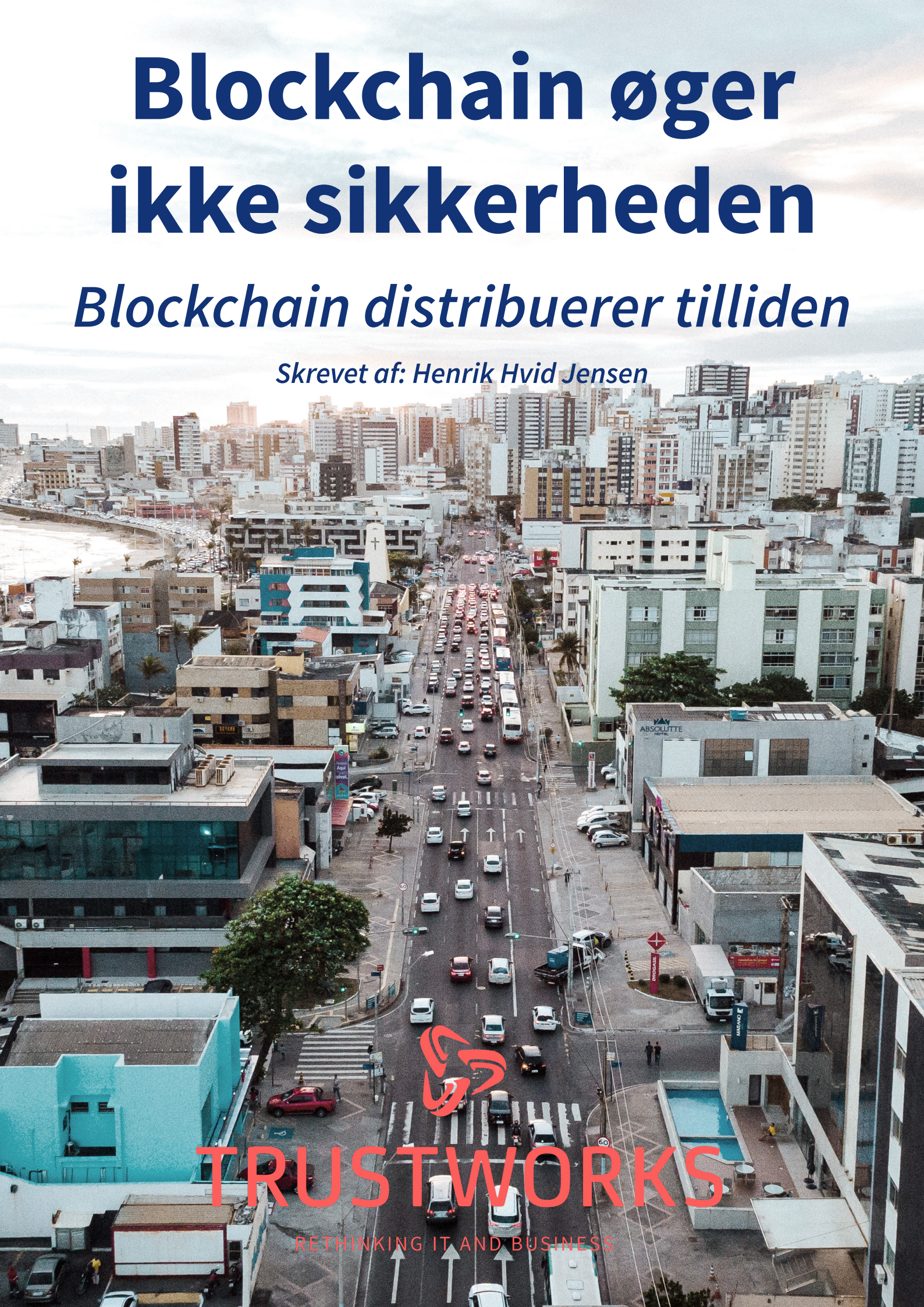
Blockchain øger ikke sikkerheden

Blockchain distribuerer tilliden

Skrevet af: Henrik Hvid Jensen



Blockchain øger ikke sikkerheden

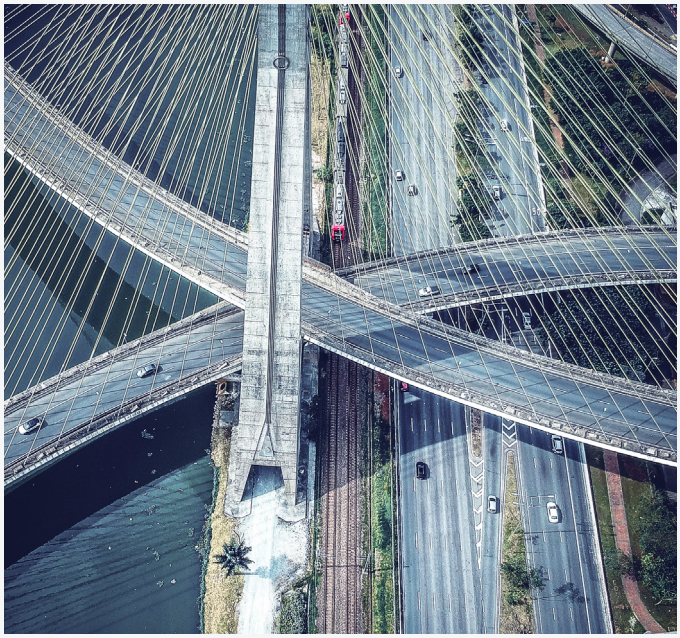
- Blockchain distribuerer tilliden

Jeg har deltaget i mange diskussioner, hvor opfattelsen har været at blockchain er mere sikker end traditionelle centraliserede løsninger. Dette er dog ikke tilfældet. Blockchain bidrager ikke med et sikkerhedsniveau, som du ikke kan få ved at bruge troværdige mellemled på konventionelle centraliserede teknologier.

Det nye med blockchain er derimod, at hvis behovet er distribueret tilgængelighed og integritet af kritiske data og tillid i et økosystem, hvor parterne ikke kender hinanden eller der ikke er tillid mellem dem og man ikke ønsker et dyrt centralt troværdigt mellemled, giver blockchain mulighed for, at man kan lave decentraliserede løsninger med et sikkerhedsniveau, der svarer til det, man kan opnå med centraliserede teknologier, men ikke bedre.

Hvis det primære behov er øget sikkerhed, er blockchain-teknologier derfor ikke svaret. Blockchain er alene svaret, hvis du har en use case der kræver decentralisering.

