



Blockchain for Real World Applications

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

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

Denne boken forklarer blokkjedeteknologiens mange-fasetterte natur og dets manipulasjonssikre økosystem for å utføre aktiviteter i den virkelige verden som utdanning, helsevesen, eiendom, transport, bank, forretning, forsyningskjedestyring, e-handel og desentralisert finans. Leserne vil oppdage den potensielle bruken av blockchain- teknologi i alle viktige samfunnslag og lære å håndtere transaksjonsprosedyrer. Fortellingen er klar, med flotte kunstverk, og vil garantert begeistre leserne. Med sin enkle håndtering av et komplekst emne, er denne boken en skatt for enhver lærd og gründer.

*Indraneel Shankar Dani,
tidligere tilleggssekretær, MP, India.*

Vi er midt i en annen stor revolusjon kalt BLOCKCHAIN, en distribuert database som opprettholder en stadig voksende liste over poster, kalt blokker. Dette innovasjonslandskapet representerer bare 12 års arbeid av en elitegruppe av nerder, kryptografer og matematikere.

I tider som kommer vil blockchain gjennomsyre alle menneskelige sysler, og gjøre prosesser effektive og smarte. Etter hvert som det fulle potensialet til disse gjennombruddene realiseres i samfunnet, vil ting gradvis begynne å skje annerledes – internasjonale pengeoverføringer vil være raskere og mer pålitelige; verifisering vil være lett; identitet vil være global, desentralisert; og ingen person – enten administrator, leder, industrimann, oppstart, arbeidsgiver, tjenesteleverandør, pedagog, student eller bruker, vil forbli uberørt. Det er klart at verden må omfavne denne teknologien med åpne armer.

I lys av dette mener forfatteren sterkt at alle deler av samfunnet bør gjøres oppmerksomme på blockchain, enten det er en spirende teknolog, en nystartet entusiast eller en ikke-teknisk bruker av desentraliserte apper. Denne artikkelen, som har blitt hentet ut boken, '**Blockchain for Real World Applications**, skrevet av **Rishabh Garg** og utgitt av *John Wiley & Sons Inc. USA*, gir en grundig forståelse av blockchain - økosystemet, arkitekturen, Ethereum, Hyperledger og kryptovalutaer, etterfulgt av en omfattende diskusjon om potensiell bruk av blokkjede som kryptografi, cybersikkerhet, identitetshåndtering, legitimasjonsverifisering, jobbsertifisering, helsetjenester, eksternt helseovervåking, organtransplantasjon, genomikk, farmasøytisk forsyningskjede, mat og sivile forsyninger, etc. Live skjermbilder og tilhørende kodeceller, gitt mellom teksten, vil hjelpe leserne til å forstå bank, business, desentralisert finans,

prediksjonsmarked, porteføljestyring, kvadratisk finansiering, crowdfunding, e-handel etc. med en *de novo* nærme seg.

Innholdet gir en praktisk trinnvis mekanisme for hver leser å implementere sitt eget innholdsbaserte lagringssystem. Vår tilnærming er å hjelpe deg med å betjene denne revolusjonerende teknologien ved å introdusere deg til hver detalj. Med denne nye teknologien under din kontroll, vil du kunne få tilgang til funksjonene til blockchain like enkelt som å bruke en enkel mobilapp. Så, bli med i blokkjederevolusjonen; lære å utvikle desentraliserte applikasjoner; og gå foran dine jevnaldrende.



Rishabh Garg | BITS India | Grunnlegger og administrerende direktør, Scholars Park har jobbet i Data Science for Indian Institute of Technology, New Delhi; en merkevarepartner med kyvette; en SDE med ServiceNow, Swiggy og Ethan AI. Han har oppnådd en spesialisering i Blockchain fra University of Buffalo, NY; Anvendt datavitenskap med Python fra University of Michigan, USA; og Investment Management fra Universitetet i Genève, Sveits (gjennom MOOC).

Han har skrevet en bok om **Blockchain for Real World Applications** (*John Wiley & Sons Inc. US*) og en annen om **Self Sovereign Identities** som ble utgitt på seks internasjonale språk i Tyskland, Frankrike, Italia, Moldova, Spania og Portugal. Han er Journal Referee med IEEE Internet of Things, og programkomitémedlem cum anmelder for internasjonale konferanser organisert av AIRCC i Toronto (Canada), Youngs (Australia) og London (Storbritannia).

Rishabh er mottaker av National Award for Exceptional Achievements in Innovation fra **Indias president** og National CSIR Innovation Award fra **Indias statsminister**.

Blokkjede: En Overhåndende Revolusjon

Bokføring har vært en hjørnestein i sivilisasjonen siden den babylonske tiden fordi utveksling av verdi krevde at to fremmede kunne stole på hverandres kontoer. Vi trenger fortsatt et integrert system som kan registrere alle våre transaksjoner, holde samfunnet organisert og opprettholde offentlig tillit [**Garg, 2023**]. Les mer, [Blockchain for Real World Applications - Rishabh Garg. John Wiley & Sons, Inc. US, 01-388: ISBN - 9781119903734](#).

Den tekniske arkitekturen og protokollene til **Distributed Ledger Technology** (DLT) tillater samtidig tilgang, verifisering og irreversibel oppdatering av data over et nettverk som spenner over flere noder eller lokasjoner. Blockchain er en av dens mange former som **DAG**, **Hashgraph**, **Holochain** og **Tempo** (Radix). Blockchain er en nært forestående revolusjon og en helt ny apputviklingsprotokoll. I likhet med Internett for et kvart århundre siden, kan blokkjedeapplikasjoner gjennomsyre hverdagen vår i de kommende årene [**Garg, 2022**].

Blockchain er i hovedsak en digital hovedbok som sporer transaksjoner. Transaksjoner kan betegne hva som helst – kontanter, digitale valutaer, aksjer eller andre eiendeler. Blockchain er i stand til å tilfredsstille et bredt spekter av vilkår og betingelser for å anskaffe eller gjøre opp disse eiendelene gjennom såkalte smarte kontrakter.

Måten transaksjoner registreres på flere datamaskiner innenfor et desentralisert nettverk skiller blokkjeden fra den enkle hovedboken. Når en konsensus er oppnådd, oppdaterer hver node på nettverket sin egen kopi av hovedboken. I mangel av konsensus, slutter resten av nettverket øyeblikkelig å forsøke å legge til eller fjerne en node.

Blokkjeden bruker triple-entry accounting, der en oppføring gjøres på kredittsiden, den andre på debetsiden og den tredje på den uforanderlige delte hovedboken – administrert av avanserte matematiske algoritmer og ugjenomtregelig kryptografi. Les mer, *Blockchain for Real World Applications - Rishabh Garg. John Wiley & Sons, Inc. US, 01-388: ISBN - 9781119903734*.

Blockchain er en serie blokker som danner en omfattende liste over transaksjoner som overføres og replikeres over nettverket som en digital offentlig hovedbok. Blockchain-økosystem består av **noder** – brukere eller datamaskiner – som opprettholder en fullstendig kopi av posten eller hovedboken, mens **blokker** er dataformater som brukes til å lagre poster over transaksjoner og overføre dem mellom alle noder i nettverket [**Garg, 2021**].

Stuart Haber og W Scott Stornetta [1991] var de første som introduserte konseptet blokkjede. Men Satoshi Nakamoto, personen bak pseudonymet, populariserte det i 2008 slik at det kunne tjene som en offentlig logg over bitcoin- transaksjoner. Programmerbare smarte kontrakter, konstitusjonell design og blockchain-konsensusprotokoll har vært kjerneområder for innovasjon det siste og et halvt tiåret.

TIDSLINJE FOR BLOKKJEDE

I løpet av de siste 15 årene har det vært mye innovasjon innen blockchain-konsensusteknologier, programmerbare smarte kontrakter og fidusiar arkitektur.

BLOKKJEDE 1.0

Blockchain 1.0 ble brukt som en digital valuta for handel i stor skala, transaksjoner med små verdier, valuta, spill og hvitvasking av penger. Det er mange fordeler med å bruke blokkjedeteknologi for digital valuta, men den grunnleggende fordel er at den gir en trygg og sikker plattform for aktivaoverføringer uten behov for mellommenn eller motparter. Mer enn 4500 forskjellige varianter av kryptovalutaer er nå tilgjengelig. De mest populære er Bitcoin (2009), Litecoin (2011), Namecoin (2011), Dogecoin (2013) og Peercoin, med en total markedsverdi på USD 295 milliarder (2012).

