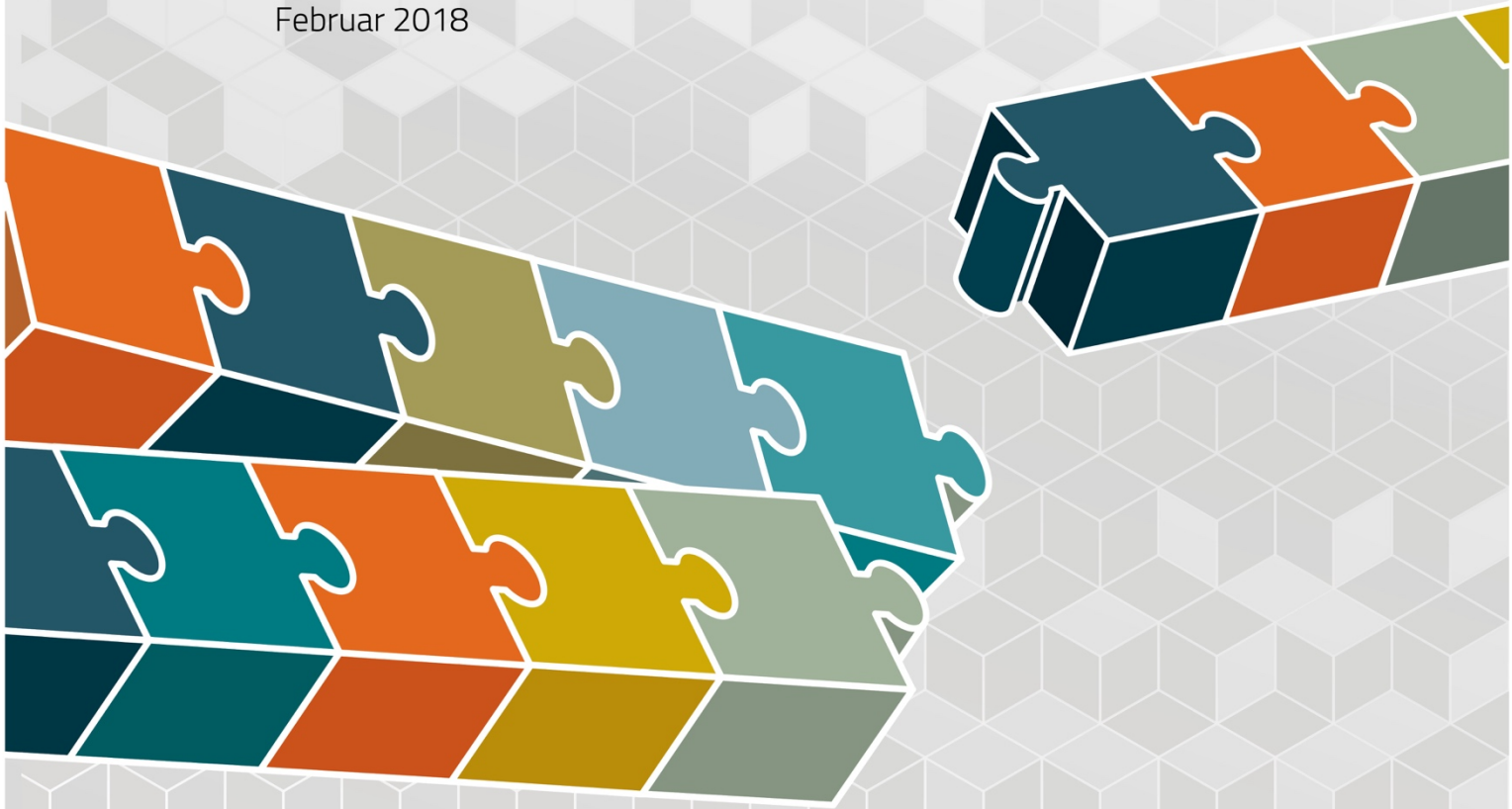
Blockchain potentialer

i den offentlige digitale infrastruktur

Februar 2018



Styrelsen for Dataforsyning og Effektivisering

ALEXANDRA INSTITUTTET

Indhold

Indledning

Blockchain er et af de mest hypede begreber i teknologiverdenen lige nu og har i den seneste tid høstet stor opmærksomhed i den globale offentlighed. Forventningerne er store. Blockchain bliver kaldt en lige så stor revolution som opfindelsen af internettet, og der bliver talt meget om de store potentialer, der ligger gemt i teknologien. Et potentiale der først rigtigt vil blive indfriet i årene, der kommer.

Teknologien er stadig ny og relativt uprøvet, og de konkrete erfaringer er meget begrænsede. Derfor kan det være svært at få greb om teknologiens muligheder og begrænsninger. Ikke mindst fordi der er så meget hype omkring teknologien, at svaret næsten er givet på forhånd. Men hvad er det særlige ved blockchain-teknologien? Og hvordan kan teknologien anvendes i praksis?

Denne rapport sætter fokus på de fremtidige anvendelsespotentialer for blockchain, men med udgangspunkt i de konkrete erfaringer, der gøres lige nu af nogle af frontløberne inden for området. Ud fra devisen, at *fremtiden er nu*, ønsker vi at give et håndgribeligt billede af, hvad teknologien rummer og skabe et mere konkret afsæt for at vurdere teknologiens anvendelsespotentialer.

Det bærende element i rapporten er fem vidt forskellige eksempler på, hvordan private og offentlige organisationer arbejder med at udvikle og implementere blockchain-teknologi, og har dermed fokus på de teknologiske såvel som de organisatoriske og forretningsmæssige aspekter ved udviklingen.

Formålet med rapporten er at give inspiration til konkrete anvendelser af blockchain og skabe et solidt fundament for at vurdere teknologiens anvendelsespotentialer inden for den offentlige digitale infrastruktur.

Rapporten er udarbejdet i et samarbejde mellem Alexandra Instituttet og Styrelsen for Dataforsyning og Effektvisering,

Ledelsesresumé

Anvendelsespotentialer for blockchain
Denne rapport sætter fokus på de fremtidige anvendelsespotentialer for blockchain med udgangspunkt i konkrete erfaringer, der gøres lige nu af nogle af frontløberne inden for området. Med afsæt i fem vidt forskellige cases, som er eksempler på, hvordan private og offentlige organisationer arbejder med at udvikle og implementere blockchain-teknologi, giver rapporten et håndgribeligt billede af, hvad teknologien rummer af muligheder og hvilke faktorer, der påvirker mulighederne for at indfri potentialerne ved blockchain.

Teknologien
Selvom *blockchain* er et at de mest hypede begreber i teknologiverden lige nu og samtidig en teknologi, der på nuværende tidspunkt, kun er meget vagt defineret, vil en række centrale teknologiske egenskaber typisk være tilstede i et blockchain-system. Rapporten giver et bud på disse egenskaber og beskriver, hvordan teknologien fungerer og placerer sig i landskabet af distribuerede systemer. Forskellen mellem åbne og lukkede blockchain-systemer trækkes op, eftersom forståelsen af blockchain meget nemt overskygges af de undertiden spektakulære sager, der bæres frem i pressen og teknologiverdenen. Sager, der oftest handler om de mest kendte digitale valutaer som fx Bitcoin – og de baserer sig netop på åbne blockchain-systemer.

Fem cases - fem eksempler på konkrete anvendelser
Alle fem cases, der indgår i denne rapport er produceret med eller tænkes produceret med det man kalder lukkede blockchain-teknologier, hvor kun en begrænset gruppe deltager i blockchainen. Dette har ikke været et udvælgelseskriterie, men er i praksis det tekniske set-up man har valgt i projekterne. Et valg der bl.a. begrundes i et behov for at begrænse transparens og beskytte data.

Casene viser derudover en bredde i anvendelsesmuligheder inden for fem vidt forskellige sektorer og i forhold til meget forskellige typer af udfordringer, der enten direkte eller indirekte relaterer sig til udviklingen af den offentlige digitale infrastruktur og den rolle det offentlige spiller i udviklingen af initiativer inden for dette område. Alt i alt giver case-beskrivelserne et helhedsorienteret billede og afdækker både de tekniske, de organisatoriske og forretningsmæssige aspekter af projekterne – og ikke mindst det indbyrdes samspil mellem disse.

Særlige potentialer
På tværs af de fem eksempler på konkrete anvendelser træder en række særlige potentialer frem.

I flere cases er effektivisering et fremtrædende tema. Når parterne i casene vurderer, at den økonomiske værdi er høj, er en vigtig pointe fra disse cases, at blockchain ikke gør det alene, da teknologien i eksemplerne udgør et element i en større digitaliseringsøvelse.

Et andet potentiale, der træder frem, er teknologiens særlige egenskaber i forhold til at sikre dataintegritet. I tre ud af fem cases sikres dataintegriteten ved, at blockchain-databasen er distribueret i en kopi enten hos udvalgte aktører eller blandt alle parterne i netværkene omkring systemet. En enkelt case skiller sig ud ved

ikke at have et netværk af aktører omkring selve blockchainen og at dataintegriteten sikres via én ekstern kontrolinstans. Sporbarhed er et nøgleelement i alle fem cases, hvor blockchain-løsningen ifølge projektejerne sikrer provenance (sporbarhed) og transparens for parterne i netværket. Det er vigtigt at understrege, at det ikke handler om datatransparens (da data ofte vil være fortrolige), men derimod om procestransparens. Parter, der hver især udgør en form for informations-ø i dag, vil blive bundet sammen af løsningen, så et fællesskab af aktører kan få overblik over en transaktionsproces.

At aktørerne omkring blockchain-løsningerne vil få nye roller er tydeligt i en række cases. Et særligt potentiale, der træder frem, handler om ejerskab og kontrol i forhold persondata og datadeling, mens et andet potentiale knytter an til nye forretningsmodeller, hvor producent-, leverandør- og forbrugerroller er under forandring.

At tilliden er distribueret i et netværk er en anden helt central faktor på tværs af casene. Selv om teknologien åbner for store potentialer, da den kan befordre tillid mellem parter i et distribueret netværk, er en vigtig pointe i analysen af de fem cases, at der ofte er en vis form for tillid tilstede mellem parterne i forvejen, for at der er vilje til at indgå i en fælles løsning. Samtidig rummer dette et paradoks – for har en kreds af aktører først formået at få organiseringen og samarbejdet på plads, vil det i praksis overflødiggøre nogle af blockchains særlige teknologiske potentialer.

I hvilken udstrækning disse potentialer er relevante i forhold til offentlige digitaliseringsprojekter vil høj grad afhænge af det konkrete projekt, men helt centralt står teknologiens mulighed for at håndtere processer og systemer, hvor mange parter er involveret, men hvor ingen af disse oplagt kan fungere som betroet tredjepart.

Det er vigtigt at bemærke at potentialerne er meget kontekstafhængige og i høj grad præget af at alle casene er lukkede blockchains. Det ser ud til at man her har fundet en model, der passer godt ind i organisatoriske set-ups, hvor det kan være afgørende at beskytte data (f.eks. forretningskritiske eller personfølsomme data) og hvor gruppen af aktører er kendte. Dette vil formentlig også gøre sig gældende for mange digitale infrastrukturprojekter. Derfor vil det i den videre vurdering af blockchain-teknologiens potentialer være vigtigt at have særligt fokus på lukkede blockchains.

Centrale forudsætninger

Når man ser på tværs af de fem cases, er det tydeligt, at der er en række faktorer, der påvirker mulighederne for at indfri potentialerne ved blockchain. Erfaringerne fra de fem cases viser med al tydelighed, at teknologien ikke i sig selv kan indfri potentialerne ved blockchain. Det er helt afgørende at se blockchainteknologien som en del af et større samspil. Både i forhold til det tekniske landskab den indgår i, og i særdeleshed i den organisatoriske, lovgivningsmæssige og forretningsmæssige virkelighed blockchainen implementeres i.