“Hvis det primære behov er øget sikkerhed, er blockchain ikke svaret. Blockchain er alene svaret, hvis du har en use case der kræver decentralisering.”



Hvis ikke du allerede er bekendt med hvordan blockchain fungerer, vil jeg henvise til kilder på internettet (f.eks. World Economic Forums Beyond the Hype).

Informationssikkerhed kan deles op i tre områder; tilgængelighed, integritet og fortrolighed. I de følgende afsnit vil jeg sammenligne sikkerheden i forbindelse med blockchain overfor sikkerheden i en centraliseret løsning med konventionelle teknologier.

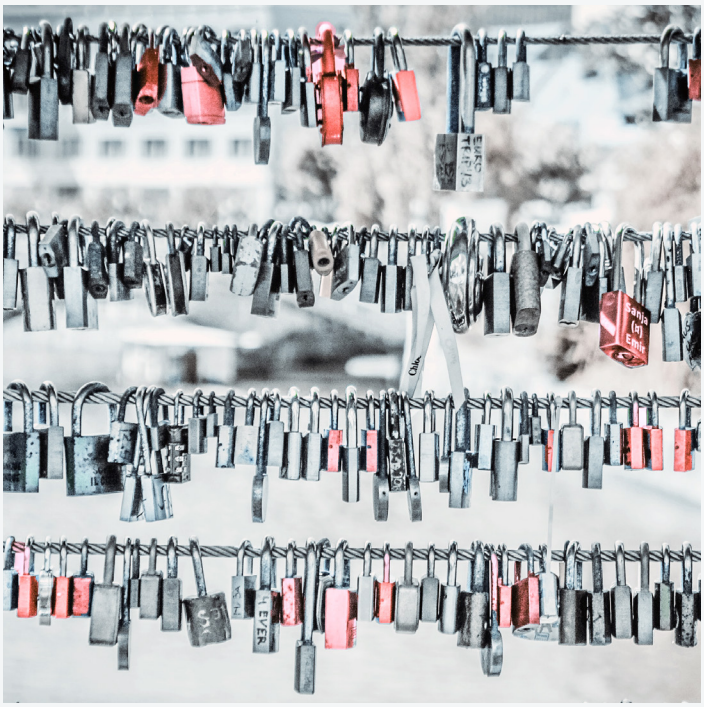
Tilgængelighed er høj, men ikke højere

Da enhver node i blockchainen opretholder sin egen kopi af det delte register, og den underliggende konsensusalgoritme sikrer, at alle noder altid synkroniseres, kan enhver kompatibel node fejle, tilslutte sig eller forlade blockchainnetværket uden at påvirke tilgængeligheden af det distribuerede system.

Enhver node kan blive kompromitteret uden at påvirke troværdigheden af netværket, så længe de kompromitterede noder repræsenterer mindre end halvdelen af netværkets ressourcer.

