privačiais reikalais.

Meksikoje identifikavimo numeris vadinamas Clave Única de Registro de Población (CURP). Nors įvairūs kiti ID, pvz., socialinio draudimo numeris, kuriuos suteikė Instituto Mexicano del Seguro Social ir Registro Federal del Contribuyente (RFC), priskirtas izdo, taip pat yra madingi, tačiau rinkimų kortelė Credencial de Elector arba Credencial del INE, kurią išleido Instituto Nacional Electoral skiriamas didžiausias pripažinimas.

Nacionalinė asmens tapatybės kortelė, Documento Nacional de Identidad (DNI), išduoda Registro Nacional de las Personas gimimo metu Argentinoje, išskyrus imigrantus, kurie gauna numerius, prasidedančius nuo 92 000 000. Šis ID reikalingas norint kreiptis dėl kredito, atidaryti banko sąskaitą ir pasinaudoti franšizės teise. Kadangi tėvai privalo registruoti savo vaikus, vargšai, o ypač našlaičiai, lieka nuošalyje.

Brazilijoje yra dvi sistemos – pirma, Registro Geral (RG), kuris yra valstybių ir kai kurių organizacijų, pvz., ginkluotųjų pajėgų, kaip įgalioto nacionalinio asmens tapatybės dokumento priskirtas numeris. Kadangi jie skiriami valstybės lygiu, galima turėti tą patį RG numerį dviem piliečiams skirtingose valstybėse.

Antroji sistema, Cadastro de Pessoas Físicas (CPF), yra federalinė ir unikali, tačiau iš pradžių ji buvo sukurta mokesčių tikslais. Brazilijoje vienas arba abu numeriai būtini atliekant tam tikras įprastas užduotis, pavyzdžiui, atidaryti banko sąskaitą ar gauti vairuotojo pažymėjimą.

Europos ekonominėje erdvėje ir Šveicarijoje Europos sveikatos draudimo kortelė išduodama sveikatos priežiūros tikslais. Šioje kortelėje pateikiamas kodas, vadinamas identifikavimo numeriu. Suomijoje asmens kodas henkilotunas (HETU arba švediškai – Personbeteckning) buvo madingas nuo 1964 m. ir naudojamas piliečiams identifikuoti atliekant vyriausybės ir įmonių sandorius.

Prancūzijoje INSEE kodas, atsiradęs Vichy režimo metu, naudojamas tapatybės nustatymo, socialinio draudimo, užimtumo ir mokesčių tikslais. Vokietijoje nuo 2007 m. socialinio draudimo bendrovės tvarkė tik decentralizuotą duomenų bazę, kurios socialinio draudimo numerį skyrė beveik kiekvienam asmeniui. Po 2008 m. buvę mokesčių bylų numeriai buvo pakeisti naujais mokesčių mokėtojo identifikavimo numeriais Steuerliche Identifikationsnummer arba Steuer-IdNr. Asmenys, kurie tuo pačiu metu yra samdomi ir savarankiškai dirbantys asmenys, gali gauti du mokesčių mokėtojo identifikavimo numerius. Atitinkamą numerį organizacijoms išduoda Federalinė centrinė mokesčių tarnyba ir jis pavadintas Wirtschafts-Identifikationsnummer.

Italijoje finansinis kodas (Codice fiscale) išduodamas SSSNNNYYMDDZZZZX formatu gimimo metu. SSS yra pirmieji trys priebalsiai šeimos pavadinime (jei nėra pakankamai priebalsių pirmasis balsis, naudojamas X); NNN yra pirmasis vardas, iš kurio vartojami pirmasis, trečiasis ir ketvirtasis priebalsiai; YY – paskutiniai du gimimo metų skaitmenys, M – gimimo mėnesiui priskirta raidė, DD – paskutinės dvi gimimo raidės; ZZZZ yra konkrečios savivaldybės, kurioje asmuo gimė, vietovės kodas; X yra pariteto simbolis, kuris apskaičiuojamas sudedant raides lyginėse ir nelyginėse padėtyse. Mėnesio raidės vartojamos abėcėlės tvarka, tačiau naudojamos tik raidės A–E, H, L, M, P, R–T (taigi, sausis yra A, o spalio – R); Siekiant atskirti lytis, patelių gimimo dienai pridedama 40; o užsieniečiams vietoje savivaldybės kodo naudojamas visos šalies kodas.

Gambija ir Nigerija savo piliečiams skiria 11 skaitmenų identifikavimo numerius, vadinamus nacionaliniais identifikavimo numeriais [NIMC, 2022].

Nacionalinis ID numeris Zimbabvėje yra vienuolikos simbolių raidinis ir skaitmeninis kodas, kurį tvarko Generalinio registro biuras. Jame yra 2 skaitmenų priešdėlis, nurodantis rajoną, kuriame pareiškėjas gyvena; kiti šeši skaitmenys žymi pareiškėjo unikalų asmens kodą; o paskutiniai 2 skaitmenys yra pirminių tėvų nacionalinio ID numerio priešdėlis.

Kinijos Liaudies Respublikoje visiems vyresniems nei 16 metų piliečiams privaloma turėti 18 skaitmenų asmens tapatybės kortelę, kurios formata yra RRRRRRRYYMMDDSSSC. RRRRRR yra standartinis apskrities ar miesto, kuriame gimęs savininkas, administracinio padalinio kodas; YYYYMMDD yra turėtojo gimimo data; ir SSS yra nuoseklus kodas, skirtas atskirti žmones, turinčius tą pačią gimimo datą ir gimimo vietą [Shaw, 1996; Perry, 1997]. Eilės kodas yra nelyginis vyrams ir lygus moterims.

Indonezija išleido 16 skaitmenų RFID kortelę su elektroniniu parašu, rainelės nuskaitymu, dešimties pirštų pirštų atspaudų nuskaitymu ir didelės raiškos pasu pavadinimu e-KTP (Electronic Kartu Tanda Penduduk) nuo 2012 m. Ši programa sukurta remiantis Indijos UIDAI.