Betydningen af de forskellige aspekter og deres indbyrdes samspil vil variere. I nogle projekter vil det organisatoriske kun spille en lille rolle. I andre vil det være her fokus bør ligge. Det kan være et projekt forudsætter en hel ny samarbejdsstruktur med parter, der ikke før har samarbejdet. Måske får den offentlige part en helt ny rolle. I nogle projekter vil realiseringen af projektet kræve ændringer af lovgivningen internationalt. I andre spiller lovgivningen måske kun en begrænset rolle med mindre justeringer i form af i sektorspecifikke reguleringer. I vurderingen af anvendelsen af blockchain i den offentlige digitale infrastruktur

er det derfor afgørende have et helhedsorienteret fokus på det tekniske og organisatoriske samspil blockchain-løsningen skal indgå i.

Valget af blockchain

Det kan være svært at vurdere, hvorvidt det giver mening at bruge blockchain. Blockchain giver nogle unikke muligheder for at sikre dataintegritet og sporbarhed i et set-up, hvor der ikke er fuldstændig tillid mellem de parter, der indgår i løsningen. Til gengæld er det en mere kompliceret og tungere løsning, der er meget ung og derfor baserer sig på relativt uprøvede løsninger. Nogle af de egenskaber, en blockchain giver, kan opnås med andre, mere gennemprøvede løsninger, og de kan derfor være at foretrække. Disse teknologiske alternativer, herunder Centraliseret database, Public Key Infrastructure og Linkede databaser, beskrives i et separat afsnit i rapporten, hvor også risici- og sikkerhedsimplikationerne ved blockchain-løsninger diskuteres.

Vurderingen bliver heller ikke nemmere af, at det på nuværende tidspunkt er meget uklart defineret, hvad der udgør en blockchain. Desuden er vi i en situation, hvor blockchain er meget hyped, hvilket giver et incitament til at omtale egen teknologi som en blockchain, selvom den måske ikke i alles øjne opfylder kriterierne for at være det.

Den hype, der er omkring blockchain, betyder dog også, at der er et utal af projekter i gang, der forsøger at implementere blockchain i mange forskellige løsninger i mange forskellige brancher og domæner. Når resultaterne af disse projekter efterhånden kommer frem, vil det gradvist blive nemmere at lave en kvalificeret vurdering af, hvilke fordele en blockchain har ift. andre teknologier, om løsningerne kan gøres anvendelige, selvom de baserer sig på kompliceret teknologi, og om de kan skalere til store løsninger med mange transaktioner. Der ligger her en vigtig teknologisk modningsproces, som er vigtig at understøtte, bl.a. gennem øget fokus på den standardiseringsproces, der er iværksat internationalt i forhold til blockchain-teknologien.

Generelt om blockchain

Begrebet *blockchain* opstod oprindeligt som en beskrivelse af den konkrete teknologi, der underligger den digitale valuta, Bitcoin. Selvom der allerede på det tidspunkt var flere systemer med de egenskaber, vi forbinder med Blockchain, i udvikling og enkelte i produktion, er det først med Bitcoin paperet[1] i 2009, at blockchain bliver en betegnelse for en særlig teknologi.

I dag er blockchain-teknologien meget vagt defineret, og begrebet bruges ofte løst til at beskrive en lang række teknologier med mere eller mindre ensartede egenskaber. Samtidig sker der det, at systemer, der blot har få af disse egenskaber, kaldes blockchain. At lave en generel beskrivelse, der er dækkende for samtlige blockchain-systemer, er dermed en umulig opgave på nuværende tidspunkt.

Typisk vil en række centrale teknologiske egenskaber dog vil være tilstede, og vi vil derfor give vores bud på de vigtigste samlende egenskaber ved blockchain-teknologi i denne del af rapporten.

Hvad er blockchain?

Blockchain-teknologi er kort formuleret et distribueret system, der gør det muligt for deltagerne i et digitalt netværk i fællesskab at vedligeholde en database. Denne database kaldes ofte en *ledger*, og blockchain-teknologi kaldes derfor også af mange Distributed Ledger Technology (DLT). Andre lidt mere abstrakte men alligevel rammende betegnelser, der bruges om denne database, er 'liste' og 'register'.

Samlet er blockchain kendetegnet ved at:

- Databasen er distribueret blandt deltagerne i netværket.
- Deltagernes tilføjelser til databasen optages kun, hvis de er tilladte.
- Der er konsensus blandt deltagerne om, hvilken version af databasen, der er gyldig.
- Den version af databasen, der er opnået enighed om er den gyldige, er uforanderlig i den forstand, at der kun kan tilføjes i databasen.

At databasen er distribueret blandt deltagerne i netværket betyder, at alle deltagere har en fuld kopi af databasen. De kan dermed følge, hvad der foregår, og hvad der opdateres, og alle ændringer kan trackes over tid. Når deltagernes tilladte tilføjelser optages i databasen, sker det som resultatet af, at deltagerne overholder reglerne for blockchain-systemet.

Der kan kun *tilføjes* i databasen, hvilket betyder, at modificeringer også registreres som en tilføjelse. At der er konsensus blandt deltagerne om, hvilken version af databasen, de betragter som den gyldige, betyder, at

[1] Nakamoto, Satoshi "Bitcoin: A Peer-to-Peer Electronic Cash System"

alle har adgang til 'a single point of truth'. Samtidig gælder det, at databasen i princippet er uforanderlig, når der blandt deltagerne er opnået enighed om, hvilken version er den gyldige.

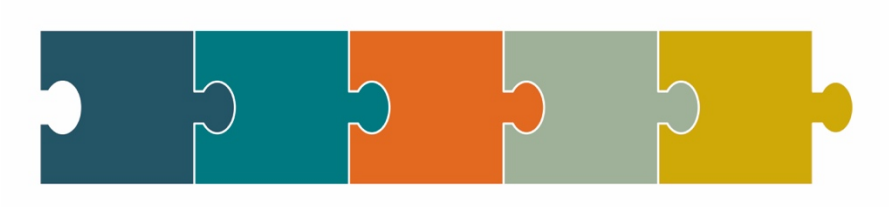
Uforanderligheden *(immutabiliteten)* sikrer, at den enkelte deltager kan føle sig sikker på, at data ikke senere kan annulleres eller ændres, hvis der først er opnået konsensus om den i netværket og den er tilføjet til blokchainen. Deltagerne skaber med andre ord et uforanderligt register, der inkluderer alle transaktionerne i netværket, og registreringerne i databasen kan ikke forfalskes, slettes eller manipuleres.

Uforanderligheden er en egenskab, vi vælger at beskrive som *principiel*, da der i forbindelse med praktiske erfaringer med blockchain i konkrete anvendelser er flere og flere eksempler på, at denne immutabilitet, der ellers er en central teknologisk egenskab, sløjfes af aktørerne, når blockchain-deltagerne i fællesskab beslutter sig for at rulle en given transaktionshistorik tilbage.

Tilliden i blockchain-systemet er ikke knyttet til en central autoritet – et mellemled – men i stedet distribueret mellem parter i netværket som helhed. Med andre ord har deltagerne i et blockchain-system som udgangspunkt ikke brug for at etablere et tillidsforhold til hver af de øvrige deltagere, så længe de har tillid til det samlede netværk af deltagere. Det gør det muligt for deltagere at indgå i blockchain-systemer med parter, de ikke kender, eller eventuelt ikke har tillid til. Det kan for eksempel være konkurrenter.

Hvordan fungerer blockchain?

Transaktionerne, der registreres i databasen, er sikret via kryptografi. Over tid bliver denne transaktionshistorik låst i blokke af data. Når først en blok er skabt, kan den i princippet ikke laves om. Datatilføjelser vil indgå i nye blokke, så det altid er muligt at spore forandringer kronologisk og dermed have en sikker fælles historik. I de enkelte blokke ligger der foruden registreringerne af transaktioner en registrering af handlinger – en sekvens, der ikke kan ændres, når først blokken er låst. Blokkene er kryptografisk forbundet med hinanden og sikrede, idet der i hver ny blok foruden data lægges en såkaldt hash fra den forrige blok, så blokkene er forbundet i en kæde.



Figur 1: Datatilføjelser indgår i nye blokke, der er sikrede og kryptografisk forbundet med hinanden

En blok lukkes, og en ny tom blok etableres, hver gang et avanceret regnestykke er løst. Dette kendes som *hashing*. Hashing er en gammel kryptografisk byggesten og giver hver transaktion en unik kode.

Hashingen tager med andre ord data (det kan være en tekst eller en hvilken som helst form for digital fil) og spytter en bitstreng (unik kode) ud med en fast længde, også kendt som hash-værdien. Forholdsvis let kan man via avancerede beregninger gå fra data til hash-værdi, mens det er umuligt kryptografisk at bevæge sig den anden vej, da det regnestykke vil tage alt for lang tid. Det betyder at man kan skabe sikkerhed for at data er uforandret samtidig med at det er umuligt at udlede, hvad der stod i data.

Figur 2: Hashingen tager data, som kan være en tekst eller en hvilken som helst form for digital fil, og spytter en bitstreng (unik kode) ud med en fast længde, også kendt som hash-værdien.

Forskel på åbne og lukkede blochchains

Der findes åbne og lukkede blockchain-systemer. Åbne blockchains kendes også som public, offentlige og permission-less, hvilket vil sige, at alle kan deltage, mens lukkede blockchains kendes som private og permissioned, hvor der er enighed om, hvem der kan deltage.

Det er vigtigt at trække de vigtigste forskelligheder op mellem åbne og lukkede. For det første er systemernes egenskaber uens, og der er betydningsfulde forskelle i elementer som deltagerkreds, tidsfaktor, performance og skalerbarhed. For det andet er det vigtigt at være opmærksom på, at en mere nuanceret og kritisk forståelse af blockchain meget nemt kan overskygges af, at de undertiden spektakulære sager, der bæres frem i pressen og teknologiverdenen, oftest har fokus på nogle af de mest kendte digitale valutaer som fx Bitcoin – og de baserer sig netop på åbne blockchain-systemer.

Åben – public, offentlig, permission-less

- Alle kan i princippet deltage
- Mange aktører i netværket
- Delvis anonymitet
- Tung transaktionstid, højt energiforbrug og enorme omkostninger pga. den store regnekraft, der skal til for at deltage i konsensusprocessen (kendt som *mining*)
- Alle transaktioner er synlige
- Deltagere kan ikke ekskluderes

Eksempler på blockchain-teknologier:
Bitcoin, Ethereum

Lukket – privat, permissioned

- Enighed om, hvem deltager
- Oftest en begrænset deltagerkreds
- Deltagernes identitet kendes af parterne
- Regler og kontrolmekanismer til at nå konsensus er defineret af netværket.
- Mulighed for at spare på regnekraften
- Reguleret synlighed
- Deltagere kan ekskluderes

Eksempler på blockchain-teknologier:
Multichain, Postchain, KSI blockchain, Hyperledger Fabric

En åben blockchain er karakteriseret ved, at alle i princippet kan deltage i at drive blockchainen i overensstemmelse med konsensusprotokollen, eller konsensusmekanismen som den også kaldes. Protokollen er en beskrivelse af, hvad man skal gøre som deltager og hvordan.

Da alle kan deltage, kan der være mange deltagere, og aktørerne i netværket kender ikke hinanden. Et eksempel på en åben blockchain er Bitcoin, hvor deltagerne i netværket (også kaldet *minere*), deltager i et kapløb i regnekraft om at få lov til at validere og dermed tilføje næste blok til blockchainen. Denne protokol kendes som *proof-of-work*. I en åben blockchain som Bitcoin er incitamentet for at være *miner* penge, da den miner, der vinder ved først at løse et bestemt kryptologisk regnestykke, udover at få lov til at tilføje næste blok til blockchainen også får en gevinst.

Denne proces er i dag meget dyr at lave og er reelt centraliseret på nogle få hænder. Dette står i kontrast til det demokratiske, ligeværdige peer-to-peer-projekt, det var lagt op til at være. Uden at gå videre i dybden med de forskellige konsensusprotokoller vil vi nævne, at der findes en hel række alternativer, fx *proof of stake (hvor* brugernes bitcoin-beholdning afgør, hvor sandsynligt det er, at de genererer blokken og høste belønningen), og at der udvikles nye former for protokoller.