Med Bitcoin i drift siden 2009 og med tanke på at andre "gamle" blockchain-platforme med tusindvis af noder, såsom Ethereum, har fungeret kontinuerligt i flere år, er det dokumenteret, at de etablerede platforme har høj tilgængelighed.

Det er anderledes for nye blockchainplatforme med kun få noder. Der vil være en risiko for, at ondsindede aktører kan kontrollere et tilstrækkeligt antal noder til, at de får mulighed for at ændre indholdet i det distribuerede register.



"Bemærk, at det også kan være tilfældet med, hvad vi i dag ser som veletablerede netværk, fordi måske endda Bitcoin og Ethereum kan miste deres attraktivitet og blive forladt af deres no-der og dermed blive mere sårbare."

Bemærk, at det også kan være tilfældet med, hvad vi i dag ser som veletablerede netværk, fordi måske endda Bitcoin og Ethereum kan miste deres attraktivitet og blive forladt af deres noder og dermed blive mere sårbare.

For private blockchains kan tilgængeligheden garanteres af den enhed, der forvalter peer-to-peer-netværket, men vil også være afhængig af antallet af noder. En af de væsentlige udfordringer i private blockchain-netværk er, at få den kritiske mængde af noder.

Med et godt designet og kontrolleret distribueret datacenter kan konventionelle centraliserede løsninger dog opnå samme tilgængelighed som en blockchain-løsning.

Integritet - Blockchains uforanderlighed er ikke unik

På blockchain er hver blok digitalt signeret, hashet og sekventielt forbundet, hvorved integritet og uforanderlighed sikres.

Hvis data blev signeret, hashet og forbundet på samme måde hos en central løsning, vil man kunne opnå samme niveau af integritet og uforanderlighed.

> **“Hvis data blev signeret, hashet og forbundet på samme måde hos en central løsning, vil man kunne opnå samme niveau af integritet og uforanderlighed.”**

Selv en databaseadministrator, der har direkte adgang til sådanne centrale data, vil ikke ubemærket kunne manipulere disse. Blockchains højt besungne uforanderlighed kan altså også opnås ved at anvende samme mekanismer på en traditionel central datalagring.

I øvrigt er det værd at spørge sig selv, om man ønsker den fuldstændige uforanderlighed uden evnen til eksempelvis rollback i tilfælde af softwarefejl i smart contracts. Uforanderligheden kan også give udfordringer ved “ret til at blive glemt”-lovgivning såsom GDPR. Forretningslogikken i applikationslaget skal kunne håndtere manglerne ved uforanderlighed.

På samme måde som med enhver anden teknologi vil også blockchain-platforme have software sårbarheder, både i den implementerede blockchain-teknologi såvel som i det underliggende operativsystem som Microsoft Windows.

Som med al anden ny teknologi skal blockchain-platforme også have været udsat for hackerangreb i flere år, før man kan kalde dem sikre.

Den konstante udvikling af nye features på for eksempel Ethereum medfører risikoen for, at nye sikkerhedshuller bliver introduceret.

Blockchains sekventering af hver ny blok der tilføjes, er en afgørende feature. Det eliminerer behovet for afstemninger mellem virksomheder, alle har samme syn på sandheden, og det giver mulighed for distribuerede noder, da det forhindrer svigagtige transaktioner fra ondsindede noder og tolerance mod fejl i en eller flere noder i netværket; transaktioner er afsluttet og registreret hos alle noder. Dette er en vigtig forudsætning for distribueret tillid.

Dette gør sig ikke gældende for et centralt betroet computersystem, da der ikke er nogen ondsindet node i en centralt betroet løsning.

Fortrolighed – Flere angrebspunkter

Fortroligheden på offentlige blockchains ligger i at ens identitet er ukendt, alle er dækket af ens hashet offentlig nøgle. Sekvensen og indholdet af begivenheder gemt på blockchainen afslører dog ofte for meget information og bør beskyttes mod uautoriserede brugere.

En uautoriseret bruger kan for eksempel bruge BI-analyser til at få kendskab til karakteristika af de skete transaktioner og de sandsynlige fremtidige transaktioner.

“En uautoriseret bruger kan for eksempel bruge BI-analyser til at få kendskab til karakteristika af de skete transaktioner og de sandsynlige fremtidige transaktioner.”

I private blockchain, hvor kun autoriserede noder kan deltage, er transaktionsparternes identitet som minimum kendt af parterne, men transaktionsoplysningerne kan krypteres.

Private blockchain tillader finkornet kontrol over hvert element i en transaktion, hvilket muliggør detaljeret specifikation af hver parts adgangsrettigheder.

I flere scenarier kolliderer kravet om et delt register med fortrolighedsprincippet.