Indija dešimtmečius siekia suteikti oficialią tapatybę visiems savo piliečiams. Iki šiol nesuskaičiuojama daugybė tapatybės dokumentų buvo išsklaidyti ir atsukti atgal, todėl piliečiai ėmė keistis ir susipainioti [Garg, 2017]. Esamų ID apribojimas yra tas, kad jie naudojami tik skirtingiems ir ribotiems tikslams. Be to, neretai skirtingose saugyklose aptinkami neatitikimai piliečio profilyje, sukeliantys painiavą ir klaidas [Garg, 2018; 2019].

Biometrinio unikalaus identifikavimo numerio (UID) arba Aadhaar idėją pasiūlė Indijos vyriausybės Informacinių technologijų departamentas, siekdamas suteikti autentišką tapatybę kiekvienam Indijos gyventojui. Daugiau nei vienas milijardas piliečių buvo įtrauktas į šią schemą, kuriai iki šiol buvo išleista 130 milijardų INR (UIDAI, 2022). Tai didžiausia pasaulyje biometrinė identifikavimo sistema, kuria siekiama suteikti identifikaciją kiekvienam tokiam gyventojui, kuriam trūksta individualios tapatybės.

## ONE WORLD-ONE IDENTITY



When a citizen can have the same name on different documents, why do we allot different identification numbers for different services? Can every citizen not be issued a 20 digit Universal Identification Number? Global identity will not only bring authenticity but it will also prevent a person from having citizenship of two different countries or availing benefits of their welfare schemes. This will curb innumerable crimes like infiltration, impersonation, fake passport, etc.



25 September 2021

The phenomenal progress in the field of computer and information technology during the last two and a half decades has shrunken the entire world into a mobile device. All tasks like education, banking, business, travel, transport, cinema, entertainment are being handled by this pocket-friendly apparatus.

In the times of Covid-19 when the world was confined within their households, people steered multi-billion dollar business, conducted classes, listened to lectures, and organized conferences through their laptops, and mobile phones. When one can avail all the facilities through digital platforms, why do we still count on physical ID cards whose authenticity, security and transferability is never assured?

A valid identity is a pre-requisite for any educational, commercial, financial or administrative transaction. Unfortunately 1100 million people around the world do not have any proof of identity and 400 million of these people are from the poorest sectors of the world.

To make identity universal and unique, Rishabh Garg, a sophomore of the Birla Institute of Technology and Science India, has proposed the idea of a universal ID number. He believes that just as every single citizen in every culture is given a name at the time of birth and that name is recorded in all records as his identity, similarly every citizen of the world is assigned a Universal Identification Number by a competent authority such as the United Nations. This unique identification number can be of 20 digits globally.



This identification number will not only establish the identity of the person but will also be able to count his educational achievement, financial transactions, property details, information of legal heirs, health-care, postal address etc.

Once his date of birth is entered correctly, he will automatically be eligible to vote as and when he attains the age of 18. He can cast his vote from his mobile or laptop based on the Unique Identification Number. After the closure of the polling at the scheduled time, the result can be declared instantly. This will save billions of dollars, time, and human resources.

Similarly, if one updates his postal address periodically on the portal of the postal department, then without inscribing the address, his important mail will reach at his doorsteps on the basis of 20 digit identification number. Last month Prime Minister of India announced the enactment of Ayushman Health Card. In the coming two years, such identity cards can be implemented in other work areas as well. However, the allotment of a separate identification number for each service and its subsequent linking with the Aadhaar number would call for endless problems to a common man.

Reiterating his stand Rishabh has discussed the idea of **One World One Identity** in university circles with more than 80,000 scholars on LinkedIn. According to him, **One World One Identity** would help in improved educational, banking, investment, healthcare, and other services, where a single card with unique number shall hold all the substantive data of a citizen, whether it be personal, biometric, educational, professional, medical, legal or financial, in different siloes, in a duly encrypted manner.

### Unique digital ID for citizen health and care facilities

Records will be protected, step to help poor and middle class: PM at launch

KAUNAIN SHERIFF M

NEW DELHI, SEPTEMBER 27

Almost a year after it was implemented on pilot basis in six Union Territories, Prime Minister Narendra Modi launched the Ayushman Bharat Digital Mission for the entire country Monday. It involves creation of not just a unique health ID for every citizen, but also creation of digital healthcare professionals and facilities registry.

The Prime Minister said the digital initiative has the "potential of bringing a revolutionary change in India's healthcare facilities. Today we will enter a new phase in our campaign to strengthen health facilities. Today, a mission is being started which has huge power to revolutionize the health facilities of India. This



PM Narendra Modi at the launch of Ayushman Bharat Digital Mission Monday.

### Unique health ID: Modi launches Ayushman Bharat Digital Mission

Technology has helped the country deal with the pandemic. It has also helped the government to launch the Ayushman Bharat Digital Mission. The mission is to create a unique health ID for every citizen and link it to their health records. This will help in providing better healthcare services to the citizens.

### DPS BOY SHINES AT INDIAN INTERNATIONAL SCIENCE FESTIVAL

Rishabh Garg, a student of Delhi Public School, Bhopal was invited for the 26th Indian International Science Festival, 2021. The Ministry of Science & Technology, Government of India, and the Ministry of Education, Government of India, jointly organized the festival. Rishabh Garg was selected to represent Madhya Pradesh, Chhattisgarh and Odisha in ISF 2021. In an outreach programme conducted by AMPRI, Rishabh was honoured by the National Convener Secretary of ISF.