I lukkede systemer, hvor aktørerne i netværket kender hinanden, kan skalerbarheden nemmere øges. Eftersom konsensusmekanismen er meget mindre omkostningstung, kan blockchain-systemet håndtere mange flere transaktioner meget hurtigere. Processerne bliver således mere enkle, idet konsensusmekanismen kan gøres mere effektiv, fordi man er i netværket med kendte aktører, og man behøver derfor ikke et kapløb i regnekraft som beskrevet ovenfor, hvorfor der kan spares på den regnekraft, der skal være tilstede.

Blockchain i landskabet af distribuerede systemer

En database implementeret via blockchain er et distribueret system. Når man skal vurdere anvendeligheden af distribuerede systemer anvender man ofte principperne i det der hedder *CAP teorem*. CAP står for *consistency*, *availability* og *partition tolerant* og dækker over tre ønskværdige egenskaber ved et distribueret system.

Consistency betyder, at systemet er konsistent, således at alle parter altid ser det distribuerede system i den samme tilstand som de andre parter. Availability betyder, at systemet altid er tilgængeligt for operationer fra alle parter. Partition tolerant betyder, at systemet kan tolerere, at der opstår partitioner i netværket af parter, dvs. at grupper af parter kan være afskåret fra resten netværket, fx i forbindelse med fejl i det fysiske netværk.

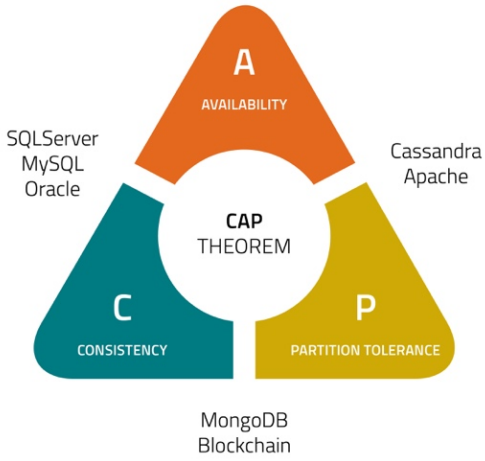
CAP-teoremet siger, at et distribueret system højest kan opfylde to ud af disse tre egenskaber samtidigt. CAP-teoremet beskriver således, at der i ethvert distribueret system findes et trade-off imellem disse tre egenskaber. Derfor inddeler man ofte systemer efter hvilke af de tre egenskaber, der fokuseres på. Fx anses systemer baseret på traditionelle SQL-databaser typisk som såkaldte AC-systemer, dvs. systemer der garanterer availability og consistency men ikke partition tolerance. På den anden side anses moderne NoSQL-databaser typisk som enten AP (fx Cassandra) eller CP (fx MongoDB).

I forhold til CAP-teoremet kan blockchain siges at falde i kategorien af CP-systemer, dvs. det tilbyder consistency og partition tolerance. Partition tolerance sikres af blockchains distribuerede natur. Opstår en partition, kan den udgave af databasen hvorom der tidligere er opnået konsensus

stadig tilgås af alle parter. Når der er opnået konsensus om en givet version af databasen, vil alle parter se den samme uforanderlige database, og således opnås consistency. I tilfælde af en netværkspartition kan det dog være problematisk at opnå konsensus omkring blockchainen i hele netværket. Derfor kan availability ikke altid garanteres, da en tilføjelse til databasen først vil ses som gyldig, når konsensus er opnået.

I vurderingen af anvendeligheden af blockchain-teknologien kan CAP teoremet bruges som redskab til at synliggøre teknologiens fordele og ulemper i forhold til andre distribuerede systemer.

Vi bemærker dog, at selv om der i følge CAP-teoremet ikke kan 'garanteres' alle tre egenskaber i alle situationer, betyder det ikke, at man helt må opgive den tredje egenskab.
Dvs. at så længe netværket ikke er opdelt, kan der også være en høj grad af availability i et blockchain-system, bl.a. via dets distribuerede natur. Det er desuden vigtigt at understrege, at de fleste systemer (inklusiv blockchain) kan konfigureres til at ligge det sted i trekanten man ønsker.



Figur 3: Ofte inddeler man distribuerede systemer efter CAP-teorems-principper og figuren beskriver, hvorledes der er et trade-off mellem de tre ønskværdige egenskaber ved systemet. Blockchain siges at falde i kategorien af CP-systemer.

Konkrete anvendelser

I processen med at udvælge cases til denne rapport har vi foretaget en screening af blockchain-projekter både nationalt og internationalt. Der viste sig at være overraskende få, og mange er endnu kun på det konceptuelle stadie, hvor man udvikler nye forretningsmodeller og overvejer det teknologiske og organisatoriske set-up.

De fem cases, vi har udvalgt til denne rapport, udmærker sig ved alle at være kommet skridtet længere i processen. En af casene er allerede i drift, mens de andre er på forskellige stadier af pilotafprøvning. Mange valg *er* foretaget, men det er vigtigt at understrege, at det er projekter under udvikling, som befinder sig i et stadie, hvor de er afsøgende og eksperimenterende. Meget kan derfor stadig nå at ændre sig i det teknologiske set-up, og i de fleste cases arbejder man stadig på at få det organisatoriske og forretningsmæssige på plads. Det er vigtigt, at casene læses med dette for øje.

Udvælgelse af cases

Vi har i udvælgelsen af cases lagt vægt på at vise en bredde i anvendelsesmulighederne. Casene er derfor sammensat, så de demonstrerer, hvordan teknologien anvendes inden for fem vidt forskellige sektorer og i forhold til meget forskellige typer af udfordringer. Vi har desuden lagt vægt på at udvælge cases, som håndterer problemstillinger, der enten direkte eller indirekte relaterer sig til udviklingen af den offentlige digitale infrastruktur og den rolle det offentlige spiller i udviklingen af initiativer inden for dette område.

Alle cases, der indgår i denne analyse, er enten produceret med, eller tænkes produceret med lukket blockchain-teknologi. Dette har ikke været et udvælgelseskriterie for os, men i praksis har dette været det tekniske set-up, man har valgt i projekterne. I casen om tracking af containere (case 3) og casen, der handler om balancering af el-nettet (case 5), testes løsningerne med Hyperledger Fabric-teknologi. Beskyttelse af persondata i elektronisk patientjournal i Estland (case 2) bygger på den specialiserede KSI blockchain, der er udviklet og patenteret af den estiske virksomhed Guardtime. I casen, der handler om administration af persondata i den finansielle sektor (case 1) produceres løsningen med Multichain-teknologien af den danske start-up New Banking, mens systemet til registrering af ejerskab i Sverige (case 4) tænkes produceret af den svenske virksomhed Cromaway med Postchain-teknologi. De konkrete use cases giver således indblik i forskellige modenhedsgrader af private blockchain-systemer.

Indholdet af casene

Case-beskrivelserne er udarbejdet i et tæt tværfagligt samarbejde mellem Alexandra Instituttets specialister med det formål at skabe et helhedsorienteret billede af de erfaringer, som projekterne lige nu gør sig i udviklingen og implementeringen af blockchain-løsninger. Vi har således haft fokus på at afdække både de tekniske og de organisatoriske og forretningsmæssige aspekter af projekterne – og ikke mindst det indbyrdes samspil mellem disse.

Casene er baseret på interviews med projekternes parter. I det omfang det har været muligt har vi interviewet både både projektejere og softwareleverandører.[2] Indholdet og detaljeringsniveauet i de enkelte cases er i høj grad afgjort af, hvor langt projekterne er i udviklingsprocessen, og hvor åbne organisationerne har kunnet tillade sig at være om deres strategier og interne udviklingsprocesser – under hensyntagen til NDA'er m.m.

[2] I case 4 *Registrering af ejerskab* er casen dog baseret på en offentlig rapport: *The Land Registry in the blockchain – testbed*.

Case 1: Validering af persondata

Effektvisering af KYC-processer

New Banking er en dansk start-up virksomhed, der har specialiseret sig i udvikling af systemer til håndtering af personfølsomme data via anvendelse af blockchain-teknologi.

De arbejder med en teknologisk platform, der skal effektivisere bankernes valideringsprocesser i forbindelse med oprettelsen af nye kunder. Know Your Customer, også kaldet KYC, er en valideringsproces, som banker gennemgår med nye kunder. KYC er en del af reguleringen af den finansielle sektor og er med til at undgå, at bankerne bliver brugt til hvidvaskning af penge. Ved hjælp af KYC sikrer banken, at den kender nye kunders identitet.

Danmark

Blockchain Type
Multichain (Lukket)

MODENHED
Pilot

FØR

Fra manuel håndtering

Processen er i dag manuel og kræver typisk, at banken indhenter en lang række oplysninger og dokumenter fra kunden. Dette kan fx omfatte kopi af pas, kørekort, adresse- og cpr-oplysninger. Efterfølgende gennemgår bankens medarbejdere materialet for at sikre sig oplysningernes rigtighed og dokumenternes ægthed, undertiden via involvering af en tredjepart. Dette er en kompleks og tidskrævende proces, som kræver mange ressourcer af bankerne. For kunden er processen yderligere tidskrævende, da den skal gennemføres i forhold til alle kundernes bankforbindelser og skal gentages hver gang, kunden måtte ønske at skifte bank. Desuden kan det være svært for kunden at danne sig et overblik over, hvilke banker der ligger inde med kopier af vedkommendes personlige dokumenter.

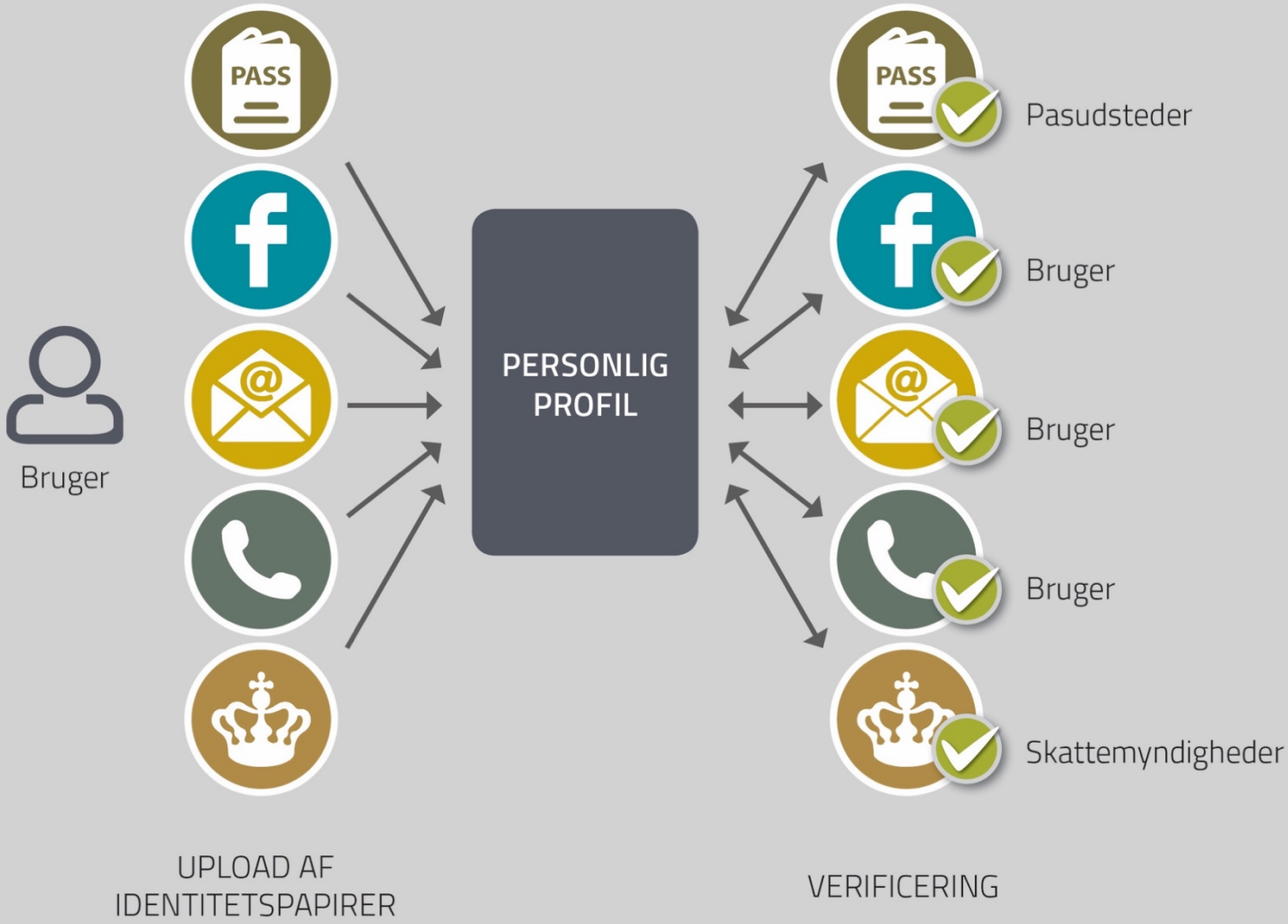
EFTER

Til fuldautomatisk verificering

New Bankings løsning samler de personlige data ét sted uafhængigt af den enkelte bank. Ideen er at kunden én gang for alle indtaster sine oplysninger i New Bankings system og uploader forskellige informationer om sig selv. Det kan være kopi af pas og kørekort. Det kan også være personlige oplysninger som fx mailadresse, telefonnummer, forskellige profiler på de sociale medier eller andre oplysninger, der kan være med til at dokumentere, at brugeren rent faktisk er den, han påstår, han er.