BLOCKCHAIN 2.0

Utvidelsen av Blockchain 2.0-applikasjoner muliggjorde smartkontrakter, desentraliserte applikasjoner (dApps) og desentraliserte autonome organisasjoner (DAO). Det spilte en sentral rolle i spesifikke områder av finans - bank, aksjehandel, kredittsystemer, forsyningskjedefinansiering, betalingsclearing, anti-forfalskning, gjensidig forsikring og forstyrrelse av tradisjonelle valutaer og betalingsmetoder. Det lettet implementeringen av smarte kontrakter ved å bruke noen programmerbare kontraktsspråk, inkludert Ethereum, Codius og Hyperledger.

BLOCKCHAIN 3.0

I tillegg til valuta og finans har Blockchain 3.0 vært i stand til å etablere dominans innen områder som utdanning, helse, vitenskap, transport og logistikk. Det innebærer en mer sofistikert type smart kontrakt for å skape en desentralisert organisatorisk enhet som lager sine egne regler og gir betydelig autonomi.

BLOCKCHAIN 4.0

Blockchain 4.0 utvikler seg til et forretningsvennlig økosystem for massene. Det er en fusjon av blokkjede med de mest omfattende alternativene for fremtidens banebrytende teknologier som Internet of Things, cloud computing, kunstig intelligens og robotikk. Ved å undersøke potensialet til virtuelle blokkjeder i en enkelt blokkjede, kan systemet oppnå uhemmet skalerbarhet. Blockchain 4.0 refererer til ideer og løsninger som rasjonaliserer teknologi for forretningsbehov, spesielt industri 4.0 og handel. Blokkjedeteknologi kan brukes til å forbedre en rekke prosesser, inkludert forsyningskjedestyring, bedriftsarbeidsflyt, finansielle transaksjoner, IoT -datainnsamling, helseovervåking, kapitalforvaltning og kredittsystemer.

Dermed lover blockchain 4.0 en digital arkitektur som kombinerer automatisering, ansvarlighet og personvern for å generere en friksjonsfri opplevelse i den virkelige verden [**Garg, 2021; 2023**].

BLOKKJEDEARKITEKTUR

Blockchain verifiserer gyldigheten av transaksjoner gjennom en asymmetrisk kryptografiteknikk. Her brukes en matematisk prosess kjent som **hash-funksjon** for å konvertere data til en streng med alfanumeriske verdier. Det er en prosess som kalles **kryptering** som krypterer den lesbare teksten som kun kan leses av personen som har den hemmelige koden eller dekrypteringsnøkkelen. Det er to hovedformer for kryptering – **asymmetrisk kryptering** (offentlig nøkkel) og **symmetrisk kryptering**. Symmetrisk kryptering har kun én privat (hemmelig) nøkkel, og brukes av alle kommuniserende parter for både kryptering og dekryptering.

Her fungerer feltet hash og krypterte transaksjonsdata som en digital signatur. Den originale kopien av dataene og en sikker hash av dataene sendes til mottakeren. Mottakeren beregner en ny hash ved å bruke de originale dataene som er hentet etter dekryptering av den sikre hashen. Hvis begge er like, betyr det at de mottatte dataene ikke er endret.

DESENTRALISERT IDENTIFIKASJON

Desentraliserte IDer muliggjør peer-to-peer-forbindelser mellom to parter som er globalt unike, seige og pseudo-anonyme. DID-er gir identitetseierkontroll og suverenitet over identiteter fordi de ikke er avhengige av sentraliserte registre, myndigheter eller identitetsleverandører. Siden en person kan ha flere DID-er, er det vanskeligere å overvåke dem i alle deres aktiviteter. Les mer, [*Blockchain for Real World Applications - Rishabh Garg. John Wiley & Sons, Inc. US, 01-388: ISBN - 9781119903734.*](#)

ØKOSYSTEM FOR BLOKKJEDE

Et blokkjede-økosystem er et nettverk av brukere som deler noder for felles forretningsaktivitet og formål. Hver blokkjedeblokk inneholder omtrent 1 MB data. Når 1 MB datakapasiteten til den første blokken er fylt, lagres informasjonen kronologisk i denne blokken før den gjentas i den andre blokken [Garg, 2021].

Hver blokk mottar en annen hash som nøyaktig samsvarer med datastrengen i den blokken for å knytte alle disse blokkene sammen i en sekvens. En blokk mottar en ny hash selv om det er en mindre endring i den. Systemet er avhengig av desentraliserte databaser for å kontrollere fremveksten av data mellom enheter via et P2P (peer-to-peer) nettverk, der konsensusmetoder sikrer replikering på tvers av noder i nettverket.

De enkelte nodene utgjør et blokkjede-økosystem, og hver har sin egen kopi av hovedboken. Noder kommuniserer med hverandre for å bli enige om en hovedbokpost, noe som eliminerer behovet for en sentral myndighet eller en tredjepart for å koordinere eller verifisere. I tillegg til overføring og verifisering av tilførte data på blokkjeden, hjelper noder også med å legge inn nye data. Handlingen med å registrere transaksjoner på en ny blokk og legge dem til en eksisterende kjede kalles **mining** og det skjer når alle noder når en konsensus. I en blokkjede har hver blokk sin egen nonce og hash, som innledes med hashen til blokken i kjeden.

En kryptografisk hash-funksjon genererer en hash i en blokkjede, som gjør hver inngangsstreng til en utgangsstreng med 64 sifre. Ikke alle hashes er gyldige. Hashen til en blokk må starte med minst ti påfølgende nuller for å være kvalifisert på blokkjeden. Hver blokk mottar en **nonce**, som er en liten mengde unike data. Gruvearbeidere må kontinuerlig engasjere seg i gruvedrift, som er prosessen med konstant å modifisere og hashe blokkens data på jakt etter en brukbar hash. For å finne en gyldig signatur (utgang), må gruvearbeidere hele tiden endre blokkstrukturen (nonce) og bruke mye strøm. Jo mer regnekraft de har, jo raskere behandler de de ulike blokksammensetningene for å finne en god hash.

OFFENTLIG OG PRIVAT BLOKKJEDE

Det er tre hovedtyper blokkjeder : offentlige, private og konsortium -blokkjeder . Enhver bruker som ønsker å engasjere seg i nettverkstransaksjoner kan gjøre det på en **offentlig blokkjede** uten begrensninger. På den annen side, på **private blokkjeder**, kan bare noder fra en bestemt organisasjon delta i konsensusprosessen. Derfor er det også kjent som permissioned blockchain. **Consortium blockchain** er et semi-privat nettverk av likesinnede virksomheter for å øke produktivitet, ansvarlighet og åpenhet.

KONSENSUS FOR BLOKKJEDE

For å oppnå konsensus om tilstanden til blokkjeden og sikre gyldigheten av transaksjoner, brukes en feiltolerant mekanisme, som kalles **konsensusmekanismen**. I dette er den nåværende tilstanden til den distribuerte hovedboken avtalt av hvert medlem av blokkjedenettverket. For å

legge til en ny blokk i kjeden, må en node utføre en databehandlingsoppgave, kjent som **Proof-of-Work**. PoW er en form for konsensus som bitcoin-nettverket bruker. Mye energi er bortkastet i disse operasjonene fordi PoW krever at gruvearbeidere utfører enorme beregninger. **Proof-of-Stake** er et mindre energikrevende alternativ til PoW som krever at gruvearbeidere beviser at de er de legitime eierne av valutaen. Dette er basert på et ulogisk premiss om at brukere med mer valuta har mindre sannsynlighet for å angripe nettverket. Flere konsensusalgoritmer har blitt foreslått for å overvinne dette utføret, inkludert **PBFT, DPoS, Peercoin, Ripple, Tendermint**, etc.

For å sikre effektivitet, sikkerhet og bekvemmelighet har noen arbeidere foreslått det grådige tungobservasjonsundertreet (**GHOST**) kjedevalgsregel. I dette systemet veies grener av GHOST slik at gruvearbeidere kan velge den beste grenen å følge, i stedet for den lengste grenplanen [Simpolinski og Zohar, 2013].