### भोपाल के ऋषभ ने तीन साल पहले दिया था बहुउद्देशीय कार्ड का आइडिया

अमर के अग्रणी की श्रेणी में ऋषभ ने भी बोल दिया

अमर का बहुउद्देशीय कार्ड 2018 में ही शुरू हो चुका है

भोपाल, 25 सितंबर: ऋषभ गार्ग, जो तीन साल पहले 'अमर' नामक बहुउद्देशीय कार्ड का आइडिया दिया था, आज इसे लागू करने में मदद कर रहे हैं। ऋषभ गार्ग, जो दिल्ली पब्लिक स्कूल, भोपाल में पढ़ा करते हैं, ने अपने आइडिया को 'अमर' नामक एक ऐप में बदल दिया था। यह ऐप लोगों को उनके डॉक्टर, दवाइयों, और अन्य स्वास्थ्य जानकारी तक पहुंचा देता है।

### Modi launches digital Ayushman health IDs

अमर के अग्रणी ने भोपाल में आयोजित 2021 की अंतरराष्ट्रीय विज्ञान महोत्सव में भी भाग लिया

भोपाल, 25 सितंबर: प्रधानमंत्री नरेंद्र मोदी ने आज देशभर में आयोजित 'आयुष्मान भारत डिजिटल मिशन' का शुभारंभ किया। उन्होंने कहा कि यह मिशन लोगों को बेहतर स्वास्थ्य सेवाएं देने में मदद करेगा। ऋषभ गार्ग, जो इस मिशन के अग्रणी हैं, ने भी भाग लिया और अपने आइडिया को प्रस्तुत किया।

### डीपीएस के ऋषभ गार्ग को मिला सीएसआईआर इनोवेशन अवॉर्ड

भोपाल में आयोजित विज्ञान महोत्सव में ऋषभ गार्ग को यह अवार्ड मिला

भोपाल, 25 सितंबर: ऋषभ गार्ग को 'सीएसआईआर इनोवेशन अवॉर्ड' मिला है। यह अवार्ड उनके 'अमर' नामक बहुउद्देशीय कार्ड के आइडिया के लिए है। ऋषभ गार्ग, जो दिल्ली पब्लिक स्कूल, भोपाल में पढ़ा करते हैं, ने इस अवार्ड को जीतने में मदद की।



## **Vienas Pasaulis - Viena Tapatybė**

### **RISHABH GARG - BITS INDIA**

Atsakydamas į tai, **Garg [2016–2023]** pristatė One World – One Identity idėją, kuri yra vienintelė alternatyva kelioms tapatybės kortelėms. Šis visame pasaulyje unikalus daigiafunkcis skaitmeninis tapatybės numeris gali būti valdomas naudojant naujausią blockchain technologiją.

Kiekvienam Žemėje gyvenančiam žmogui tam tikrą dieną gali būti priskirta 20 skaitmenų tapatybė. Tai leis asmenims saugoti savo prisijungimo duomenis ir asmenį identifikuojančią informaciją piniginiėje arba programoje, vadinamoje IPFS [**Garg, 2021**]. Failų bendrinimui IPFS naudos decentralizuotą, paskirstytą peer-to-peer (P2P) tinklo modelį, kuris gali būti paskirstytas keliuose kompiuteriuose ar mazguose. Failus galima suskirstyti į segmentus ir laikyti mazgų tinkle, kurie juos seka naudodami maišą. Pradinį failą galima atkurti sujungus visą failą, remiantis kiekvieno komponento maišos verte.

Priešingai nei tradicinės hiperteksto perdavimo protokolo (HTTP) protokolų šeimos arba centralizuotos vardų erdvės, IPFS yra vieta pagrįsta saugojimo sistema. Kai saugojimo sistema yra pagrįsta vieta, ji stebi pagrindinius kompiuterius naudodama IP adresą arba kitą loginio adresavimo schemą, susietą su žinomu pavadinimu. Jei priegloba pakeičia pavadinimą arba adresą, reikia atnaujinti ir vardų tarnybos lentelę.

Turinio adresų saugykloje reikalingas turinio identifikatorius, kad būtų galima tiksliai nustatyti failo vietą. Vietoj loginio adreso čia duomenys pasiekiami remiantis kriptografinė maiša, kuri veikia kaip skaitmeninio failo piršto atspaudas. Tinklas visada grąžina tą patį turinį pagal maišą, neatsižvelgiant į tai, kas ir kur failas yra įkeltas. IPFS yra decentralizuotas failų saugojimo būdas, kai tapatybės valdymui originalus dokumentas gali būti išsaugotas IPFS, o jo turinio metaduomenys arba maiša gali būti saugomi blokų grandinės serveryje.

Papildomą saugumo sluoksnį gali suteikti ir biometriniai sprendimai, tokie kaip nykščio atspaudas išmaniajame telefone, pirštų atspaudai, rankos geometrija, balso ar veido atpažinimas, terminis žemėlapis, akių raštai – tinklainės skenavimas, rainelės nuskaitymas ar bet koks kitas biometrinio patikrinimo protokolas. Biometrinius duomenis galima išsaugoti ir apdoroti naudojant duomenų bazės serverį, fizinius prieigos raktus, šifruotus žetonus arba abu. Saugios sistemos dažnai saugo biometrinius šablonus įrenginyje arba vietoje, kad būtų galima patikrinti tapatybę neperduodant jokių jautrių biometrinių duomenų į kitą serverį ar vietą internete.

Nors vidinis biometrinio autentifikavimo mechanizmas priklauso nuo technologijos, jis yra nepaprastai paprastas ir greitas vartotojo požiūriu. Paprasčiau uždėti pirštą ant skaitytuvo nei įvesti ilgą slaptažodį su keliais specialiais simboliais, kad iš karto atrakintumėte paskyrą. Dauguma biometrinių autentifikavimo metodų naudojami tik su fizinėmis programomis; negalite perduoti ar perduoti biologinių metrikų internetu. Biometrinius duomenis, tokius kaip pirštų atspaudai, rainelės nuskaitymai, veido raštai ir kt., sunku atkurti naudojant dabartines

technologijas. Tikimybė, kad jūsų pirštų atspaudai sutaps su kieno nors kito pirštų atspaudais, yra viena iš 64 mlrd. Skaityti daugiau, [\*Blockchain for Real World Applications - Rishabh Garg. John Wiley & Sons, Inc. US, 01-388: ISBN - 9781119903734.\*](#)

Neseniai buvo atrasta, kad naudojant blokų grandinę, tradicinius bet kurio gilaus mokymosi modelio blokus galima paversti saugia sistema. Tai biometrinio atpažinimo architektūra, kuri naudoja blokų grandinės technologiją, kad užtikrintų gedimams atsparią prieigą paskirstytoje aplinkoje. Jis apsaugo tiek gilaus mokymosi modelį, tiek biometrinį šabloną ir įspėja visą sistemą, kai pažeidžiamas konkretus komponentas. Taip pat lengviau nustatyti galimus sutrikimus.