Oplysningerne verificeres herefter i en fuldautomatisk proces, hvor brugeren selv verificerer sine oplysninger gennem feedbackmekanismer via fx mail og sms. Virksomheden har desuden indgået samarbejde med bl.a. Gemalto, en stor international pasudsteder, om automatisk verificering af pas og kigger på mulighederne for at anvende forskellige offentlige registre i valideringsprocessen.

Den nye løsning



New Banking forventer, at der vil være store gevinster at hente for bankerne alene på automatiseringen af KYC-processen. Men det løser i høj grad også en udfordring i forhold til EU's nye Persondataforordning (GDPR). Det centrale er, at de personfølsomme data flyttes ud af banken og i stedet placeres under kundens egen kontrol. Fra et kundeperspektiv betyder det, at det ikke længere er nødvendigt at tage hen til bankens filial for at aflevere dokumentationen eller sende den via e-mail med de sikkerhedsrisici, dette indebærer. Samtidig får kunden et samlet overblik over, hvilke personlige oplysninger de forskellige banker ligger inde med.

Hvordan indgår blockchain i løsningen?

New Banking-systemet giver den private kunde et overskueligt interface, hvor kunden let kan give samtykke og inddrage adgang til data. Det er i denne del af processen, New Banking anvender blockchain-teknologien. Selve persondataene ligger i en krypteret database kontrolleret af New Banking. New Banking bruger så blockchain-teknologien til at styre, hvem der har rettighed til at se hvilke data. Det foregår på den måde, at New Banking indgår i en lukket blockchain med de involverede banker. På blockchainen lægges således adgangsnøgler til kundens data på en sådan måde, at kun de rette banker kan tilgå nøglen. Og samtidig lægges et krypteret fingeraftryk af blockchainen hos de enkelte banker, som hele tiden verificerer op mod blockchainen og dermed sikrer systemet mod uautoriserede ændringer i blockchainen. Men det sker ikke med en såkaldt *proof of work*. De benytter sig i stedet af en rettighedsbaseret algoritme. En model de i øjeblikket er i gang med at patentere.

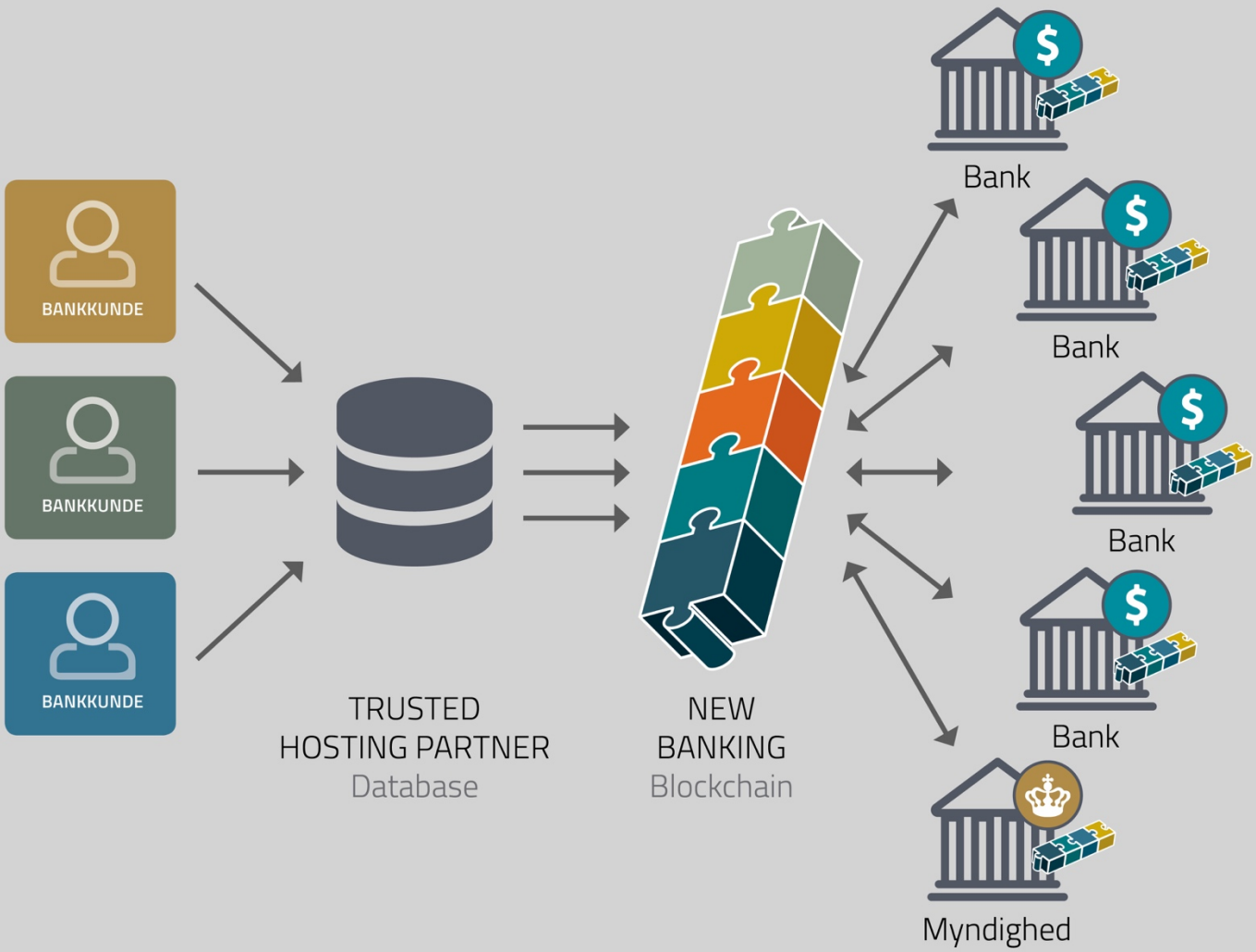
New Banking har i den sammenhæng valgt at bruge den private blockchain-teknologi, Multichain, som er en specifik videreudvikling af Bitcoin. Det har først og fremmest betydet, at teknologien allerede er velafprøvet og har nået det nødvendige modenhedsniveau. Men New Banking har også fundet Multichain velegnet, fordi der er lavet en enterprise-udgave, der bl.a. giver gode muligheder for permission management. Permissions er et vigtigt redskab for New Banking til at styre governance – altså hvem der har rettighed til at læse hvad – og da teknologien samtidig giver mulighed for at oprette såkaldte *streams* til de forskellige kunder, så kan New Banking sikre, at når en kunde giver samtykke, bliver det kun kanaliseret videre til den involverede bank. På sigt forestiller New Banking sig desuden, at offentlige myndigheder, som fx Finanstilsynet, kan indgå som en del af netværket. Dette vil skabe yderligere transparens og styrke compliance.

Hvorfor en blockchain?

Den væsentligste årsag til at New Banking har valgt at implementere en blockchain i deres løsning er at sikre provenance, dvs. at der er en indbygget beviselighed i løsningen. At man til enhver tid kan dokumentere, hvem der har haft rettigheder til at se informationerne på et givent tidspunkt. Det er afgørende i forhold til at kunne dokumentere, at systemet er compliant.

Når du har opsagt dit samarbejde, så går der måske tre uger, så modtager du en marketing-mail. Hvis du har trukket dit samtykke tilbage, så vil banken sidde med røde ører. Men hvis det kommer til en sag, så kommer det til at handle om provenance. Blockchainen dokumenter det. Så vil myndigheden have adgang til at se nøjagtigt, hvornår du trak dit samtykke tilbage… Vi vil gerne være regulators friend.

Blockchainens funktion



Blockchainen bruges i dette projekt til at administrere rettigheder til at se data. Data ligger i en central database, som hostes af en betroet ekstern udbyder. Blockchainen sikrer integritet, ved at kopier af blockchainen ligger hos flere parter. En myndighed (fx Finanstilsynet) vil indgå som ekstra kontrolinstans, der sikrer, at der ikke ændres i blockchainen.

Opmærksomhedspunkter i implementeringen af Blockchain

Nøgleord
Governance
Compliance
Provenance
Standardisering
Certificeringer

Behov for etablering af tillid omkring produktet

I en gennemreguleret branche som banksektoren er det helt afgørende at kunne dokumentere, at man som virksomhed er compliant. Derfor er New Banking i gang med en omfattende certificeringsproces bl.a. i forhold til sikkerhed og EU's Persondataforordning (GDPR). Det handler på den ene side om at få skabt tillid til, at den tekniske løsning fungerer, som den skal, og driftes på en forsvarlig måde. Det handler på den anden side i lige så høj grad om at udvikle modeller, der tager højde for fx kontraktophør og konkurs. Her arbejder New Banking med etablering af partnerskaber med en række tredjeparter, fx KPMG, PWC og IBM, der skal være med til at skabe den nødvendige tillid til den tekniske løsning og New Bankings governance. En klar udfordring I denne sammenhæng er, at teknologien stadig er helt ny og uprøvet, og at der derfor endnu ikke findes fælles standarder inden for området.

Der bliver gjort en masse fejl derude lige nu, og blockchain bliver brugt til en masse, det slet ikke er egnet til.

Behov for udvikling af internationale standarder

New Banking har i den sammenhæng involveret sig i det internationale standardiseringsarbejde omkring blockchain. Det handler både om at få etableret en standard for hele governance-delen, fx hvordan man administrerer blockchains, hvordan man sikrer blockchains, og hvilken form for forhandling, der skal finde sted for at sikre compliance. Det handler også om tekniske standarder.
Hvordan håndteres fx nøgler, og hvordan får man basalt set skabt enighed om terminologierne. I sidste ende handler det om at sikre interoperabilitet inden for området, så de mange blockchain-implementeringer ikke kommer til at fungere som isolerede øer men også har forudsætningerne for at spille sammen.

Der er en masse forvirring omkring terminologi, og den bliver kun større, når man graver i overfladen. Vi er nødt til at være enige om, hvad vi snakker om.

Vi vil gerne kunne sige, at vi er compliant med standarden. Så kan vores kunder nemmere skifte til andre. Et regulatorisk krav kan også være, at andre skal kunne få adgang.

Case 2: Beskyttelse af person-data

Dataintegritet i elektronisk patientjournal

Hovedparten af de cirka 1.3 mio. borgerne i Estland har tilknyttet en elektronisk patientjournal, der lovpligtigt opdateres, hvergang sundheds-profesionelle lægger nye helbredsinformationer ind i det elektroniske system, *Estonian National Health Information system* (ENHIS). Når en borger ser sin læge, er på hospitalet, får en vaccine, modtager en recept, afhenter medicin på apoteket eller får taget prøver i et laboratorium opdateres informationerne i patientjournalen.