BETALINGSVERIFIKASJON I BLOCKCHAIN

Det er to mulige typer betalingsverifikasjoner: Enkel betalingsverifisering og Full betalingsverifisering.

Som en del av SPV-prosessen (**Simple Payment Verification**), kan en tynn eller lett klient laste ned blokkhodet, som er mye lettere enn hele blokken. Det er enklere og mer nyttig for brukeren å lagre bare én kopi av blokkhodet fra den lengste proof-of-work- kjeden og få tak i Merkle - grenen som knytter transaksjonen til blokken. Verifikasjon er pålitelig så lenge ærlige noder har kontroll over nettverket. Men i det øyeblikket en angriper tar kontroll over nettverket, blir systemet avslørt.

I kontrast krever **full betalingsverifisering** en tykk eller tung lommebok, som er en komplett kopi av blokkjeden. Disse lommebokprogrammene validerer og videresender andres handler i tillegg til å administrere brukerens egne transaksjoner. For å gi personlige resultater og velge blokkjeden med høyest bevis på arbeid, må alle parter (alle noder) på nettverket være tilkoblet. Avhengig av tilkobling kan det derfor ta flere dager før et blokkjedenettverk blir lastet ned ved hjelp av bitcoin wallet-applikasjonen. Les mer, [Blockchain for Real World Applications - Rishabh Garg, John Wiley & Sons, Inc. US, 01-388: ISBN - 9781119903734](#).

KRYPTOVALUTA

Kryptovalutaer , som Bitcoin, Ether eller Litecoin, er digitale tokens som handles på en blokkjede og brukes til å kjøpe produkter og tjenester. Blokkjedeteknologi brukes av kryptovalutaer for å utfylle fordelene med en offentlig hovedbok og et sofistisert kryptografisk sikkerhetssystem. Gjennom årene har disse valutaene blitt utrolig populære, noe som har ført til eksistensen av mer enn 18 000 kryptovalutaer over hele verden med en markedsverdi på 3,2 billioner dollar. En bitcoin er for tiden verdt 3 120 210,68 INR.

SKRIFTER

Skript anses som en av de grunnleggende hensynene i implementeringen av forretningslogikklaget på blokkjeden. Enkelt sagt er bitcoin- transaksjoner informasjon som gjenspeiler bevegelsen av bitcoins fra en lommebok til en annen. Vanligvis skaper den første transaksjonen i en ny blokk ny valuta, men bruker den aldri. I disse transaksjonene er inngangen tom og en slik tom inngang kalles en **Coinbase- transaksjon** . Belønningen som skapes av denne transaksjonen kan også distribueres til en eller flere lommebokadresser som en typisk bitcoin- transaksjon. Etter at et spesifikt antall vellykkede blokker er bidratt, halveres belønningen for hver vellykket blokk som legges til blokkjeden, og opprettholder bitcoin som en begrenset forsyning, inflasjonsbestandig ressurs.

Siden Bitcoin ikke er en form for offentlig utstedt lovlig betalingsmiddel, har populariteten skapt nye veier for å kunne byttes mot fiat-penger, for eksempel kryptovalutautveksling, bitcoin - debetkort, bitcoin -minibanker, Metal Pay og peer-to-peer-nettverk. Opprinnelig ble peer-to-peer- kryptovalutaen kjent som Bitcoin brukt til vanlige transaksjoner, men Bitcoin endret seg over tid fra en krone til et investeringsmiddel etter hvert som den ble populær og økte i verdi.

Det ble antatt at blokkjedeteknologien den opererte på manglet skalerbarhet siden den i seg selv ikke var i stand til å håndtere store transaksjonsvolumer. Dermed, i august 2017, den opprinnelige kryptovalutaen Bitcoin delt inn i to forskjellige kryptovalutaer, **Bitcoin Cash** og **Bitcoin SV**. I november 2018 opplevde kryptovalutaen en annen gaffel, og delte seg inn i **Bitcoin Cash ABC** og **Bitcoin Cash SV (Satoshi Vision)**. Fordi den bruker den originale Bitcoin Cash-klienten, blir Bitcoin Cash ABC nå referert til som Bitcoin Cash.

Utviklere kan bruke smarte kontraktsspråk som CashScript for å muliggjøre mer komplekse operasjoner med Bitcoin Cash enn med Bitcoin. Bitcoin Cash kan være en hard ressurs, for eksempel eiendom, gull eller andre fysiske varer, ettersom Bitcoin har en hard cap på 21 millioner mynter, noe som lar brukere beholde verdi i digital form i svært lang tid.

ETHEREUM

Ethereum er en variant av blockchain laget av den russisk-kanadiske programmereren Vitalik Buterin og hans kolleger. Ethereum er en desentralisert blokkjedeplattform som ble bygget med en delt global infrastruktur. Hver node i nettverket kjører et operativsystem - Ethereum Virtual Machine, som har evnen til å forstå og kjøre programmer kjent som smarte kontrakter. Dermed forsterker Ethereum fordelene med bitcoin blockchain ved å gjøre det mulig for programmerere å skrive kode som emulerer den grunnleggende funksjonaliteten til en desentralisert app eller dApp.

SMARTE KONTRAKTER

Smart kontrakt er en applikasjonskode lagret på en bestemt adresse (kontraktadresse) på blokkjeden. Applikasjoner kan implementere driften av smarte kontrakter, endre deres tilstander og starte transaksjoner. Et spesialisert programmeringsspråk, som Solidity eller Viper, brukes til

å lage slike kontrakter. Uttalelser som "hvis ... da" brukes ofte til å utføre kontraktene. Les mer, [Blockchain for Real World Applications - Rishabh Garg. John Wiley & Sons, Inc. US, 01-388: ISBN - 9781119903734.](#)

HYPERLEDGER

Hyperledger er en global åpen kildekode-samarbeidsinnsats som gir rammeverket, standardene, retningslinjene og verktøyene som trengs for bruk i en rekke bransjer. Den ønsker ethvert fellesskapsmedlem med programmeringskunnskap eller interesse velkommen til å bidra til utviklingen av kildekode. Koden kan gjennomgås, opprettes, endres eller distribueres av enhver programmerer i verden.

Bare de enhetene eller enkeltpersonene som har et autorisasjonssertifikat kan sjekke transaksjoner på Hyperledger- nettverket. Bedrifter som private eller B2B som ikke vil ha sin personlige informasjon på en offentlig blokkjede, kan bruke dette blokkjedenettverket med tillatelse og begrenset tilgang – Ethereum Hyperledger .

DESENTRALISERT APPLIKASJON

I et sentralisert system kan applikasjonsprogramvare plasseres på en eller flere sentrale steder, avhengig av størrelsen på klientbasen som er installert. Men i et desentralisert system brukes smarte kontrakter for å gjøre det mulig for applikasjonsprogramvare å kjøre uavhengig på et peer-to-peer blockchain-nettverk, i stedet for på en enkelt maskin. En **desentralisert applikasjon** (dApp) utgjør en front-end, en blockchain back-end og mellomvare – programvaren som forbinder de to.

Selv om dApps lover å løse mange av de store bekymringene med tradisjonelle apper, har de også en rekke ulemper, for eksempel vedlikeholdskrav, betydelige ytelseskostnader, overbelastning av nettverket, etc.

IDENTITETSBEKYRINGER

Identitet er sentralt i alle menneskelige aktiviteter. En gyldig identitet er en forutsetning for skoleregistrering, arbeidssøknader, drift av bankkonto, skaffe pass, signering av kontrakter eller tilgang til økonomisystemet [Garg, 2019]. Imidlertid har mer enn en milliard individer, inkludert 21 millioner flyktninger, fortsatt ikke en juridisk identitet. Dette skyldes skjulte kostnader, intervensjon fra mellommenn og kjedelige prosesser.

IDENTITETER OVER HELE VERDEN

Mennesker rundt om i verden har ulike former for identitet, for eksempel pass for internasjonale reiser, førerkort for å kjøre kjøretøy, velgerkort for valg, personnummer for å føre regnskap over lønn eller selvstendig næringsvirksomhet, osv. [Garg, 2020]. Historien om identifikasjonssystemet begynner trolig i 1803, da Napoleon Bonaparte introduserte det første identifikasjonssystemet i verden.