Biometrinės identifikavimo sistemos, kuriose derinami biometriniai duomenys ir blokų grandinės technologija, gali būti naudojamos siekiant pagerinti saugumą, pasiekti sutarimą nepastovioje aplinkoje ir priimti audituojamus sprendimus. Naudodami asmeninį įrenginį, pvz., išmanųjį telefoną, vartotojai gali bendrinti savo skaitmeninį ID su paslaugų teikėju, net jei jie fiziškai nėra, ir vis tiek galės pasiekti pagrindines paslaugas nekeldami pavojaus savo privatumui.

Be aiškaus vartotojo leidimo jokia operacija nebus vykdoma naudojant jo informaciją. Suteikus galimybę vartotojui valdyti savo asmenį identifikuojančią informaciją, sistema bus labiau sąveiki, vartotojas galės laisvai pasiekti duomenis keliose platformose ir nebus verčiamas naudoti tik vieną.

Kadangi blokų grandinės tapatybių naudojimui nėra geografinių apribojimų, vartotojai gali pasiekti ir patikrinti savo tapatybę iš bet kurio pasaulio kampelio. Blockchain pašalins kelių vartotojo vardų ir slaptažodžių poreikį, nes vartotojai galės mėgautis savarankiška ir užšifruota skaitmenine tapatybe.

Kortelėje su unikaliu numeriu visi fiziniai piliečio duomenys - asmeniniai, biometriniai, išsilavinimo, popamokiniai, profesiniai, medicininiai, teisiniai ar finansiniai – saugomi atskirose talpyklose, visiškai užšifruotai. Tokiu būdu **One World - One Identity** bus veiksminga geresnio švietimo, bankininkystės, investicijų, sveikatos priežiūros, viešojo platinimo schemų ir kitų paslaugų srityse [**Garg 2017**].

## KRIPTAVIMAS

Ryšio šifravimas leidžia tik tikram pranešimo siuntėjui ir numatomam gavėjui perskaityti atitinkamą turinį. Yra trys pagrindinės kriptografijos kategorijos – asimetrinio rakto kriptografija, maišos funkcijos kriptografija ir simetrinio rakto kriptografija.

Kriptografijos istorijoje buvo keletas lūžių, kurie padėjo pagrindą šiuolaikiniams algoritmams. Terminas šifras iš pradžių reiškė bendrą slaptų pranešimų perdavimo idėją, kurios pagrindinis komponentas buvo raidės. Paprastas pakeitimo šifras, Cezario šifras, Hill šifras, Playfair šifras, Vigenere šifras, perkėlimo šifras ir kt. yra keletas žinomų pavyzdžių. Playfair šifras C gali



saugiai perkelti iš šaltinio į paskirties vietą nenutekėdamas informacijos naudojant šifravimą ir iššifravimą.

Hillo šifras yra poligrafinis pakeitimo šifras, pagrįstas tiesine algebra, kurį 1929 m. įkūrė Lesteris S. Hillas. Jis gali lengvai sudaryti nuoseklų šifrą, kai naudojamas su dviračiais (dviejų raidžių blokais), trigrafais (trijų raidžių blokais) arba bet kokie kiti kelių dydžių blokai. Taip pat galima įdiegti daug daugiau kriptografinių algoritmų, įskaitant RSA algoritmą, kelių tikslumo aritmetikos biblioteką, GNU kelių tikslumo aritmetikos biblioteką, kinų priminimo teoremą ir SHA-512 maišą Java. Skaityti daugiau, [\*Blockchain for Real World Applications - Rishabh Garg, John Wiley & Sons, Inc. US, 01-388: ISBN - 9781119903734.\*](#)

## **KIBERNETINĖ SAUGA**

Kibernetinė sauga apsaugo sistemas ir tinklus nuo internetinių grėsmių. Kibernetinių atakų aplinka pastaraisiais metais sparčiai plėtėsi. Užpuolikai naudoja kenkėjiškas programas, tokias kaip Trojos arklys, šaknų rinkiniai ir virusai, žinomi kaip paskirstytos paslaugų atsisakymo (DDoS) atakos, Man in the Middle (MITM) atakos, sukčiavimo atakos ir Ransomware atakos. Įmonės visame pasaulyje įsisavino blokų grandinę, kuri tapo potencialia kibernetinio saugumo mažinimo priemone.

## **IŠSILAVINIMAS IR UŽIMTIS**

Milijonai kandidatų visame pasaulyje kasmet pateikia savo akademinius įgaliojimus, tikėdamiesi, kad juos įdarbins aukštosios mokyklos arba įmonės. Daugelis kandidatų per kiekvieną įdarbinimą perdeda savo išsilavinimą.

Siekdamas išsaugoti dokumento autentiškumą, kredencialų turėtojas gali saugoti visus savo kredencialus savo Pi piniginėje ir dalytis jais su tikrintojais šifruotu režimu, naudodamas Ethereum blokų grandinę. Pajal Garg [2021] maiša, sukurta įkėlus kredencialus į IPFS, gali turėti du šifravimo sluoksnius. Studento viešasis raktas gali būti naudojamas pirmam šifravimo sluoksniui sukurti, o vėliau išdavėjo privatus raktas gali būti naudojamas antrajam ir trečiajam šifravimo (autorizacijos) lygiams įgyvendinti. Jis bus iššifruotas naudojant išdavėjo viešąjį raktą, kad būtų patvirtinti bendrinami kredencialai. Sukurtą užšifruotą maišą galima palyginti su emitento duomenų bazėje saugoma maiša. Jei abu sutampa, kredencialas gali būti laikomas galiojančiu.