Med implementering af blockchain-teknologi har de estiske sundhedsmyndigheder ønsket at tilføre et ekstra lag sikkerhed til beskyttelse af persondata.

E-HEALTH
Estonian e-Health Foundation

guardtime

ESTLAND

BLOCKCHAIN-TYPE
KSI (lukket)

MODENHED
I drift

De anvender en specialiseret blockchain-teknologi, som er udviklet af den estiske virksomhed Guardtime. KSI blockchain, som den hedder, er opfundet og patenteret allerede to år inden blockchain kom. Den er således afprøvet og de første løsninger har været i produktion siden 2012. Teknologiens integration med det elektroniske patientjournalsystem er imidlertid ny, og denne specifikke løsning har været i drift mindre end et år.

Blockchainen integrerer med det eksisterende system

Med blockchainen er der ikke introduceret radikale ændringer i det eksisterende elektroniske patientjournalsystem, hvor data er lagret i det centrale register, som er en krypteret Oracle database. Den nye løsning er kendetegnet ved at være meget lidt gennemgribende, idet blockchainen lægger sig som et ekstra sikkerhedslag oven på det eksisterende system.

Sundhedsprofessionelle bruger den nationale krypterede kommunikations- og dataudvekslings- kanal X-Road til at udveksle data på sikker vis. Så selve blockchainen fungerer ikke som et register til deling eller udveksling af data, idet de personlige data, dvs. selve patientjournalerne, ikke lagres i selve blockchainen, men altså forbliver hos partnerne i netværket og i en krypteret database centralt. Da private data ikke opbevares i blockchainen rummer den ikke problemstillinger i forhold til den nye EU-dataforordning, GDPR, og udgør altså heller ikke nogen trussel for privatliv.

Fra et slutbrugerperspektiv, hvad enten der er tale om borgere eller sundhedsprofessionelle, er der ikke et 'før' og 'efter' blockchain i forhold til den elektroniske patientjournals funktionalitet. Borgerne havde allerede inden implementeringen af blockchain-løsningen mulighed for at kommunikere sikkert og udveksle personfølsomme oplysninger. Heller ikke for læger, sygeplejersker og andre sundhedsprofessionelle er der forandringer i, hvad de kan se og hvad de skal gøre, når der journaliseres i systemet. Med teknologien er der snarere tale om et administratorværktøj, der anvendes af sikkerhedseksperter. I de estiske myndigheder er det eksempelvis et sikkerhedsteam på tre personer, der blandt andet har som ansvarsområde at overvåge systemet.

Med implementeringen af blockchain-løsningen, er den væsentligste værdi for brugerne af systemet, herunder de estiske sundhedsmyndigheder, at de personlige data sikres endnu bedre mod trusler, uautoriserede opdateringer eller manipulation – fra intern såvel som ekstern hånd.

Det fungerer som ekstern bevis på at vi til stadighed er en troværdig organisation. At vi ikke forfalsker vores logs.

Hvordan indgår blockchainen?

Hver gang en sundhedsprofessionel opdaterer persondata i den elektroniske patientjournal dannes hashes, en slags fingeraftryk af data. Disse aggregeres med kort interval på blockchainen, der udsteder en digital kvittering i form af en signatur. Den registrerer tidspunkt og hvem der har lavet opdateringen, og fungerer som et ægthedsbevis på at hver opdatering er gyldig. Dermed låses data fast og kan ikke ændres, og enhver efterfølgende ændring vil kunne spores.

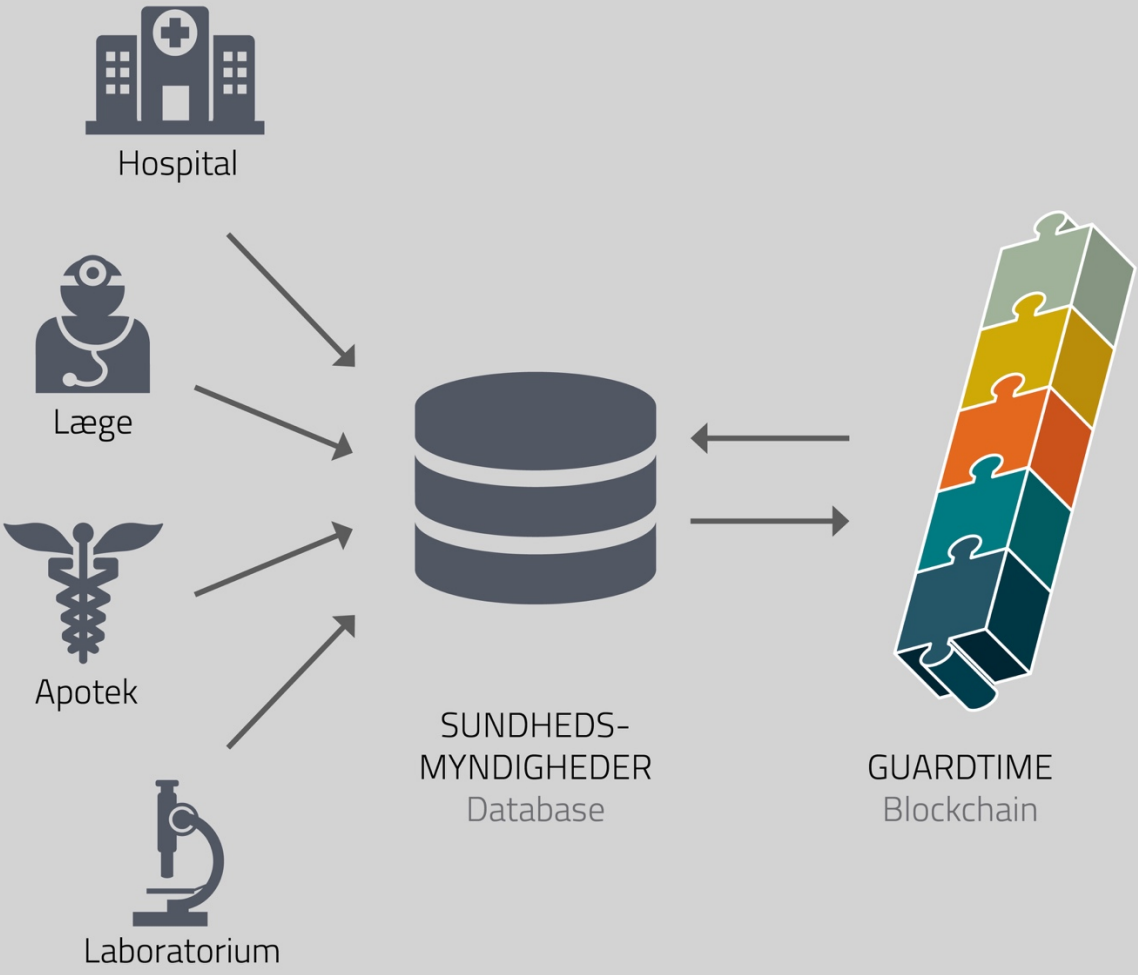
Blockchainen leverer beviser i forhold til tid, integritet og vidnesbyrd på oprindelse - altså provenance.

På trods af at der er mange aktører i sundhedssystemet er den eneste aktør, der taler direkte med blockchainen således det centrale register, der også lagrer signaturerne i en database centralt. Blockchainen ligger eksternt på en Guardtime-server, og er en del af deres service til de estiske myndigheder. En ekstra feature i Guardtimes service er, at de løbende publicerer blockchainens aktuelle rod-hash værdi i offentlige aviser, bl.a. Financial times. Publiceringen fungerer som et eksternt tidsstempel, ægthedsbeviset, der giver dataintegritet, sporbarhed og viser at opdateringer er gyldige.

Så er der nogen, hvad enten det er indefra eller udefra, der forsøger at lave uautoriserede ændringer eller manipulere data, skal de ikke blot manipulere de specifikke data men også dataloggen samt de to lag af hash-strenge. Den, der ligger centralt i myndighedernes egen database såvel som den, der ligger eksternt sikret hos Guardtime.

KSI blockchain er en lukket blockchain. Der er ikke behov for en konsensus protokol, da der kun er en part. Det betyder også, at transaktionsraten er høj og dermed meget mere effektiv end åbne blockchains. I den centrale database kan der hvert sekund være helt op til 5000 transaktioner, der hashes løbende, og disse fingeraftryk af data aggregeres efterfølgende på blockchainen. Selvom de interne administratorer har oplevet tekniske udfordringer i forhold til performance i implementeringsfasen, er det bemærkelsesværdige, at løsningen kan køre op mod så stort et system. Blockchainen er særlig i forhold til andre løsninger, idet den specielt er designet til denne type systemer, der hovedsageligt sikrer integriteten af data.

Blockchainens funktion



Blockchainen bruges i dette projekt som ekstra sikkerhedslag til beskyttelse af persondata. Data ligger i en central krypteret database hos de estiske sundhedsmyndigheder. Denne løsning er særlig idet der i dette projekt ikke er noget netværk af aktører. Blockchainen fungerer udelukkende som ekstern kontrolinstans i forhold til myndighederne og er med til at sikre at der ikke manipuleres med data. Blockchainen drives af det private firma, Guardtime.

Hvorfor en blockchain?

Adspurgt viser det sig at spille en rolle for de estiske sundhedsmyndighedes valg af denne blockchain- teknologi, at Guardtime har valgt at stille deres service og teknologi gratis til rådighed for den estiske regering. De har altså ikke stået med et sikkerhedsproblem, men har takket ja til en løsning, der blev tilbudt. Guardtime sælger ikke udviklertimer og integrationsværktøjerne er open source. Så det store arbejde med den konkrete integration og implementering af blockchain-systemet har hvilet på sundhedsmyndighederne, der imidlertid ikke er i tvivl om værdien.

Tillid er omdrejningspunktet for vores arbejde og hvis vi kan tilføje nogle ekstra lag, så er det typisk anstrengelserne værd.

Samtidig fremgår det, når vi spørger ind, at sundhedsmyndighedernes it-sikkerhedsteam mener, at der kunne have været alternative teknologiske løsninger og setups, der kunne have sikret dataintegritet, men at den nuværende løsning fungerer efter hensigten. Myndighederne udelukker ikke, at de i fremtiden skaber andre implementeringer.

I øjeblikket er de nysgerrige på den såkaldte IOTA Token, som er en form for blokchain-teknologi; en virtuel valuta til mini-transaktioner knyttet til Internet of Things (IoT). De overvejer derfor en pilot med en virksomhed, der selv har haft henvendt sig. Uden at der foreligger konkrete planer på nuværende tidspunkt, retter ideerne sig mod - i en fremtidig løsning - at flytte sundhedsdata i international kommunikation med naboer.

Opmærksomhedspunkter i implementeringen

Tilliden mellem parterne er der i forvejen

Denne løsning bygger på tillid mellem parterne i netværket, ligesom modellen antager, at borgere og sundhedsprofessionelle har tillid til systemet. Det er ikke slutbrugerne, der modtager en signatur, hver gang de opdaterer oplysninger i patientjournalen. I dette set-up styrer de centrale autoriteter data, dataintegriteten og de ekstra sikkerhedslag. Dette gør de på vegne af brugerne; borgere og de omkring 18.000 sundhedsprofessionelle – der har tillid til det centrale system, og det er myndighederne, der iværksætter tiltag, der kan beskytte de personfølsomme data mod interne og eksterne trusler.

Nøgleord
Persondata
Dataintegritet Sporbarhed
Centraliseret tillid
Systemintegration

Blockchainens sikring af dataintegritet er ikke en sikring mod fejl i data

Blockchainen er et ekstra lag sikkerhed, der hovedsageligt sikrer integriteten af data. Løsningen giver dermed en høj grad af immutabilitet og sporbarhed for de data, der ligger på blockchainen.
Det er imidlertid vigtigt at være opmærksom på, at blockchain ikke sikrer, at der ikke kan være fejl i de data, der registreres og dermed ikke en garanti for, at det er de korrekte data, der lægges på blockchainen.

Ja, hvis der er en fejl, distribueres den over hele systemet. Brugen af data afslører denne slags fejl, der kan opstå, når data opdateres. Så er det muligt at ændre det. Det kan gøres nemt, men du skal vide, at der er en fejl.