Den franske regjeringen innførte et identitetskort for arbeidere med sikte på å bruke det som et verktøy for å forvandle det ubegrensede samfunnet i den franske republikken til en velorganisert politistat slik at arbeidere ikke kunne migrere til bedre jobber og høyere lønn uten arbeidsgivers tillatelse . Napoleons ID-plan var en lignelse for menneskehandel og slaveri i Russland eller Øst-Europa, men den kunne ikke blomstre på grunn av mangel på arbeidskraft og fremveksten av selvhjelpsorganisasjoner under verdenskrigene [Lyon, 1994].

På 1900-tallet var Tyskland blitt en svært demokratisk, tolerant og liberal nasjon med velferdsordninger, sosialforsikring og nasjonale helsetjenester. I et slikt miljø var nazistene besatt av den økonomiske verdien av arbeidere, tilbakeholdelse av lønn, fjerning av streikende og funksjonshemmede. Nazistene introduserte en arbeidsbok for å registrere hver enkelt ansatts arbeidshistorie, inkludert perioder med permittering og brudd på arbeidskontrakter. Dens tilslørte motiv var å identifisere de streikende, de svake, de arbeidssky, de udisponerte, seksuelt promiskuøse, hemmelige prostituerte og subproletariatet. Ordren ble avvist først i 1941-42, da krigen snudde mot Tyskland [Gotz og Roth, 2004; Black, 2012].

Kina utvidet nazistenes arbeidsbok ved å tilpasse den til et system kalt dangan- dossier , som sørget for sammenstilling av personlige poster fra skoledagene. Arbeidere kunne ikke starte et nytt yrke før dang-an-dossieret deres ble sendt av den tidligere arbeidsgiveren. Dette nye systemet var helt annerledes enn det historiske systemet, Dang-e, som var ment å føre tilsyn med adelen.

I tillegg eksisterte et såkalt nasjonalt registreringssystem i Kina som hindret kinesiske arbeidere i å flytte til et annet område uten tillatelse. På 1990-tallet begynte dangan- systemet å bryte sammen på grunn av kreftene som oppsto fra globaliseringen. Utenlandske firmaer som kom inn i Kina førte ikke dangan- registre og ansatte migranter på landsbygda uten dang-an-dossier.

Samtiden med ID-kort begynte med andre verdenskrig. I 1938 vedtok Storbritannia National Registry Act, som påla alle innbyggere å ha et identitetskort [Whitley og Hosein, 2009]. I 1940 etablerte Vichy-regjeringen i Frankrike et ID-system med Hellas og Polen, som er mer eller mindre beholdt til dags dato. Med unntak av noen få unntak, har knapt noe land, med sedvanerett, i verden vedtatt et identifikasjonssystem i fredstid.

Adopsjonen av ID-kort i Asia ble reflektert i en boom etter andre verdenskrig. Hong Kong-regjeringen introduserte et identitetskort i 1949 for å forhindre innvandring fra fastlands-Kina og styrke suvereniteten. Taiwan i 1949, Sør-Korea og Singapore på 1960-tallet fulgte etter i påskudd av økonomisk transformasjon.

MODERNE IDENTITETER

I USA utstedes et nisifret personnummer (SSN) til alle amerikanske statsborgere, fastboende og midlertidige innbyggere over 18 år. Selv om det opprinnelig var ment å identifisere enkeltpersoner for trygdeformål, er det nå også brukes til å spore enkeltpersoner for skatteformål.

I praksis har det blitt et de facto nasjonalt identifikasjonsnummer på grunn av dets brede spekter av bruksområder, for eksempel å åpne en bankkonto eller søke om førerkort.

Social Insurance Number ble introdusert i Canada, men endte i 2004 med introduksjonen av personlig informasjonsbeskyttelse og elektronisk dokument som ekte ID-numre.

I Colombia får hver person i barndommen utstedt et grunnleggende identifikasjonskort kalt Tarjeta de Identidad som inkluderer fødselsdato og et lite serienummer. Ved fylte 18 år får hver borger på nytt utstedt et statsborgerskapskort (Cedula de Ciudadanía), som er avgjørende i alle offentlige og private saker.

I Mexico heter identifikasjonsnummeret Clave Única de Registro de Población (CURP). Selv om forskjellige andre IDer, for eksempel personnummeret, tildelt av Instituto Mexicano del Seguro Social, og Registro Federal del Contribuyente (RFC) tildelt av statskassen, er også på moten, men valgt, Credencial de Elector eller Credencial del INE, utstedt av Instituto Nacional Electoral gis den høyeste anerkjennelsen.

Et nasjonalt identitetskort, Documento Nacional de Identidad (DNI), er utstedt av Registro Nacional de las Personas på fødselstidspunktet i Argentina, bortsett fra innvandrere som mottar tall som starter med 92 000 000. Denne ID-en kreves for å søke om kreditt, åpne en bankkonto og utøve franchiseretten. Siden foreldre er pålagt å registrere barna sine, blir de fattige, og spesielt foreldreløse, utelatt.

Brasil har to systemer – for det første Registro Geral (RG) som er et nummer tildelt av stater og noen organisasjoner som de væpnede styrkene som en autorisert nasjonal ID. Siden disse er tildelt på statlig nivå, er det mulig å ha samme RG-nummer for to borgere i forskjellige stater

Det andre systemet, Cadastro de Pessoas Físicas (CPF), er et føderalt og unikt, men det ble opprinnelig opprettet for skatteformål. I Brasil er ett eller begge numrene nødvendige for visse vanlige oppgaver, for eksempel å åpne en bankkonto eller skaffe førerkort.

Innenfor Det europeiske økonomiske samarbeidsområdet og Sveits utstedes det europeiske helsetrygdkortet for helseformål. Dette kortet viser en kode som kalles et identifikasjonsnummer. I Finland har den personlige identifikasjonskoden, henkilötunnus (HETU eller svensk – Personbeteckning) vært på moten siden 1964 og brukes til å identifisere borgere for offentlige og bedriftstransaksjoner.

I Frankrike brukes INSEE-koden som oppsto under Vichy-regimet for identifikasjon, sosialforsikring, sysselsetting og skatteformål. I Tyskland ble det fra 2007 bare vedlikeholdt en desentralisert database av sosialforsikringselskaper, som tildelte et personnummer til nesten hver person. Etter 2008 ble de tidligere skattefilnumrene erstattet av nye skattebetalers identifikasjonsnumre, Steuerliche Identifikationsnummer eller Steuer-IdNr. Personer som er både arbeidstaker og selvstendig næringsdrivende på samme tid kan få to skattyter-

identifikasjonsnummer. Det tilsvarende nummeret for organisasjoner er utstedt av Federal Central Tax Office, og heter Wirtschafts-Identifikationsnummer.

I Italia utstedes en finanskode (Codicefiscale) i formatet SSSNNYYMDDZZZZX på fødselstidspunktet. SSS er de tre første konsonantene i familienavnet (hvis det ikke er nok konsonanter den første vokalen, så brukes X); NNN er fornavnet, hvorfra den første, tredje og fjerde konsonanten brukes; YY er de to siste sifrene i fødselsåret, M er bokstaven som er tilordnet fødselsmåneden, DD er de to siste fødselsbokstavene; ZZZZ er det spesifikke retningsnummeret for kommunen der personen ble født; X er et paritetskarakter som beregnes ved å legge sammen bokstavene i partall og oddetall. Månedens bokstaver brukes alfabetisk, men bare bokstavene A til E, H, L, M, P, R til T brukes (således er januar A og oktober R); For å skille mellom kjønn legges 40 til fødselsdagen for kvinner; og for utlendinger brukes en landsdekkende kode i stedet for en kommunekode.

Gambia og Nigeria tildeler 11-sifrede identifikasjonsnumre til sine innbyggere kalt nasjonale identifikasjonsnummer [NIMC, 2022].

Det nasjonale ID-nummeret i Zimbabwe er en alfanumerisk kode på elleve tegn som administreres av kontoret til generalregistratoren. Den har et 2-sifret prefiks som angir distriktet der søkeren er bosatt; de neste seks sifrene representerer søkerens unike personlige kode; og de to siste sifrene er prefikskoden til det nasjonale ID-nummeret til de opprinnelige foreldrene.