Dažnai mokinio pasiekimų pažymėjime nenurodoma mokymo programa ar mokymo metodai. Tai trukdo studentui perkelti savo akademinius kreditus ar mokymosi pasiekimus iš vienos institucijos į kitą. Išsamus mokymo programos, mokymo, mokymosi ir vertinimo įrašas gali būti išsaugotas kiekvienam mokiniui suteikiant prieigą prie vertinimo informacijos suvestinės [Garg, 2021]. Darbdaviai galės pasirinkti geriausią kandidatą, išnagrinėti savo praeitį ir įvertinti patvirtinamuosius dokumentus, jei kandidato pasiekimai bus užfiksuoti kiekviename jo akademinės karjeros etape tvirtoje platformoje, pvz., Blockchain. Iš esmės blockchain gali būti naudinga priemonė atliekant kandidato biografijos patikrinimus ir sutaupant laiko, pinigų bei

žmogiškųjų išteklių. Skaityti daugiau, [\*Blockchain for Real World Applications - Rishabh Garg. John Wiley & Sons, Inc. US, 01-388: ISBN - 9781119903734.\*](#)

## **SVEIKATOS APSAUGA**

Sveikatos priežiūros institucijos visame pasaulyje susiduria su tokiomis problemomis kaip duomenų pažeidimo vėlavimas, medicinos reikmenų atsiradimas ir prašymų grąžinti receptinius vaistus. Blockchain siūlo platų programų ir privalumų spektrą sveikatos priežiūros srityje. Tai padeda valdyti vaistų tiekimo grandines, apsaugoti pacientų medicininių įrašų perdavimą ir suteikti sveikatos tyrėjams prieigą prie biologinių ir genetinių kodų.

Naudojant blokų grandinę, visa paciento medicininė informacija, įskaitant receptus, pastabas ir laboratorijos rezultatus, gali būti pasiekama viename rodinyje. Kiekvieną informaciją galima konvertuoti į atskirą maišos funkciją. Kiekviena maišos funkcija yra atskira ir gali būti bendrinama tik gavus duomenų savininko leidimą. Be to, naudojant blokų grandinę, galima stebėti prekę nuo jos pagaminimo iki kiekvieno tiekimo grandinės etapo, suteikiant pirkėjui visišką prekių, kurias jis ketina įsigyti, matomumą ir skaidrumą. Technologijų naudojimas gali pagreitinti verslo partnerių ir draudimo kompanijų ieškinų nagrinėjimą, suteikti teisėsaugai galimybę ištirti bet kokią įtartina veiklą, pvz., narkotikų gabenimą ar kaupimą didelės nelaimės, pvz., pandemijos, metu, ir sujungti organų donorus, organų recipientus ir sveikatos priežiūros įstaigas, kad būtų lengviau persodinti organus.

## **GENOMIKA**

Begalinis skaičius genetinių duomenų taškų gali būti saugiai saugomas blokų grandinėje. Ji virsta rinka, kurioje asmenys gali prekiauti savo genetiniais duomenimis. Ji linkusi kurti išsamias duomenų bazes ir pateikti svarbią informaciją mokslininkams greičiau nei bet kada anksčiau. Skirtingai nuo dabartinių sistemų, jei duomenų savininkai gali užmegzti ryšį su duomenų pirkėjais tiesiogiai, nesinaudodami tarpininku, analizės sąnaudos gali sumažėti, o duomenų savininkai gali uždirbti daugiau pelno. Skaityti daugiau, [\*Blockchain for Real World Applications - Rishabh Garg. John Wiley & Sons, Inc. US, 01-388: ISBN - 9781119903734.\*](#)

## **TIEKIMO GRANDINĖ**

Kiekvieną dieną milijardai plataus vartojimo prekių gaminami ir platinami sudėtingomis tiekimo grandinėmis, kurios pasiekia kiekvieną pasaulio kampelį. Tačiau informacija apie šių prekių kilmę, gamybą ir naudojimą per visą jų gyvavimo ciklą lieka neaiški. Kiekvienas produktas praeina per platų tiekėjų, prekybininkų, platintojų, vežėjų, sandėlių ir kitų įrenginių tinklą prieš parduodant galutiniam klientui, tačiau beveik visada jie lieka paslaptimi šios sudėtingos kelionės metu.

Dėl to esminė verslo kliūtis, neleidžianti daugumai organizacijų nieko žinoti apie savo antros ir trečios pakopos tiekėjus, yra tiekimo grandinės matomumas. Skaidrumas ir matomumas



įvairiuose visos tiekimo grandinės kanaluose gali palengvinti prekių judėjimą nuo žaliavų iki gatavų prekių gamybos, testavimo ir platinimo.

Geresnių rezultatų galima tikėtis pritaikius blockchain technologiją tiekimo grandinėje. Tiekimo grandinė gali naudoti bendrą, sutarimu pagrįstą viešąją knygą, kad atsektų produktų kilmės ir gamybos procesus. Valdant tiekimo grandinę, produkto gyvavimo ciklas, sertifikavimas ir dokumentacija gali būti akimirksniu prieinama visoms šalims naudojant blokų grandinę. Nuo gamintojo iki sandėliavimo, kelionių, platinimo ir pardavimo, produktus galima stebėti.

## **MAISTO TIEKIMAS**

Didelė dalis mūsų vartojamo maisto gaminama per sudėtingą pasaulinę tiekimo grandinę, o tai taip pat padidina klastojimo, klastojimo, klaidingo pateikimo ir tikslingo pakeitimo riziką. Pasaulinis maisto sektorius kasmet praranda milijardus dolerių dėl maisto vagysčių. Pienas, arbata, kava, vaisių sultys, alyvuogių aliejus, klevų sirupas, vėžiagyviai, medus ir daugelis kitų maisto produktų yra įtraukti į daugumą maisto produktų kategorijų. Paprastas žmogus neįsivaizduoja savo dienos be šių maisto produktų.