Case 3: Tracking af containere

Digitalisering af global handel

I et større europæisk forskningsprojekt om ineffektivitet i den globale handel har Mærsk identificeret administration og dokumentation i forbindelse med containerfragt som et område med potentiale for effektivisering og store besparelser via digitalisering.

International

Blockchain type
Hyperledger Fabric

Modenhed
Pilot

Siden har Mærsk i samarbejde med IBM startet et projekt med dette formål ved navn *Global Trade Digitization* (GTD). Som en komponent i GTD er systemet *Paperless Trade,* der skal digitalisere håndteringen af dokumenter af juridisk karakter, såsom kontrakter og tilladelser i forbindelse med den globale containerfragt. Målet er at erstatte den nuværende langsommelige og ugennemsigtig manuelle håndtering af disse dokumenter med en mere transparent, effektiv og sikker håndtering via blockchain. Ambitionen er et globalt system, der ikke kun skal anvendes og drives af Mærsk, men af hele netværket omkring shippingindustrien. Overordnet vurderes det, at administrationen forbundet med containerfragt udgør omkring 20% af den samlede udgift; med andre ord: mere end det dobbelte af selve den fysiske transport. Der er altså mulighed for store besparelser, og Mærsk vurderer at branchen vil kunne spare op til 27 milliarder.

Før havde man måske en fyr på en scooter, der fysisk transporterede et stykke papir mellem tre kontorer for at få det underskrevet og godkendt. Eller man var nødt til at sende dokumentet foran med fly for at kunne håndtere processen omkring import. Der var måske omkring 30 dokumenter involveret, og de faktiske shippingudgifter oversteg transportudgifterne. Så dette blev identificeret som en væsentlig barriere, hvor der var mulighed for store besparelser.

FØR

Fra manuel håndtering

Den internationale containerfragt er et ekstremt kompliceret system med mange aktører og varer, der skifter hænder mange steder undervejs. Til denne fragt knytter der sig et meget stort antal juridiske dokumenter, såsom kontrakter med kunder og underleverandører og ikke mindst dokumentation og tilladelser overfor de lokale myndigheder i forbindelse med import/eksport, told osv. I det nuværende system er disse dokumenter typisk fysiske papirer, der håndteres manuelt. Det betyder, at det ofte kan være nødvendigt fysisk at tranportere dokumenter til flere forskellige kontorer i et afsenderland for at indhente underskrifter, hvorefter disse dokumenter fragtes med fly til modtagerlandet til brug for importprocessen. Processen er i dag fuldstændig uigennemsigtig for de involverede parter. Derfor er man nødt til at tage direkte kontakt til fx lokale myndigheder, hvis man ønsker at få en status for fragten af en given container.

Man får en masse information ved at ringe eller sende e-mails. Der er rigtig mange af de involverede, som gerne ville vide mere om, hvad der foregår, men det er alt for besværligt. Så digitalisering ville også reducere den administrative byrde.

EFTER

Til digitalisering via blockchain

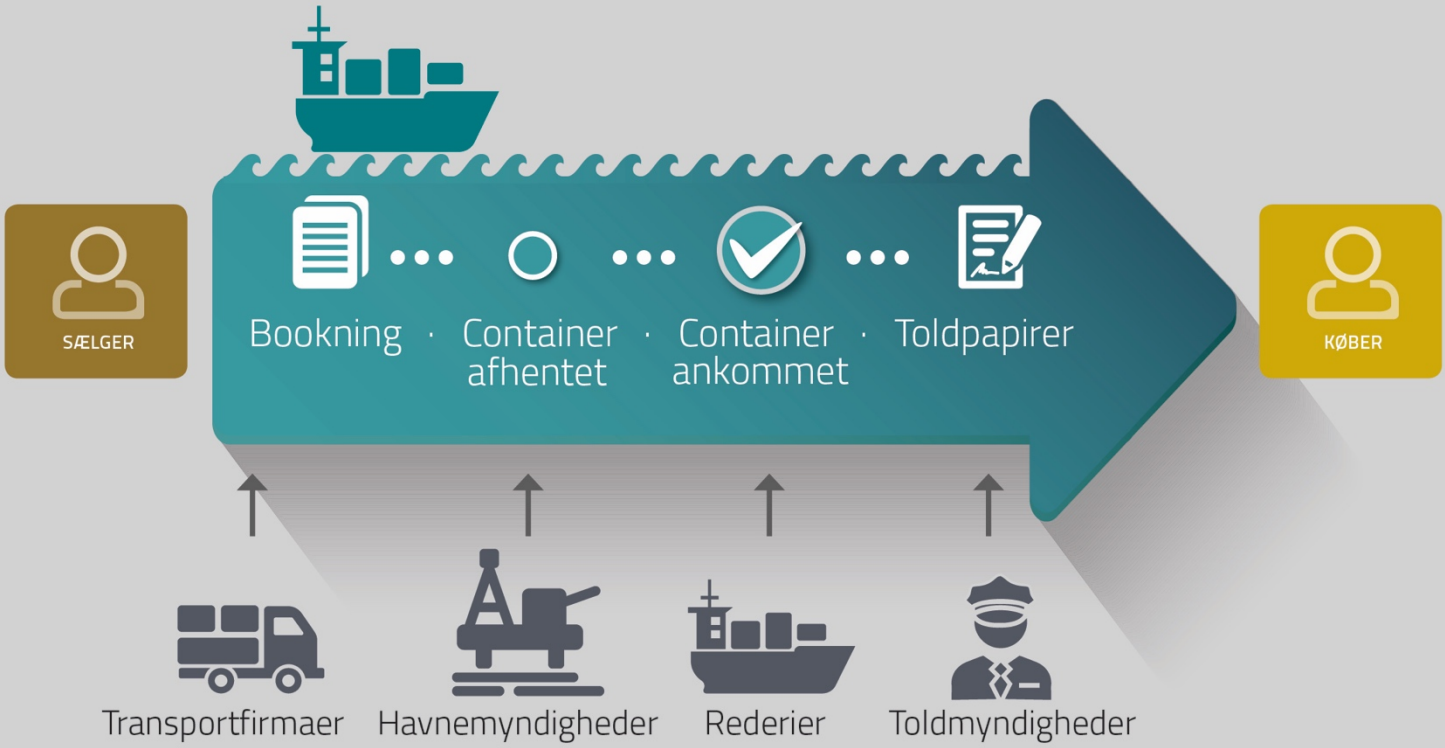
Formålet i *Paperless Trade*-systemet er, som navnet antyder, fuldkommen at digitalisere håndteringen af disse dokumenter. Systemet skal således fungere som et system, der anvendes på tværs af alle aktører i forbindelse med containerfragten. Skal der fx indhentes tilladelser i forbindelse med fragt, vil de nødvendige dokumenter kunne uploades i et digitalt system, hvor de straks gøres tilgængelige for de relevante myndigheder. Når dokumenterne er blevet godkendt, vil det så være muligt via *Paperless Trade* at underskrive og udstede de påkrævede tilladelser digitalt. Den afgivne tilladelse vil ligeledes være tilgængelig i systemet, så snart den er givet. På den måde vil arbejdet med disse dokumenter kunne gøres langt mere effektivt, da alle relevante parter vil have de informationer, de skal bruge, så snart de er klar, uden fysisk at skulle transportere dokumenter fra en part til en anden.

Når fragtdokumenterne er uploadet af shipperen, så har du en digital version, som er verificeret og sikret i blockchainen, og den overføres mellem alle de involverede parter gennem fragtprocessen – til underskrift.

I *Paperless Trade* vil der samtidig skabes en fælles log over alle dokumenter, der lægges i systemet, hvornår og af hvem, og loggen vil være tilgængelig for alle parter. Denne gennemsigtighed håber Mærsk også vil kunne hjælpe med at afgøre eventuelle tvister eller svindelsager, der kan opstå i det komplekse fragtsystem. Afleveres en container fx for sent, eller opdages der svindel med tolddokumenter, vil man ved at følge loggen let kunne spore, hvor i processen noget er gået galt og finde den skyldige part. Systemet fungerer på den måde som en såkaldt *Single Source of Truth*.

Systemet kører i dag som et pilotprojekt med flere af de aktører, der vil være at finde i det endelige system. Foruden Mærsk er der konkret tale om fire *shipper*s (dvs. kunden der skal have fragtet gods), tre speditører, to toldmyndigheder og tre havne. I pilotprojektet kører systemet som en skyggeproces. Dvs. at den gamle manuelle proces stadig udføres som hidtil, men ved siden af kører man *Paperless Trade*-systemet, hvor de fysiske dokumenter digitaliseres og lægges ind i systemet, og toldmyndighederne har mulighed for at udstede godkendelser. Skyggeprocessen er nødvendig, da det vil kræve store ændringer i bl.a. det regulative system i de forskellige lande fuldt at erstatte de gamle dokumenter og processer med *Paperless Trade*-systemet. Disse ændringer er Mærsk ikke i stand at gennemføre alene. Så ud over det tekniske system ligger der også et stort arbejde for projektet i at overbevise myndighederne i de forskellige lande om, at systemet skal tages i brug. Bl.a. derfor er det essentielt for projektets succes at få så mange parter inden for branchen som muligt med på systemet, så det ikke fremstår som et rent Mærsk-projekt.

Den nye løsning



Hvordan indgår blockchain i løsningen?

Paperless Trade-systemet benytter blockchain-teknologi til at lagre de forskellige dokumenter, der uploades til systemet på en måde, der ligner flere af de øvrige cases (eksempelvis New Banking). I blockchain-systemet lægges der hashes af dokumenterne, mens de faktiske dokumenter lægges i en sideløbende krypteret decentral database. Dette giver systemet mulighed for at styre adgangen til dokumenterne, så det kun er de parter, der har en berettiget brug af dokumenterne, der kan læse dem. Præcis hvilke parter der skal have adgang til hvilke dokumenter er endnu ikke fastlagt. Men man kan fx forestille sig, at den enkelte *shipper* kun kan læse dokumenter omhandlende hendes egen fragt, hvorimod toldmyndighederne kan have brug for at læse dokumenter fra mange forskellige *shippers.*

Systemet bygger på blockchain-platformen Hyperledger Fabric, der er et lukket (*permissioned*) blockchain-system. Dvs. at de deltagere, der driver systemet først er blevet identificeret og autoriseret til at deltage i systemet. I det endelige system forestiller man sig, at de store spillere i branchen, dvs. de større fragtselskaber, myndigheder osv., deltager i blockchain-netværket, dvs. at de har en direkte tilkobling til blockchainen og deltager i at vedligeholde den. Mindre aktører, såsom små lokale fragtmænd, der måske ikke har de nødvendige ressourcer og kompetencer til at drifte netværket, vil via en eller flere af de større aktører også kunne få adgang til data på blockchainen.