I Folkerepublikken Kina er et 18-sifret ID-kort i formatet RRRRRRRYYMMDDSSSC obligatorisk for alle borgere over 16 år. RRRRRR er en standardkode for den administrative inndelingen i fylket eller byen der innehaveren er født; ÅÅÅÅMMDD er fødselsdatoen til innehaveren; og SSS er en sekvensiell kode for å skille personer med samme fødselsdato og fødselssted [Shaw, 1996; Perry, 1997]. Den sekvensielle koden er oddetall for menn og partall for kvinner.

Indonesia har rullet ut et 16-sifret RFID-kort med elektronisk signatur, irisskanning, ti-fingers fingeravtrykkskanning og et høyoppløselig pass under navnet e-KTP (Electronic Kartu Tanda Penduduk) siden 2012. Dette programmet er designet på grunnlag av UIDAI of India.

India har i flere tiår forsøkt å gi en offisiell identitet til alle sine innbyggere. Så langt har utallige ID-er blitt flyttet og rullet tilbake, noe som har ført til en tilstand av fluks og forvirring blant innbyggerne [Garg, 2017]. Begrensningen for eksisterende ID-er er at de kun tjener forskjellige og begrensede formål. Videre er det ikke uvanlig å finne avvik i innbyggerens profil mellom ulike depoter, noe som forårsaker forvirring og feil [Garg, 2018; 2019].

Ideen om et biometrisk aktivert unikt identifikasjonsnummer (UID), eller Aadhaar, ble foreslått av Institutt for informasjonsteknologi, Indias regjering, med sikte på å gi en autentisk identitet til alle innbyggere i India. Mer enn én milliard innbyggere har blitt koblet til ordningen, som anslagsvis 130 milliarder INR (UIDAI, 2022) har blitt brukt på så langt. Det er verdens største

biometriske identifikasjonssystem som tar sikte på å gi identitet til alle slike innbyggere som mangler en individuell identitet.

Blockchain Innovations

A Quarterly Newsletter by Scholars Park

25 September, 2021

www.scholarspark.wordpress.com

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
NEW DELHI, SEPTEMBER 22

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 registers.

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 revolutionise the health facilities of India. This

Unique health ID: Modi launches Ayushman Bharat Digital Mission

technology had helped the country deal with the pandemic. He said the digital health ID will be used to create a unique health ID for every citizen. He said the digital health ID will be used to create a unique health ID for every citizen. He said the digital health ID will be used to create a unique health ID for every citizen.

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

आय के आधार पर की सेवाएं देते हैं और वो भी वे सार्वजनिक... 2018 में ही शुरू होकर... 2018 में ही शुरू होकर... 2018 में ही शुरू होकर...

Modi launches digital Ayushman health IDs

श्रम ने बनाया जैनारिक इनफार्मेशन टैकर... 2020 तक एनएनडी... 2020 तक एनएनडी... 2020 तक एनएनडी...

डीपीएस के ऋषभ गर्ग को मिला सीएसआईआर इनोवेशन अवॉर्ड

प्रेस नोट में भी सार्वजनिक... 2020 तक एनएनडी... 2020 तक एनएनडी...

DPS BOY SHINES AT INDIAN INTERNATIONAL SCIENCE FESTIVAL

Rishabh Garg, a student of Delhi Public School, Bhopal was invited for the 2nd Indian International Science Festival, 2016. The Ministry of Science & Technology, Ministry of Earth Science, Ministry of Process Research and Advanced Material & Process Research Institute, Bhopal selected him to represent Madhya Pradesh, Chhattisgarh and Orissa in ISF 2016. In an outreach programme conducted by AMPRI, Rishabh was honoured by the National Convener-Secretary of ISF.

and a mobile SIM with unique digital identification number, generic data and biometric information of the subject. This digital number would serve as the digital identity of a person and all information (right from registration of birth, school admission, grade sheets of all examinations, certificates, credentials, degrees, achievements, awards, scholarships, job details, income, assets, liabilities, vehicles, marital, medical and legal history) are recorded in the same card. During the Platinum Jubilee Celebration of CSIR at Vigyan Bhawan in New Delhi, Rishabh's project was applauded by Prime Minister Narendra Modi.

SCHOLARS PARK

Rishabh Garg | BITS Global Identity through Blockchain

Sep 14, 2021 9:00 PM IST +0530

DJ Metzler • Senior Producer

Studio (866) 496-4065 ext 821 | Local (561) 899-4771

1106 W. Indiantown Rd. Studio 1, Jupiter, FL 33458

A Series Hosted By Ted Danson

CNBC TV

in f t v a

Én Verden - Én Identitet

RISHABH GARG – BITS INDIA

Som svar introduserte **Garg [2016 – 2023]** ideen om One World – One Identity, som er et ensomt alternativ til flere identitetskort. Dette globalt unike flerbruks digitale identitetsnummeret kan betjenes ved hjelp av toppmoderne blokkjedeteknologi.

Hver person som bor på jorden kan tildeles en 20-sifret identitet på en bestemt dato. Dette vil gjøre det mulig for enkeltpersoner å lagre påloggingsinformasjonen og personlig identifiserbar informasjon i en lommebok eller applikasjon kjent som IPFS [**Garg, 2021**]. For fildeling vil IPFS bruke en desentralisert, distribuert peer-to-peer (P2P) nettverksmodell som kan spres over flere datamaskiner eller noder. Filer kan deles inn i segmenter og holdes i et nettverk av noder som holder styr på dem ved hjelp av hashen. Den opprinnelige filen kan rekonstrueres når hele filen er satt sammen, basert på hash-verdien til hver komponent.

I motsetning til de tradisjonelle Hyper-Text Transfer Protocol (HTTP)-familiene av protokoller eller sentraliserte navnerom, er IPFS et stedsbasert lagringssystem. Når et lagringssystem er stedsbasert, holder det styr på verter ved å bruke en IP-adresse eller et annet logisk adresseskjema tilordnet et kjent navn. Hvis verten endrer navn eller adresse, må navnetjenestetabellen også oppdateres.

En innholdsidentifikator kreves i innholdsbasert adresseringslagring for å finne den nøyaktige plasseringen til filen. I stedet for en logisk adresse, får man tilgang til dataene her basert på dens kryptografiske hash, som fungerer som et digitalt filfingeravtrykk. Nettverket returnerer alltid det samme innholdet basert på hashen, uavhengig av hvem og hvor filen er lastet opp. IPFS er en desentralisert måte å lagre filer på, hvorved, for identitetshåndtering, det originale dokumentet kan lagres på IPFS, mens metadataene eller hashen av innholdet kan lagres på en blokkjedeserver.

Et ekstra lag med sikkerhet kan også legges til med biometriske løsninger, for eksempel tommelavtrykk på en smarttelefon, fingeravtrykk, håndgeometri, stemme- eller ansiktsgjenkjenning, termisk kartlegging, øyemønstre – netthinneskanning, iris-skanning eller annen biometrisk verifiseringsprotokoll. Biometriske data kan lagres og behandles ved hjelp av en databaseserver, fysiske tokens, krypterte tokens eller begge deler. Sikre systemer lagrer ofte biometriske maler på enheten eller på stedet for å muliggjøre identitetsverifisering uten å overføre sensitive biometriske data til en annen server eller plassering på Internett.

Selv om den interne mekanismen for biometrisk autentisering er avhengig av teknologi, er den bemerkelsesverdig enkel og rask fra brukerens synspunkt. Det er lettere å sette fingeren på en skanner enn å skrive inn et langt passord med flere spesialtegn for å låse opp en konto umiddelbart. De fleste biometriske autentiseringsmetoder brukes bare med fysiske applikasjoner; du kan ikke overføre eller kommunisere biologiske beregninger på nettet. Biometri som

fingeravtrykk, iris-skanning, ansiktsmønstre og annet er vanskelig å rekonstruere med dagens teknologi. Sjansen for at ditt fingeravtrykk samsvarer med andres er én på 64 milliarder. Les mer, *Blockchain for Real World Applications - Rishabh Garg. John Wiley & Sons, Inc. US, 01-388: ISBN - 9781119903734*.

Nylig har det blitt oppdaget at ved å bruke blockchain, kan de tradisjonelle byggesteinene til enhver dyplæringsmodell konverteres til et sikkert system. Det er en biometrisk gjenkjenningsarkitektur som bruker blokkjedeteknologi for å gi feiltolerant tilgang i et distribuert miljø. Den beskytter både dyplæringsmodellen og den biometriske malen og varsler hele systemet når en spesifikk komponent tukles med. Det gjør det også lettere å identifisere potensielle forstyrrelser.