Plečiantis pasaulinei tiekimo grandinei, maisto sauga tampa dideliu rūpesčiu tiek vartotojams, tiek reguliavimo institucijoms. Pasaulio sveikatos organizacijos duomenimis, vienas iš dešimties žmonių nukenčia nuo apsinuodijimo maistu, dėl kurio kasmet 33 milijonai metų gyvena sveikai ir miršta 420 000 žmonių [PSO ataskaita, 2019 m.]. Be to, per maistą plintančios ligos kasmet nusineša 125 000 vaikų iki penkerių metų gyvybių. Šiuo atveju blockchain yra patikima alternatyva, galinti išsaugoti nekintamų dokumentų atsekamumą. Naudojant blokų grandinę, galima stebėti maisto produktus visais lygiais – nuo ūkio iki prekybos centrų.

Blockchain taip pat sparčiai dominuoja kitose nei maisto tiekimo grandinės valdymo srityse. Nors dauguma geriausių įmonių turi pažangiausią skaitmeninę infrastruktūrą, įskaitant tiekimo grandinės valdymo (SCM) ir įmonės išteklių planavimo (ERP) programinę įrangą, sistemoje vis dar yra analoginių spragų, kai produktai stebimi nuo prijungtos gamybos įrangos (kilmės) iki skaitmeninio pristatymo, pranešimai ir RFID nuskaitymas. Netgi pažangiausia technika negali tiksliai apskaičiuoti, kiek ilgai gaminys tarnaus. Įmonės gali naudoti blockchain technologiją, kad realiuoju laiku palaikytų nekintamą skaitmeninę visų operacijų ir judesių knygą kiekvienam savo tiekimo grandinės tinklo nariui. Skaityti daugiau, [\*Blockchain for Real World Applications - Rishabh Garg. John Wiley & Sons, Inc. US, 01-388: ISBN - 9781119903734.\*](#)

## **NEKILNOJAMASIS TURTAS**

Nuo neatmenamų laikų nekilnojamas turtas buvo patikima investavimo galimybė turtingiesiems. Tik nedidelis turto skaičius užtikrina tokį patį kapitalo prieaugį. Nepaisant viso to, globalioje aplinkoje yra daug suvaržymų, pavyzdžiui, galimybė susisiekti su potencialiais rėmėjais, finansuotojais ir fondų valdytojais; šalies pilietybė; pirkėjo verslo įsteigimo, tarptautinių banko sąskaitų, kredito balų, atitinkamų lėšų ir tt pripažinimas. Be to, kiekvienas nekilnojamojo turto savininkas be reikalo išleidžia didžiulę pinigų sumą įregistruodamas

nuosavybės teises, atleisdamas turto suvaržymą ir perleisdamas nuosavybės teisę į savivaldybės įrašus, kad užtikrintų savo investicijas.

Blockchain visiems žaidėjams siūlo tą pačią tiesos versiją apie žemės nuosavybės pavadinimą. Dėl to gali būti pašalintos procedūros, dažnai susijusios su nekilnojamuoju turtu, pavyzdžiui, dvigubas pardavimas, suklastoti registrai ir kėsanimasis. Išmaniosios sutartys gali būti naudojamos nekilnojamojo turto sandoriams reguliuoti, tuo pačiu sumažinant popierizmą, tarpininkus ir nekilnojamojo turto vertintojus.

## **RINKIMŲ PROCESAS**

Pagrindinis bet kurios rinkimų institucijos tikslas yra sąžiningai, patikimai ir skaidriai surengti rinkimus. Siekdama šio tikslo, biurokratija beatodairiškai išleidžia milijardus dolerių ir verčia milijonus vyriausybės darbuotojų eiti rinkimų pareigas. Blockchain technologija gali būti veiksminga, kad balsavimo procesas būtų paprastas, sklandus ir skaidrus.

Tai gali padėti balsuoti žmonėms, kurie dažnai nesinaudoja savo teise į franšizę, galbūt todėl, kad gyvena atokiose vietovėse, neturi galimybės patekti į rinkimų apylinkes arba yra visiškai nedarbingi. Kadangi ji naudoja paskirstytą knygą, rinkėjai gali atiduoti savo balsus iš bet kurios pasaulio vietos neprarandant privatumo. Tai leidžia rinkėjams lengviau balsuoti rinkimų dieną sėdėdami namuose, nestovėdami eilėje ir neperžengdami pernelyg didelių formalumų.

Kai kiekvienas pilietis turi decentralizuotą tapatybę, taip pat žinomą kaip savarankiška tapatybė, paskirstyta knyga gali būti naudojama visiems svarbiems jo gyvenimo įvykiams įrašyti. Piliečiams gali būti leista dalyvauti rinkimų procese remiantis jų informacija, įskaitant nuolatinę gyvenamąją vietą (rinkimų apygardą, kurioje jie turi teisę balsuoti), gimimo datą (kai sulauks teisėto balsavimo amžiaus) ir esant kitoms sąlygoms (jei bet kuris). Rinkėjas gali balsuoti naudodamas savo prisijungimo ID, bet negali vėl naudoti to paties decentralizuoto identifikavimo numerio, kuriuo remdamasis balsavo per minėtus rinkimus. Atskirdama kiekvienos rinkimų apygardos balsus naudodami programinę įrangą antrą balsavimo dieną, blokų grandinė suskaičiuos balsus, atiduotus už kiekvieną kandidatą per skirtingus mazgus.

Nepaisant to, paslaptis, kad kiekvienas pilietis žino, kad balsavimo procesą ir rinkimų rezultatus supa daug priešiškos ir neteisėtos veiklos. Niekur pasaulyje rinkimų procesas nėra baigtas be kabinų fiksavimo, balsavimo įrangos pakeitimo balsavimo vietose ar melagingų balsavimo teiginių. Vyriausybės gali būti atsargios įgyvendindamos „blockchain“ pagrįstus rinkimus, nes tai yra visiškai audituojami procesai, ribojantys politinių partijų manipuliavimo galimybes. Skaityti daugiau, [Blockchain for Real World Applications - Rishabh Garg, John Wiley & Sons, Inc. US, 01-388: ISBN - 9781119903734](#).