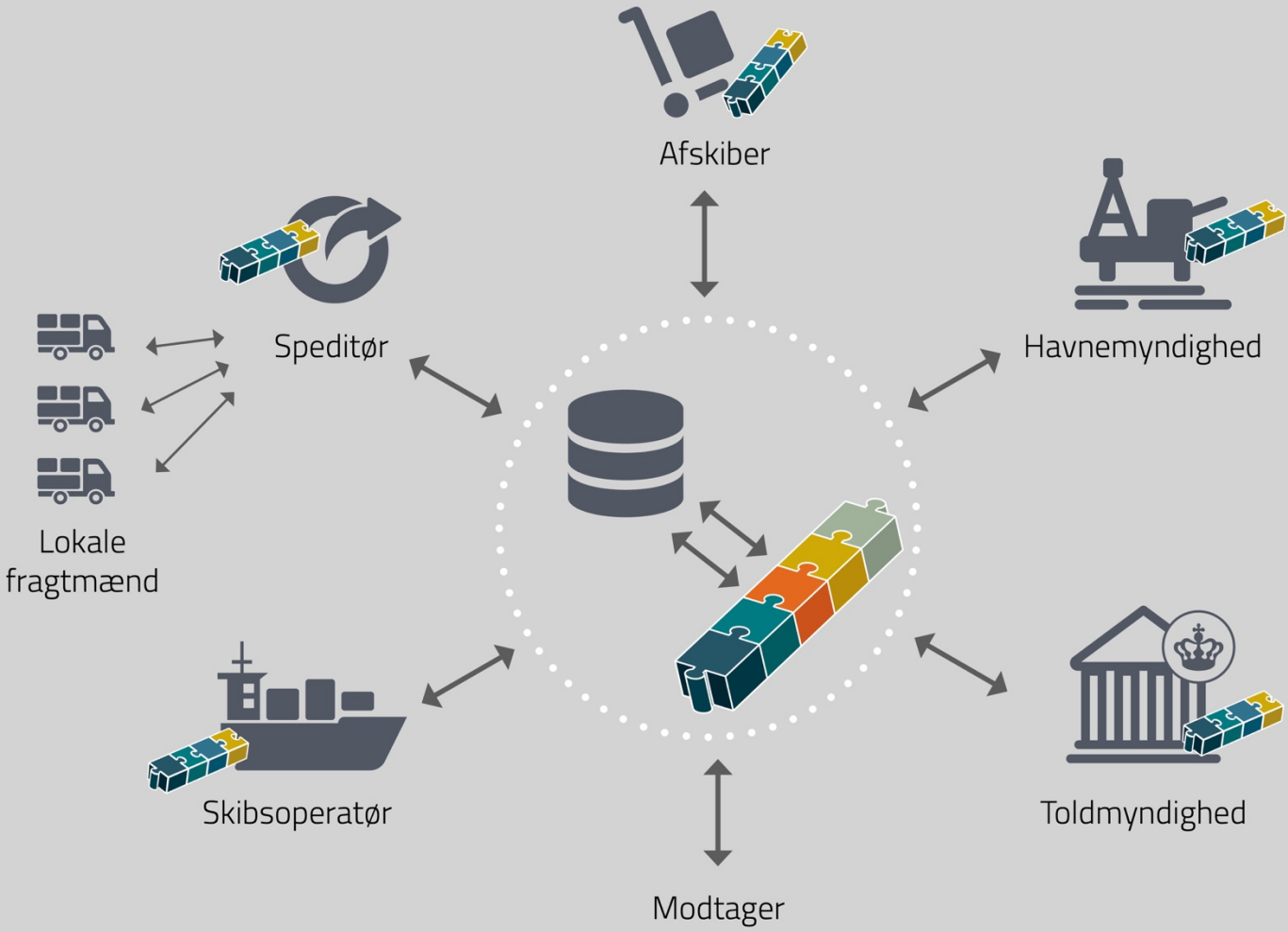
Hvorfor en blockchain?

Den primære besparelse i *Paperless Trade*-systemet kommer via den effektivitet, hvormed dokumenterne kan håndteres og distribueres imellem de involverede parter. Blockchain understøtter netop dette, idet data automatisk distribueres blandt deltagerne i systemet. Samtidig giver den konsensus der opnås omkring data i et blockchain-system, sammen med den høje dataintegritet og sporbarhed, en *Single Source of Truth,* der gør det muligt at løse eventuelle tvister imellem parter og forebygge svindel.

Der er klart lande, hvor dokumenter bliver forfalsket. Dette vil ikke stoppe nogen i at forfalske dokumenter, inden de lægges i blockchainen, men hvis dokumentet er uploadet, så kan man spore nøjagtigt, hvor dokumentet kom fra. Så det giver noget i forhold til ansvarspådragelse.

Om systemet reelt kan komme i anvendelse er desuden i høj grad afhængigt af, om der opstår en kritisk masse omkring det. Dvs. det er nødvendigt, at en stor del af de mange aktører omkring den globale shippingindustri går med til at benytte systemet, ikke mindst de lokale myndigheder. Da mange af disse aktører vil have modstridende interesser (fx i kraft af at være konkurrenter eller leverandører til hinanden), vil det være svært at skabe opbakning til systemet, hvis det var baseret på tillid til Mærsk alene, og en anden betroet part er heller ikke oplagt. Blockchain løser dette problem ved at distribuere tillid over det samlede netværk af deltagere, i stedet for at bero på tillid til en eller flere specifikke parter.

Blockchainens funktion



Blockchainen bruges i dette projekt til at sikre dataintegritet og styre adgangen til data. Data ligger i en decentral database, som bliver hostet af Mærsk og IBM i fællesskab. Blockchainen sikrer integritet, ved at kopier af blockchainen ligger hos toldmyndighederne og de store spillere i branchen. Som noget særligt arbejder man i dette projekt med flere tilknytningsgrader til blockchainen. Det er ikke alle aktører, der kommer til at skulle have en kopi af blockchainen liggende. Mindre aktører får adgang til informationen gennem det overordnede system – Global Trade Digitization.

Opmærksomhedspunkter i implementeringen af blockchain

Nøgleord
Distribueret tillid
Lovgivning
Åbent software
Kontrol

De største udfordringer ligger uden for det tekniske
Som beskrevet ovenfor er der et meget stort antal aktører, der vil skulle kobles på *Paperless Trade*-systemet. I dag har disse deres egne forskellige interne systemer og processer til at håndtere dokumenter. Det har resulteret i et stort arbejde med at integrere *Paperless Trade* i miljøet hos hver af de mange forskellige aktører. En særlig udfordring er, at der i flere lande vil være brug for at ændre i lovgivningen, for at et system som *Paperless Trade* kan blive tilladt og anvendt af myndighederne. Mærsk vurderer, at de største udfordringer i forbindelse med den videre implementering af systemet vil være problemstillinger, der ikke har noget at gøre med det tekniske omkring blockchain, men snarere det organisatoriske ved at samle en stor gruppe aktører omkring et globalt system.

Bevarelse af den distribuerede tillid
Mærsk vurderer desuden, at den distribuerede tillid er vigtig for at skabe bred tilslutning til systemet inden for branchen. I den sammenhæng er det essentielt, at der ikke ad omveje skabes punkter, hvor tilliden alligevel samler sig hos en enkel part. Det kunne fx være at lade løsningen afhænge af software, der kun kan anskaffes fra en enkelt leverandør, eller ved lade en enkelt part stå for at tildele adgang til systemet for de øvrige parter. På den måde vil man få samlet uforholdsmæssigt meget magt over systemet hos nogle centrale parter. For at undgå dette har Mærsk stort fokus på, at systemet skal bero sig på åbne standarder, og at rettigheder i systemet skal kunne tildeles via konsensus i netværket.

Case 4: Registrering af ejerskab

Mere effektiv handel med ejendomme

I Sverige har Lantmäteriet, der håndterer landmåling og ejendomme, arbejdet på et projekt med Telia, SBAB, Landshypotek Bank, ChromaWay and Kairos Future for at effektivisere hele processen, der finder sted i forbindelse med køb og salg af jord og ejendomme.

FØR

Fra langsom og uigennemsigtig

Når en aftale om en ejendomshandel bliver underskrevet i Sverige i dag, tager det typisk tre til seks måneder, før det bliver meddelt til Lantmäteriet, der skal lave den endelige registrering af overdragelse af ejerskab og pantebreve, før overdragelsen af ejerskabet er gennemført. Det medfører komplikationer for de mange involverede parter i en ejendomshandel, fx for sælger, køber, banker og ejendomsmæglere, der ikke har nem adgang til alle dokumenter, før de bliver offentligt tilgængelige hos Lantmäteriet. Derfor har de forskellige parter indtil videre brugt deres egne løsninger til at opbevare og dele dokumenter. Derudover er dele af processen omkring overdragelse og handel af ejendomme i dag ikke digital.

EFTER

Til hurtig og transparent proces

Den foreslåede løsning vil digitalisere hele processen omkring en ejendomshandel, og hele processen vil blive drevet af Lantmäteriet, så detaljerne om en handel vil være offentligt tilgængelige med det samme en købsaftale er underskrevet. Forskellige brugergrænseflader bliver tilpasset tre kategorier af brugere af systemet. På denne måde skabes forskellige adgange til systemet, hvor hashes af alle dokumenter vil være tilgængelige via en blockchain. Mens købere og sælgere får adgang via en særligt udviklet og nemt tilgængelig app, hvor de kan følge alle dele af processen og kan se, hvornår de selv skal gøre noget aktivt, fx underskrive dokumenter, får de såkaldt professionelle brugere og administrative brugere en adgang, hvor det vil være muligt for alle de involverede parter at tjekke, at processen kører i den rigtige rækkefølge, og at alle dokumenter og underskrifter bliver færdiggjort til tiden.

LANTMÄTERIET

ChromaWay

KAIROS FUTURE

Landshypotek Bank

SBAB!

Telia

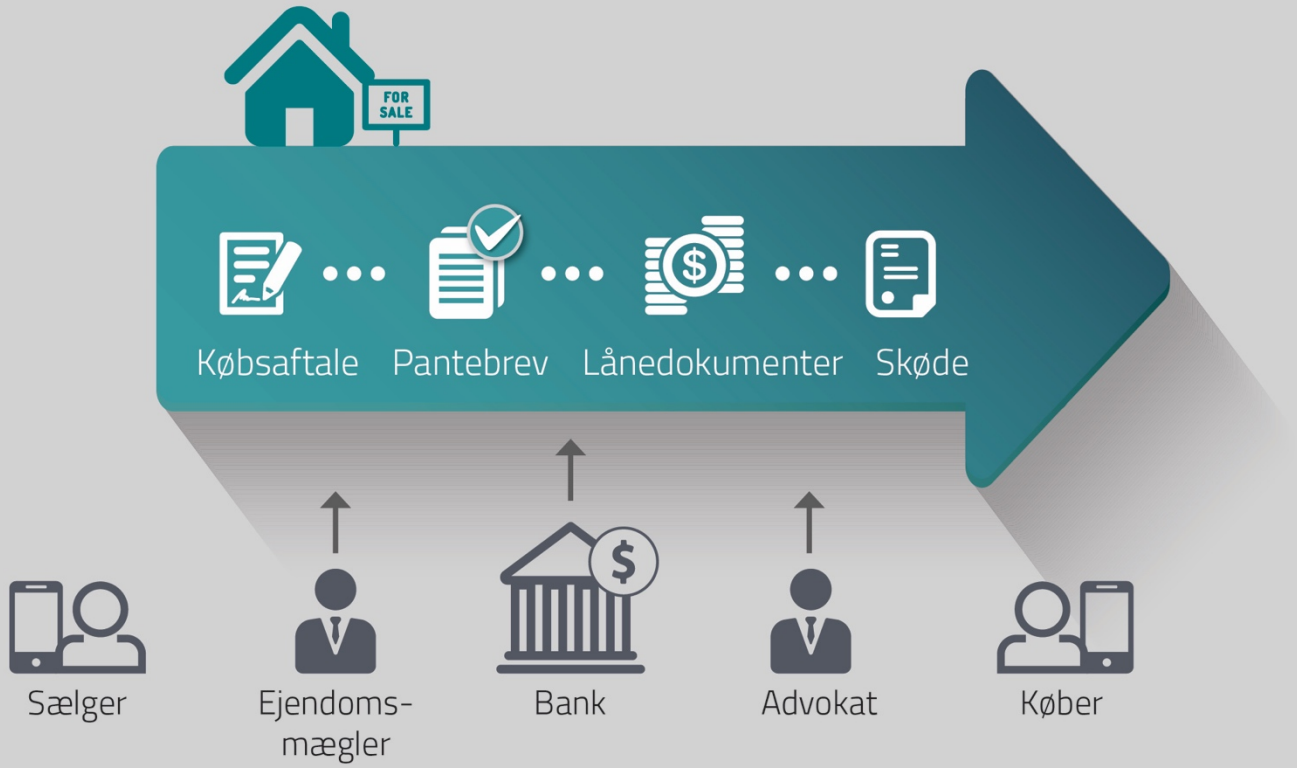
Sverige

Blockchain type
Postchain (lukket)

Organisation Type
Offentlig myndighed

Det vurderes, at de effektiviseringer som den nye løsning vil føre med sig vil være mere en 100 millioner euro værd for det svenske samfund.

Den nye løsning



Hvordan indgår blockchain i løsningen?