Biometriske identifikasjonssystemer, som kombinerer biometri og blokkjedeteknologi, kan brukes til å forbedre sikkerheten, oppnå konsensus i flyktige miljøer og ta reviderbare beslutninger. Gjennom en personlig enhet, for eksempel en smarttelefon, kan brukere dele sin digitale ID med tjenesteleverandøren selv om de ikke er fysisk til stede og fortsatt kunne få tilgang til viktige tjenester uten å sette personvernet i fare.

Uten brukerens eksplisitte tillatelse vil ingen transaksjon finne sted gjennom deres informasjon. Ved å la brukeren administrere sin personlig identifiserbare informasjon, vil systemet være mer interoperabelt, brukeren vil være fri til å få tilgang til dataene på tvers av flere plattformer og ikke bli tvunget til å bruke bare én.

Siden det ikke er noen geografiske begrensninger på bruken av blokkjede-identiteter, kan brukere få tilgang til og bekrefte identiteten deres fra ethvert hjørne av verden. Blockchain vil eliminere behovet for flere brukernavn og passord ved å gjøre det mulig for brukere å nyte en selvstyrt og kryptert digital identitet.

Et kort med et unikt nummer skal lagre alle fysiske data til en borger, enten personlige, biometriske, pedagogiske, utenomfaglige, yrkesfaglige, medisinske, juridiske eller økonomiske, i separate siloer, på en fullstendig kryptert måte. På denne måten vil **One World – One Identity** vise seg å være effektiv innen bedre utdanning, bank, investeringer, helsevesen, offentlige distribusjonsordninger og andre tjenester [Garg 2017].

KRYPTERING

Kryptering av kommunikasjon gjør at bare den sanne avsenderen og den tiltenkte mottakeren av meldingen kan lese det relevante innholdet. Det er tre hovedkategorier av kryptografi - asymmetrisk nøkkelkryptografi, hashfunksjonskryptografi og symmetrisk nøkkelkryptografi.

Det har vært flere vendepunkter i kryptografiens historie som la grunnlaget for moderne algoritmer. Begrepet "chiffer" refererte opprinnelig til en generell idé for å overføre hemmelige meldinger som inkluderte bokstaver som en grunnleggende komponent. Enkelt substitusjonschiffer, Cæsar-chiffer, Hill-chiffer, Playfair - chiffer, Vigenere- chiffer, transposisjons-chiffer,

etc. er noen av de kjente eksemplene. Playfair - chiffer i C kan trygt overføre mellom kilden og destinasjonen uten å lekke informasjon ved hjelp av kryptering-dekryptering.

Hill-chifferet er et polygrafisk substitusjons-chiffer basert på lineær algebra som ble grunnlagt av Lester S. Hill i 1929. Det kan lett danne et sammenhengende chiffer når det brukes med digrafer (to-bokstavsblokker), trigrafer (trebokstavsblokker), eller andre blokker i flere størrelser. Mange flere kryptografiske algoritmer kan også implementeres, inkludert RSA-algoritmen, Multiple Precision Arithmetic Library, GNU Multiple Precision Arithmetic Library, Chinese Remainder Theorem og SHA-512-hashen i Java. Les mer, [Blockchain for Real World Applications - Rishabh Garg. John Wiley & Sons, Inc. US, 01-388: ISBN - 9781119903734.](#)

CYBERSIKKERHET

Cybersikkerhet beskytter systemer og nettverk mot trusler på nettet. Landskapet for cyberangrep har eksplandert raskt de siste årene. Angripere bruker skadelig programvare som trojanere, rootkits og virus som er kjent som DDoS -angrep (Distributed Denial of Service), MITM-angrep (Man in the Middle), Phishing-angrep og Ransomware- angrep. Bedrifter over hele verden har omfavnet blockchain, som har dukket opp som et potensielt verktøy for cybersikkerhetsreduksjon.

UTDANNING OG SYSSELSETTING

Millioner av søkere over hele verden sender inn sin akademiske legitimasjon hvert år i håp om å bli rekruttert av høyere utdanningsinstitusjoner eller ansatt av bedriftshus. Et stort antall søkere overdriver sin utdanningsbakgrunn ved hver rekruttering.

For å bevare autentisiteten til dokumentet, kan en legitimasjonsinnehaver beholde all legitimasjonen i Pi-lommeboken og dele den med validatorer i en kryptert modus ved hjelp av Ethereum-blokkjeden. I samsvar med Garg [2021] kan hashen som genereres etter opplasting av legitimasjonen til IPFS ha to lag med kryptering. Studentens offentlige nøkkel kan brukes til å lage det første laget med kryptering, og deretter kan utstederens private nøkkel brukes til å implementere det andre og tredje laget med kryptering (autorisasjon). Den vil bli dekryptert ved hjelp av utstederens offentlige nøkkel for å bekrefte den delte legitimasjonen. Den krypterte hashen som produseres kan sammenlignes med den som er lagret i utsteders database. Hvis begge stemmer overens, kan legitimasjonen anses som gyldig.

Ofte nevner ikke en elevs prestasjonsbevis pensum eller undervisningsmetoder. Det forhindrer en student i å overføre sin akademiske studiepoeng eller læringsprestasjoner fra en institusjon til en annen. En fullstendig oversikt over pensum, undervisning, læring og vurdering kan opprettholdes ved å gi hver elev tilgang til et vurderingsdashboard [Garg, 2021]. Arbeidsgivere vil kunne velge den beste kandidaten, undersøke fortiden deres og evaluere støttedokumenter forutsatt at en kandidats prestasjoner registreres på hvert trinn av hans/hennes akademiske karriere på en robust plattform som Blockchain. Som sådan kan blockchain vise seg å være et nyttig verktøy for å gjennomføre bakgrunnssjekker av en kandidat, og spare tid, penger og menneskelige ressurser.

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

HELSEVESEN

Helseinstitusjoner rundt om i verden sliter med problemer som forsinkelser i datainnbrudd, opprinnelse av medisinsk utstyr og tilbakeføringskrav for reseptbelagte legemidler. Blockchain tilbyr et bredt spekter av bruksområder og fordeler innen helsevesenet. Det hjelper med å administrere legemiddelforsyningskjeder, beskytte overføringen av pasientjournaler og gi helseforskere tilgang til biologiske og genetiske koder.

Ved å bruke blokkjede kan all medisinsk informasjon om pasienten, inkludert resepter, notater og laboratorieresultater, være tilgjengelig i en enkelt visning. Hver del av informasjonen kan konverteres til en egen hash-funksjon. Hver hash-funksjon er distinkt og kan bare deles med tillatelse fra eieren av dataene. I tillegg, ved å bruke blockchain, er det mulig å overvåke en vare fra produksjonspunktet gjennom hvert trinn i forsyningskjeden, noe som gir kjøperen fullstendig synlighet og åpenhet over produktene han er i ferd med å kjøpe. Bruken av teknologi kan fremskynde skadeoppgjøret for forretningspartnere og forsikringsselskaper, gjøre det mulig for rettshåndhevelse å etterforske enhver mistenkelig aktivitet som narkotikasmugling eller hamstring under store nødsituasjoner som pandemier, og koble sammen organdonorer, organmottakere og helsetjenester for å lette organtransplantasjon .

GENOMI

Et uendelig antall genetiske datapunkter kan lagres sikkert på en blokkjede. Det er i ferd med å bli et marked der enkeltpersoner kan handle sine genetiske data. Den har en tendens til å lage omfattende databaser og gi viktig informasjon til forskere raskere enn noen gang før. I motsetning til dagens systemer, hvis dataeierne kan etablere kontakt med datakjøperne direkte uten bruk av en mellommannbedrift, kan analysekostnaden reduseres og dataeierne kan tjene mer. Les mer, [Blockchain for Real World Applications - Rishabh Garg. John Wiley & Sons, Inc. US, 01-388: ISBN - 9781119903734.](#)

FORSYNINGSKJEDE

Hver dag produseres og distribueres milliarder av forbruksvarer gjennom komplekse forsyningskjeder som når hvert hjørne av verden. Informasjon om opprinnelsen, produksjonen og bruken av disse varene gjennom hele livssyklusen forblir imidlertid uklare. Hvert produkt går gjennom et omfattende nettverk av leverandører, forhandlere, distributører, transportører, lager og andre fasiliteter før de selges til sluttkunden, men de forblir nesten alltid et mysterium gjennom denne komplekse reisen.