## **BANKININKYSTĖ IR FINANSAI**

Bankinių institucijų kūrimo tikslas tikriausiai buvo įgalinti visokią prekybą ir verslą suburiant žmones. Blockchain leidžia atokioms nepatikimoms bankų ir finansų sektorių šalims lengvai

pasiekti sutarimą dėl duomenų bazės būklės be vartų sargų pagalbos. Vartotojai galės pasirinkti, su kuo ir kiek nori dalintis savo tapatybe. Blokų grandinėje jiems tereikia vieną kartą įvesti savo tapatybę. Jei paslaugų teikėjai naudoja blokų grandinę, jokiam vartotojui nereikia kartoti registracijos.

Panašiai kaip patikimas buhalteris, jis valdo visas finansines operacijas, įskaitant mokėjimus, atsiskaitymo sistemas, lėšų rinkimą, vertybinių popierių valdymą, paskolas, kreditus ir prekybos finansavimą. Kalbant apie tapatybės patvirtinimą, mokėjimus, išėmimus, atsiskaitymus, kreditus ir paskolas, turto pervedimus, tarpusavio pervedimus, rizikos draudimo fondus, saugumą ir atskaitomybę, jis sugebėjo pranokti tradicines sistemas.

Tai gali žymiai sumažinti operacijų mokesčius, nes sumažėja pridėtinės išlaidos, patiriamos rankiniu būdu nustatant, vykdant ir keičiant turtą. Pašalinus tarpininkus, procesai, tokie kaip tarptautiniai mokėjimai, prekyba ir atsiskaitymai, tapo greitesni, patikimesni ir pigesni.

## **PREKYBOS FINANSAI**

Informacijos perdavimas, turto perdavimas ir mokėjimų atlikimo procesas labai priklauso nuo popierinių verslo operacijų prekybos finansavimo srityje. Šios sutartys gali būti geriau paaiškintos Python programavimo kalba, o ne legalios, kad prekybininkai galėtų jas suprasti. Todėl blockchain ir išmaniosios sutartys suteikia verslo investuotojams saugią, atvirą, skaidrią, audituojamą ir automatizuotą sandorių aplinką. Jis gali pakeisti prekybos finansavimą supaprastindamas išmaniųjų sutarčių, įmonės išteklių planavimo, žaibo tinklo, išankstinių ir poprekybinių procesų, sąskaitų ir auditų, lojalumo programų ir kt.

## **DECENTRALIZUOTI FINANSAI**

Decentralizuotas finansavimas (DeFi) yra nauja finansų technologija, sukurta blokų grandinės pagrindu. Jis labai skiriasi nuo kitų finansinių tinklų, nes yra atviras ir programuojamas. Išmaniosios sutartys ir jas grindžiančios sąlygos leidžia jai veikti automatiškai be centrinės institucijos. Tai leidžia kūrėjams kurti naujus mokėjimo, investicijų, skolinimo, prekybos ir mainų modelius, nepriklausomus nuo bankų ir kitų institucijų.

Centralizuotuose finansuose jūsų pinigai priklauso bankui, finansų įstaigai ar verslui, garantuojančiam sandorį. Jie gauna didžiulį dividendą iš jūsų pinigų, nes turi daug finansinės laisvės. DeFi išmanioji sutartis veikia kaip finansų įstaigos sandorio pakaitalas. Kai jie pradeda veikti, atitinka tik išmaniąsias sutartis. Šių sutarčių keisti negalima, nes jos visada skirtos automatizavimui.

Decentralizuoti finansiniai protokolai suteikė vartotojams visame pasaulyje prieigą prie daugybės naujų ekonominių galimybių. Tai apima turto valdymą, žetonų sudarymą, žetonų išvestines priemones, decentralizuota autonomiją, duomenų analizę ir vertinimą, mokėjimus, skolinimą ir skolinimą, draudimą, maržų prekybą, rinkas, lošimus ir pelno auginimą. Skaityti

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

## **ETHEREUM KAIP DEFI PLATFORMA**

Ethereum yra novatoriška, algoritmais pagrįsta ekonominė sistema, kurią skatina pasitikėjimas, galimybės ir finansinė prieiga. Jis gali būti panaudotas siunčiant pinigus, naudojant programuojamą valiutą, skolinant ar skolinantis pinigus, dalyvaujant neprarandančiose loterijose, prekiaujant žetonais, kvadratine prekyba, lėšų pritraukimu, sutelktiniu finansavimu, portfelio valdymu ir kt. Be to, prognozavimo rinkoms taip pat gali būti naudinga Ethereum blokų grandinė. keliais būdais - padidinta prieiga, pasipriešinimas cenzūrai ir tarpininkų pašalinimas.

## **PASKIRSTYTI IŠTEKLIAI IR IOT**

Blockchain suteikia saugesnį duomenų saugojimą ir valdymą, o tai suteikia didelę naudą, siūlydama vienodą, sąveikią ir apsaugotą nuo klastojimo architektūrą vyriausybėms, įmonėms, vartotojams ir daiktų interneto valdymo sistemoms. Jis atlieka vidutinio ir užpakalinio biuro funkcijas taip pat, kaip jas atlieka internetas ir žiniatinklio frontas, automatizuoja užduotis, kad padidintų produktyvumą ir atveria naujas verslo galimybes.