Som eksempel kan nævnes internationale værdikæder, hvor det er relevant for flere parter længere henne i værdikæden at få kendskab til tidligere transaktioner. Disse transaktioner skal samtidig holdes fortrolige fra aktører, der ikke er en del af værdikæden.

Værdikædens parter kender ikke hinanden og ved ikke præcist, hvem der vil producere og forbruge hver begivenhed, eksempelvis hvilken lastbilchauffør, der håndterer en container.

For at sikre den fælles version af sandheden sammen med fortrolighed er det nødvendigt at implementere et meget sofistikeret koncept for distribution af dekrypteringsnøgler.

Det er værd at bemærke, at med en centraliseret løsning er der kun ét angrebspunkt for hackere, der forsøger at få adgang til dataene.

VS

I en privat blockchain er der derimod flere angrebssteder, en for hver node, hvorfor data kun beskyttes lige så godt som det svageste led i kæden.

På blockchainen sikres brugerens identitet via offentlig-privat nøgle og er som sådan ikke beskyttet eller styret af konsensusalgoritmen.

På samme måde som med centrale løsninger er sikkerheden ved kryptografiske løsninger kun lige så sikker, som den måde hvorpå den private nøgle er beskyttet.

Det betyder, at alle traditionelle metoder til at stjæle private nøgler (malware, phishing, social engineering osv.) er lige så effektive på løsninger baseret på blockchain som på konventionelle teknologier."

"Det betyder, at alle traditionelle metoder til at stjæle private nøgler (malware, phishing, social engineering osv.) er lige så effektive på løsninger baseret på blockchain som på konventionelle teknologier."

Sammendrag - fokus er på distribueret tillid, ikke sikkerhed

“Blockchain bidrager ikke med sikkerhedsniveauer, der ikke kan implementeres lige så godt i en konventionel centraliseret løsning.”

1

Blockchain muliggør at integritet, tilgængelighed og fortrolighed kan understøttes i et distribueret peer-to-peer-netværk, hvilket gør det muligt at udvikle løsninger, der kræver sikker distribueret gensidig tillid i et økosystem.

Det er derfor nu muligt at placere kritiske data eller programmer på blockchainen og være forvisset om at sikkerhedsmekanismerne kan implementeres på **samme niveau** som med et centralt betroet mellemled.

2

Blockchain muliggør distribueret tillid, hvilket vil ændre forretningsmodellen i alle brancher.

Før man vælger en blockchain-løsning, er det vigtigt at sikre sig, at man virkelig har brug for tilgængelighed, integritet og distribueret tillid blandt parter, som ikke kender hinanden, men som skal dele kritiske data og funktionalitet uden tilstedeværelsen af en betroet tredjepart.

3

Det er også vigtigt at forstå, at blockchain er en underliggende nøgleteknologi, ikke løsningen i sig selv.

Integration til forretningsprocesser og it-systemer kræver traditionel infrastruktursikkerhed og god kodepraksis på præcis samme måde som en centraliseret løsning.

“Det er derfor nu muligt at placere kritiske data eller programmer på blockchainen og være forvisset om at sikkerhedsmekanismerne kan implementeres på samme niveau som med et centralt betroet mellemled.”

Om forfatteren - Henrik Hvid Jensen

Henrik Hvid Jensen har en master i Computer Science og en bachelor i International Economics.

Han er idemanden bag og har designet Maersk/IBMs Blockchainløsning til digitalisering af verdenshandelen.

Henrik er i dag seniorkonsulent hos Trustworks og involveret i Port Collaborative Decision Making (Port-CDM); World Economic Forums initiativ for Inclusive Deployment of Blockchain for Supply Chains, hvor han er medforfatter af en anbefaling om at grundlægge en fælles digital Global Trade Identity (GTID) for regeringer og virksomheder involveret i verdenshandelen.

Henrik har desuden undersøgt brugen af Blockchain i Trade Single Windows.

Henrik rådgav Blockshipping vedrørende deres ICO såvel som designet af deres platform til et blockchain-baseret centralt registeringssystem til containere baseret på software agenter der kører autonomt på blockchainen.

Henrik har tidligere designet platformen til et af de globalt set mest lovende offentlige digitaliseringsprojekter; Tinglysningen i Danmark. Denne platform er han nu ved at indføre på Færøerne.

Henrik har baseret alle platforme på de visioner og digitale trends, som han har forklaret i sin bog, som han også har undervist i på Københavns Universitet og IT-Universitetet i København som ekstern lektor.

Henrik kan kontaktes på
https://www.linkedin.com/in/henrikhvid/
og henrik.hvid.jensen@trustworks.dk

TRUSTWORKS
RETHINKING IT AND BUSINESS