Som et resultat er en kritisk forretningsbarriere som hindrer de fleste organisasjoner fra å vite noe om sine andre og tredje tierleverandører forsyningskjedesynlighet. Åpenhet og synlighet på

tvers av ulike kanaler i hele forsyningskjeden kan lette bevegelsen av varer fra råvarer til ferdigvareproduksjon, testing og distribusjon.

Bedre resultater kan forventes fra bruk av blokkjedeteknologi i forsyningskjeden. Forsyningskjeden kan bruke en delt, konsensusbasert offentlig hovedbok for å spore prosessene for opprinnelse og produksjon av produkter. I supply chain management kan livssyklusen, sertifisering og dokumentasjonen av et produkt gjøres umiddelbart tilgjengelig for alle parter gjennom blockchain. Fra produsent til lagring, reise, distribusjon og salg, produkter kan spores.

MAT TILSYN

En stor andel av maten vi konsumerer produseres gjennom en kronglete global forsyningskjede, noe som også øker risikoen for forfalskning, tukling, feilaktig fremstilling og målrettet substitusjon. Den globale matsektoren taper milliarder av dollar hvert år på mattyveri. Melk, te, kaffe, fruktjuice, olivenolje, lønnesirup, skalldyr, honning og mange andre matvarer er inkludert i de fleste matvarekategorier. Den gjennomsnittlige personen kan ikke forestille seg dagen uten disse matvarene.

Etter hvert som den globale forsyningskjeden utvides, blir matsikkerhet en stor bekymring for både forbrukere og regulatorer. I følge Verdens helseorganisasjon rammes én av ti mennesker av matforgiftning, noe som resulterer i 33 millioner år med sunt liv og 420 000 dødsfall hvert år [WHO-rapport, 2019]. I tillegg tar matbåren sykdom livet til 125 000 barn under fem år hvert år. Også her er blockchain et pålitelig alternativ som kan bevare sporbarheten til uforanderlige dokumenter. Ved hjelp av blockchain er det mulig å overvåke matvarer på alle nivåer, fra gården til supermarkedene.

Blockchain etablerer også raskt sin dominans i andre bransjer enn styring av matforsyningskjeden. Selv om flertallet av toppbedriftene har banebrytende digital infrastruktur, inkludert supply chain management (SCM) og enterprise resource planning (ERP) programvare, viser systemet fortsatt analoge hull når produkter spores fra tilkoblet produksjonsutstyr (opprinnelse) til digital frakt varsler og RFID-skanning. Selv det mest avanserte maskineriet kan ikke nøyaktig beregne hvor lenge et produkt vil vare. Bedrifter kan bruke blokkjedeteknologi for å opprettholde en sanntids, uforanderlig digital hovedbok over alle transaksjoner og bevegelser for hvert medlem av deres forsyningskjedenettverk. Les mer, [*Blockchain for Real World Applications - Rishabh Garg. John Wiley & Sons, Inc. US, 01-388: ISBN - 9781119903734.*](#)

EIENDOM

I uminnelige tider har eiendom vært et pålitelig investeringsalternativ for de velstående. Bare et lite antall eiendeler gir samme mengde kapitalvekst. Til tross for alt dette er det mange begrensninger på et globalt landskap, som tilgang til potensielle sponsorer, finansfolk og fondsforvaltere; statsborgerskap i landet; anerkjennelse av kjøpers forretningsetablering, internasjonale bankkontoer, kredittscore, matchende midler osv. I tillegg bruker hver

eiendomseier unødvendig en enorm sum penger på å registrere eiendomsrett, frigi panterett og overføre eierskap til kommunale registre for å sikre investeringene sine.

Blockchain tilbyr alle spillere den samme versjonen av sannheten om tittelen landeierskap. Som et resultat kan prosedyrer som ofte er knyttet til eiendom, som dobbeltsalg, falske registre og inngrep, elimineres. Smarte kontrakter kan brukes til å regulere eiendomstransaksjoner, samtidig som man reduserer papirarbeid, mellommenn og eiendomstakstmenn.

VALGPROSESS

Det primære målet for enhver valgmyndighet er å gjennomføre valg på en rettferdig, pålitelig og transparent måte. For å nå dette målet bruker byråkratiet hensynsløst milliarder av dollar og kaster millioner av statsansatte inn i valgplikt. Blokkjedeteknologi kan være effektiv for å gjøre stemmeprosessen enkel, smidig og gjennomskiktig.

Dette kan hjelpe folk til å stemme som ofte unnlater å utøve sin rett til franchise, kanskje fordi de bor i avsidesliggende områder, mangler tilgang til valglokaler eller er fullstendig uføre. Fordi den bruker en distribuert hovedbok, kan velgerne avgi stemme fra hvor som helst i verden uten å ofre privatlivet. Det gjør det enkelt for velgerne å avgi sin stemme på valgdagen sittende hjemme, uten å stå i kø eller gå gjennom overdrevne formaliteter.

Når hver enkelt innbygger har en desentralisert identitet, også kjent som en selvsoverent identitet, kan en distribuert hovedbok brukes til å registrere alle viktige hendelser i deres liv. Innbyggere kan få lov til å delta i valgprosessen basert på deres informasjon, inkludert deres vanlige bosted (valgkretsen der de er stemmeberettigede), fødselsdato (når de når lovlig stemmerettsalder) og underlagt andre betingelser (hvis noen). En velger kan avgi sin stemme gjennom sin innloggings-ID, men kan ikke igjen bruke det samme desentraliserte identifikasjonsnummeret som han har avgitt sin stemme på under nevnte valg. Ved å separere stemmene til hver valgkrets ved å bruke programvare på den andre dagen av avstemningen, vil blokkjeden telle stemmene som er avgitt til fordel for hver kandidat gjennom forskjellige noder.

Likevel er det en hemmelighet at enhver innbygger vet at mange fiendtlige og ulovlige aktiviteter omgir stemmeprosessen og valgresultatene. Ingen steder i verden er valgprosessen komplett uten båsfangst, utskifting av stemmeutstyr ved valglokaler eller falske stemmepåstander. Regjeringer kan være på vakt mot å implementere blokkjede-baserte valg fordi de er fullt reviderbare prosesser som begrenser mulighetene for manipulasjon for politiske partier. Les mer, [*Blockchain for Real World Applications - Rishabh Garg. John Wiley & Sons, Inc. US, 01-388: ISBN - 9781119903734.*](#)

BANK OG FINANS

Formålet med opprettelsen av bankinstitusjoner var trolig å muliggjøre all slags handel og forretning ved å bringe mennesker sammen. Blockchain gjør det enkelt for eksterne upålitelige parter i bank- og finanssektoren å nå en konsensus om tilstanden til databasen, uten hjelp fra portvakter. Brukere vil kunne velge hvem og hvor mye de vil dele identiteten sin med. På

blokkjeden trenger de kun å angi identiteten sin én gang. Hvis tjenesteleverandørene er blokkjededrevne, er det ikke nødvendig for noen bruker å gjenta registreringen.

I likhet med en pålitelig bokholder, administrerer den alle finansielle transaksjoner, inkludert betalinger, oppgjørssystemer, innsamling, verdipapirforvaltning, lån, kreditter og handelsfinansiering. Når det gjelder identitetsverifisering, betalinger, uttak, oppgjør, kreditter og lån, aktivaoverføringer, peer-to-peer-overføringer, hedgefond, sikkerhet og ansvarlighet, har det vært i stand til å utkonkurrere tradisjonelle systemer.

Dette kan dramatisk redusere transaksjonsgebyrene ved å redusere de faste utgiftene som påløper når man manuelt setter opp, utfører og utveksler eiendeler. Elimineringen av mellomledd har gjort prosesser, som betalinger over landegrensene, handel og oppgjør raskere, mer pålitelige og rimeligere.