IoT sistemų prijungimas prie blokų grandinės užtikrina IoT programų efektyvumą ir duomenų saugumą. Algoritmas gali būti derinamas su nauja lyderio pasirinkimo technika, kad būtų lengviau naudoti blokų grandinę daiktų interneto galutiniuose įrenginiuose, kurių išteklių prieinamumas yra ribotas. Daiktų interneto duomenys, saugomi bendroje blokų grandinės knygoje, leidžia visoms šalims stebėti komponentų kilmę per visą produkto gyvavimo ciklą. Dabar saugu, paprasta ir ekonomiška dalytis visa svarbia informacija su reguliavimo institucijomis, siuntėjais ir gamintojais. Skaityti daugiau, [\*Blockchain for Real World Applications - Rishabh Garg, John Wiley & Sons, Inc. US, 01-388: ISBN - 9781119903734.\*](#)

## **E. VALDYMAS**

Nepaisant to, kad daugelis geekų bandė spręsti saugumo problemas e. valdymo sistemose, esamos sistemos ir modeliai paprastai neatitinka saugumo reikalavimų. Kadangi neįmanoma ignoruoti nepasitikėjimo internetu tarpininkaujamomis operacijomis ir neteisėtos viešai neatskleistos prieigos prie sistemos, blokų grandinės technologijos diegimas yra vienintelis būdas pašalinti šiuos trūkumus. Tai žada veiksmingesnę, saugesnę ir patikimesnę viešąją paslaugą.

Per pastaruosius ketverius ar penkerius metus daugiau nei trisdešimtyje šalių buvo pradėta šimtai blockchain iniciatyvų, skirtų pakeisti vyriausybės sistemas. Estija priėmė ID su blokų grandine, kad būtų galima patikrinti piliečių tapatybę. Blockchain technologija naudojama kuriant elektroninio balsavimo sistemas Australijoje ir Ukrainoje. JAV jis naudojamas saugiai dalytis mediciniais duomenimis, o JK - viešosioms paslaugoms gerinti. Gruzijoje ir Hondūre žemės

registracija tvarkoma naudojant paskirstytų knygų technologiją. Netolimoje ateityje Kinija svajoja pastatyti blockchain miestą.

Automatizuotos blokų grandinės sistemos gali padėti vyriausybėms agentūroms veikti efektyviau, nes sumažėja pastangos, laikas ir išlaidos, paprastai reikalingos rankiniu būdu valdyti prieigą prie savo tinklų. Be to, tai gali palengvinti:

- išduodančiosios ir tikrinančios institucijos duomenų išsaugojimas;
- dokumentų apsauga nuo klastojimo;
- visos svarbios informacijos pateikimas valdžios institucijoms naudojant viešąjį raktą;
- prieiga prie asmeninės informacijos arba originalių dokumentų bet kada ir bet kur naudojant privačius vartotojų raktus;
- sumažinti sukčiavimą, mokesčių slėpimą ir netinkamą veiklą; ir
- šalies ekonomikos skatinimas [Garg, 2020].

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

## **DECENTRALIZUOTAS STRAUKIMAS**

Vaizdo įrašai gali būti linksmi, pamokantys ir suteikiantys galių. Tačiau transliuotojai, įkeliantys vaizdo įrašą į internetą, pirmiausia turi jį perkoduoti. Jis sunaudoja iki 80% viso interneto pralaidumo, todėl vaizdo transliacija yra labai brangi. Vaizdo įrašų infrastruktūra reikalinga norint teikti labiau keičiamus ir ekonomiškus sprendimus, o norint tai pasiekti, tokios technologijos kaip blockchain gali leisti programų kūrėjams vaizdo įrašų perkodavimo rinkoje prieiti prie įvairesnių paskirstytų procesorių, kurie yra prieinami, saugūs ir ekonomiški.

## **DVIGUBA KASDYBA**

Dviguba kasyba – tai praktika, kai ta pačia pavara atliekamos skirtingos operacijos. Pirmą kartą ši frazė pasirodė PoW kasybos kontekste, kur ji apibūdino kelių kriptovaliutų gavybą vienu metu naudojant vieną GPU, kad būtų paleistas PoW maišos algoritmas. Dviguba kasyba - naudojant GPU kriptovaliutoms, pvz . Ethereum, išgauti, taip pat naudojant jį vaizdo įrašams perkoduoti kaip vaizdo įrašų kasyklą savo tinkle - vis tiek gali būti įmanoma transliuoti vaizdo įrašus. Vienas iš perkodavimo kaip papildomos dvigubos kasybos veiklos pranašumų yra tas, kad jis naudoja mažiau GPU branduolių nei kiti galimi darbo krūviai, nes GPU aparatinės įrangos koduotuvai ir dekoderiai atlieka didžiąją darbo dalį.

## **NUOLAT PLEČIANTIS TINKLAS**

Nuolat besiplečiantis blockchain tinklas apima daugybę realaus pasaulio aspektų, įskaitant žmogiškųjų išteklių valdymą, teisėsaugą, viešąją pagalbą, gerovės pristatymą, pašto paslaugas, sąskaitas ir mokėjimus, mokesčius, vaistus, skiepijimą ir bendruomenės sveikatą, atsiskaitymą su medikamentais, draudimą, gabenimą, krovinių gabenimas, viešasis transportas, kelionės ir mobilumas, pavėžėjimas, kelionės lėktuvu, daiktų internetas, informacija ir ryšiai, pranešimų

siuntimas, svetingumas, pramogos, lošimai, maistas ir gėrimai, žuvininkystė, gyvulininkystė, žemės ūkis ir gamtos ištekliai, infrastruktūra ir energetika, gamyba, nekilnojamasis turtas, statyba, transporto priemonės, testamentai ir palikimai.

## TRUMPAI TARIANT

Blockchain nežada per naktį padaryti vartotojo milijardieriumi arba pasiūlyti mechanizmo, kaip apsaugoti jų finansines operacijas nuo politiškai įkvėptų vyriausybių. Tačiau akivaizdu, kad tiesa yra tai, kad jis siūlo naują požiūrį į administracinių ir ekonominių organizacijų struktūrizavimą, tuo pačiu žymiai sumažinant pasitikėjimo išlaidas taikant radikalų, decentralizuotą knygos metodą.

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

## NUORODOS

- 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.