HANDELSFINANS

Overføring av informasjon, overføring av eiendeler og prosessen med å foreta betalinger er i stor grad avhengig av papirbasert forretningsdrift innen handelsfinansiering. Disse kontraktene kan være bedre forklart i Python-programmeringsspråket i stedet for lovlige, slik at handelsmenn kan forstå dem. Derfor gir blockchain og smarte kontrakter forretningsinvestorer et sikkert, åpent, transparent, reviderbart og automatisert transaksjonsmiljø. Det har potensial til å transformere handelsfinansiering ved å strømlinjeforme driften av smarte kontrakter, bedriftsressursplanlegging, lynnettverk, prosesser før og etter handel, regnskap og revisjoner, lojalitetsprogrammer, etc.

DESENTRALISERT FINANS

Desentralisert finans (DeFi) er en ny finansteknologi bygget på blockchain. Det er ganske forskjellig fra andre finansielle nettverk siden det er åpent og programmerbart. Smarte kontrakter og vilkårene som ligger til grunn for dem gjør at de kan fungere automatisk uten en sentral myndighet. Det lar utviklere lage nye betalings-, investerings-, utlåns-, handels- og byttemodeller uavhengig av banker og andre institusjoner.

I sentralisert finans eier banken, finansinstitusjonen eller virksomheten som garanterer transaksjonen pengene dine. De tar et stort utbytte fra pengene dine, da de har mye økonomisk frihet. I DeFi fungerer en smart kontrakt som en transaksjonserstatning for en finansinstitusjon. Når de går live, er det bare smarte kontrakter som overholder. Disse kontraktene kan ikke endres fordi de alltid er designet for automatisering.

Desentraliserte finansielle protokoller har gitt forbrukere over hele verden tilgang til et bredt spekter av nye økonomiske muligheter. Asset management, tokenisering, token-derivater, desentralisert autonomi, dataanalyse og verdivurdering, betalinger, utlån og utlån, forsikring, marginhandel, markeder, spill og avkastningsoppdrett er alle dekket. Les mer, [Blockchain for Real World Applications - Rishabh Garg, John Wiley & Sons, Inc. US, 01-388: ISBN - 9781119903734](#).

ETHEREUM SOM EN DEFI-PLATTFORM

Ethereum er et innovativt, algoritmedrevet økonomisk system drevet av tillit, muligheter og økonomisk tilgang. Det kan utnyttes til å sende penger, bruke programmerbar valuta, låne ut eller låne penger, delta i lotterier uten tap, trading tokens, kvadratisk handel, innsamling av penger, crowdfunding, porteføljestyring, etc. Dessuten kan prediksjonsmarkeder også dra nytte av Ethereum blockchain på flere måter – økt tilgang, motstand mot sensur og fjerning av mellomledd.

DISTRIBUTERTE RESSURSER OG IOT

Blockchain gir sikrere datalagring og -administrasjon med betydelige fordeler ved å tilby en enhetlig, interoperabel og manipulasjonssikker arkitektur for myndigheter, bedrifter, forbrukere og IoT - administrasjonssystemer. Den utfører mellom- og bakkontorfunksjoner på samme måte som Internett og nettfronten utfører dem, automatiserer oppgaver for å øke produktiviteten og åpner for nye forretningsmuligheter.

koble IoT - systemer til blockchain sikrer effektiviteten og datasikkerheten til IoT - applikasjoner. En algoritme kan kombineres med en ny ledervalgsteknikk for å gjøre det enklere å bruke blokkjede på IoT-endeenheter med begrenset ressurstilgjengelighet. IoT-data som holdes på en delt blokkjede bok gjør det mulig for alle parter å spore opprinnelsen til komponenter gjennom et produkts livssyklus. Det er nå trygt, enkelt og økonomisk å dele all relevant informasjon med tilsynsorganer, avsendere og produsenter. Les mer, [Blockchain for Real World Applications - Rishabh Garg. John Wiley & Sons, Inc. US, 01-388: ISBN - 9781119903734](#).

E-STYRING

Til tross for at mange nerder har forsøkt å løse sikkerhetsproblemer i e-governance-systemer, blir sikkerhetskrav generelt ikke oppfylt av eksisterende rammeverk og modeller. Siden det er umulig å ignorere mangelen på tillit til Internett-medierte transaksjoner og uautorisert tilgang av insidere til systemet, ser ut til å implementere blokkjedeteknologi å være den eneste måten å løse disse manglene på. Dette lover en mer effektiv, trygg og sikker offentlig tjeneste.

Hundrevis av blokkjedeinitiativer har blitt lansert i mer enn tretti land de siste fire til fem årene for å erstatte offentlige systemer. Estland har tatt i bruk en blokkjedeaktivert ID for å bekrefte identiteten til borgere. Blockchain-teknologi brukes til å bygge elektroniske stemmesystemer i Australia og Ukraina. I USA brukes den til å dele medisinske data på en sikker måte, og i Storbritannia for å forbedre offentlige tjenester. I Georgia og Honduras administreres landregistrering ved hjelp av distribuert reskontroteknologi. I nær fremtid drømmer Kina om å bygge en blokkjedeby.

Automatiserte blokkjedesystemer kan gjøre det mulig for offentlige etater å operere mer effektivt, ved å redusere innsatsen, tiden og kostnadene som vanligvis kreves for å manuelt administrere tilgangen til nettverkene deres. I tillegg kan det også lette:

- opprettholde detaljene til den utstedende og verifisere myndigheten;
- sikring av dokumenter fra tukling;
- gjøre all relevant informasjon tilgjengelig for myndighetene gjennom den offentlige nøkkelen;
- tilgang til personlig informasjon eller originale dokumenter når som helst, hvor som helst gjennom brukernes private nøkler;
- redusere svindel, skatteunndragelse og feilbehandling; og
- øke landets økonomi [Garg, 2020].

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

DESENTRALISERT STREAMING

Videoer kan være underholdende, lærerike og styrkende. Kringkastere som laster opp video til Internett må imidlertid omkode den først. Den bruker opptil 80 % av hele Internett-båndbredden, noe som gjør videostrømming svært kostbart. Videoinfrastruktur er nødvendig for å gi mer skalerbare og kostnadseffektive løsninger, og for å møte dette kan teknologier som blokkjede gi apputviklere i videotranskodningsmarkedet tilgang til et bredere spekter av distribuerte prosessorer, som er tilgjengelige, trygge og kostnadseffektive.

DOBBELGRUVE

Dual mining er praksisen med å utføre forskjellige operasjoner på samme utstyr. Uttrykket dukket først opp i sammenheng med PoW- gruvedrift, der det beskrev samtidig gruvedrift av flere kryptovalutaer ved å bruke en enkelt GPU for å kjøre PoW -hash-algoritmen. Dobbel gruvedrift – bruk av en GPU for å utvinne kryptovalutaer som Ethereum , samt å bruke den til å omkode video som en videominer på ditt eget nettverk – kan fortsatt være mulig for videostreaming. En fordel med å bruke transkoding som en tilleggsaktivitet til dual mining er at den bruker færre GPU-kjerner enn andre mulige arbeidsbelastninger fordi GPU-ens maskinvarekodere og dekodere gjør det meste av arbeidet.

STEDEVIS NETTVERK

Det stadig voksende blokkjedenettverket dekker mange aspekter av den virkelige verden, inkludert menneskelig ressursforvaltning, rettshåndhevelse, offentlig bistand, velferdslevering, posttjenester, regninger og betalinger, skatt, narkotika, vaksinasjon og samfunnshelse, legemiddeloppgjør, forsikring, frakt, gods, offentlig transport, reise og mobilitet, turprat, flyreiser, tingenes internett, informasjon og kommunikasjon, meldingstjenester, gjestfrihet, underholdning, gambling, mat og drikke, fiskeri, husdyrhold, landbruk og naturressurser, infrastruktur og energi, produksjon, eiendom, bygg, kjøretøy, testamenter og arv.

I ET NØTTESKALL

Blockchain lover ikke å gjøre brukeren til milliardær over natten eller tilby en mekanisme for å beskytte sine finansielle transaksjoner fra politisk inspirerte regjeringer. Det som imidlertid er beviselig sant, er at det tilbyr en ny tilnærming til å strukturere administrative og økonomiske organisasjoner, samtidig som kostnadene for tillit reduseres betydelig gjennom en radikal, desentralisert hovedbok-tilnærming.

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

REFERANSER

- 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.