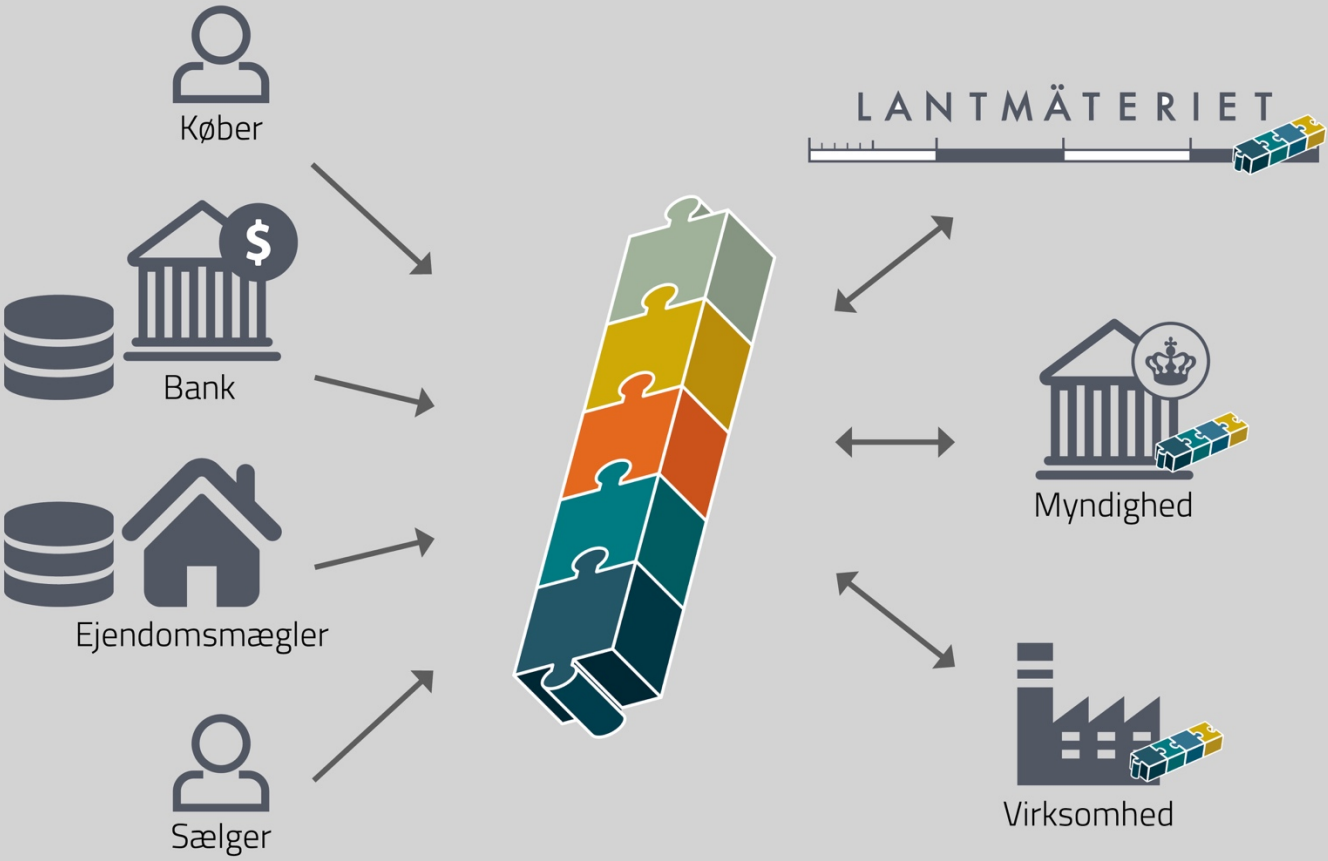
Målet med løsningen er ikke, at retten til ejendomme skal ligge på en blockchain, der derefter kan handles og overdrages mellem parter som fx det sker med Bitcoins. Derimod er det hashes af dokumenter og underskrifter, der laves i forbindelse med handel med ejendomme, der gemmes i en blockchain, således at alle aktører nemt kan holde øje med, hvilke dokumenter og underskrifter, der er registreret, og verificere ægtheden af digitale dokumenter, de modtager, ved at sammenligne med de hashes, der er på blockchainen. Selve dokumenterne og underskrifterne skal gemmes lokalt hos de enkelte aktører eller hos en fælles cloud-udbyder. Selve blockchainen skal drives af Lantmäteriet og nogle andre, indtil videre unavngivne, offentlige myndigheder og private firmaer, der dermed kommer til at stå for validering af, hvilke data der må komme på blockchainen.

Løsningen gør det muligt at uploade smarte kontrakter til blockchainen, der kan automatisere dele af handelsprocessen og sikre transparens, idet alle parter kan se indholdet af den smarte kontrakt. Fx foreslås det, at processen omkring overdragelse af et pantebrev kan skrives ind i en smart kontrakt, så overdragelsen er betinget af, at den tilhørende ejendomshandel er korrekt gennemført, og at køberen har betalt de rigtige afgifter til Lantmäteriet.

Hvorfor en blockchain?

Blockchainen sikrer i denne løsning *dataintegritet* og *transparens*: Blockchainen indeholder hashes af signaturer, dokumenter o.l. og er offentligt tilgængelig for de parter, der skal kunne se disse. Det sikrer transparens igennem en bolighandel, idet alle handlens parter kan verificere de dokumenter, de modtager, og holde øje med, hvornår og i hvilken rækkefølge dokumenter bliver underskrevet. Nogle få firmaer og myndigheder, bl.a. Lantmäteriet, kan tilføje data til blockchainen og validere dens indhold, men da den er distribueret blandt flere parter, kan én part ikke manipulere med blockchainens indhold, hvilket sikrer integritet, idet en part ikke uden videre kan manipulere med data.

Blockchainens funktion



Blockchainen fungerer i dette projekt som sikring af transparens og dataintegritet på tværs af de mange parter der er involveret i en ejendomshandel. Data vil ligge i decentrale databaser hos de forskellige dataejere eller hos en fælles cloud udbyder. Selve blockchainen drives af Läntmateriet og dataintegriteten sikres ved at et netværk af betroede virksomheder og myndigheder indgår som parter i blockchainen.

Opmærksomhedspunkter i implementeringen af blockchain

Nøgleord
Dataintegritet
Distribueret tillid
Transparens
Effektivisering

Tilslutning til fælles løsning gennem distribution og transparens
Det er en udfordring at få de mange parter omkring en ejendomshandel med i en fælles transparent løsning. Der er ingen oplagt betroet part, der kan centralisere processen omkring salget, der i dag er tung og langsommelig. De mange involverede parter i ejendomshandler, dvs. sælger, køber, sælgers bank, købers bank, ejendomsmæglere og advokater har derfor alle konstrueret deres egne løsninger. Lantmäteriet går nu foran i processen som central myndighed, men ved at bruge blockchain undgås en centraliseret løsning. Alle parter behøver ikke at stole fuldstændig på Lantmäteriet ift. at opbevare deres dokumenter. I stedet for at Lantmäteriet opbevarer alle dokumenter for alle parter, opbevares kun verifikationer af ændringer og underskrifter, som alle parter kan validere mod dokumenter, de selv opbevarer. Det sikrer tillid parterne imellem og transparens i hele processen.

Blockchain i forhold til EU's nye Persondataforordning
Det vurderes ikke, at den nye løsning vil blive vurderet anderledes i forhold til EU's Persondataforordning (GDPR) end den eksisterende løsning. Det kan være svært at slette data på en blockchain, hvilket kan være i konflikt med retten til at blive glemt, men da det kun er hashes, der opbevares på blockchainen, vil det i højere grad være der, hvor selve dokumenterne gemmes decentralt, at det vil være et problem, og ikke på selve blockchainen.

Case 5: Balancering af el-nettet

Balancering af et stadigt mere komplekst el-net

I et el-net hvor en stor del af strømmen produceres af vedvarende energikilder er det et problem at balancere produktionen, så den passer med forbruget, idet man ikke, som det fx er tilfældet med kraftværker, har kontrol over, hvor meget strøm der bliver produceret. Det forsøger den hollandske el-netudbyder TenneT at løse i et digitaliseringsprojekt, hvor de arbejder med såkaldt *crowd balancing*. Her udnytter de allerede eksisterende batterianlæg hos almindelige el-forbrugere til at opbevare overskudsstrøm. TenneT er som Energinet i Danmark en statsejet Transmission System Operator (TSO).

I dag bruges der store ressourcer på at kontrollere energiproduktionen, så den stemmer overens med el-nettets kapacitet. Fx blev der i Tyskland i 2016 brugt 800 millioner euro på at begrænse vindmøllers el-produktion. Så der er mange penge at hente ved en bedre balancering af nettet, hvis det kan betyde, at sådanne begrænsninger bliver mindre nødvendige. Det er derfor TenneT's håb, at deres løsning vil kunne begrænse de prisstigninger på el, de forventer kommer som følge af en overgang til et el-net, hvor en stor del af strømmen produceres af vedvarende energikilder.

Holland/Tyskland

Blockchain Type
Hyperledger Fabric (Lukket)

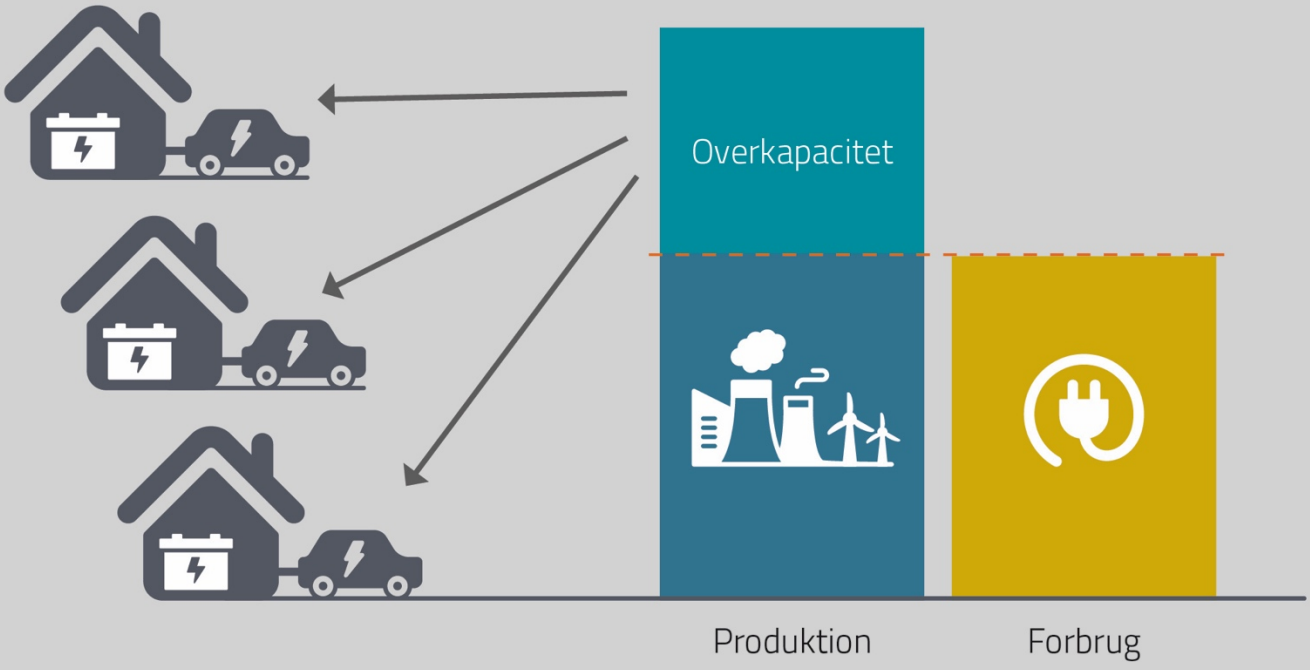
Modenhed
Pilotprojekt

Løsningen testes i øjeblikket i to pilotprojekter: Et med det tyske firma Sonnen eServices, der leverer batteriløsninger til solcellesystemer, og et andet med det hollandske firma Vandebron, der bl.a. repræsenterer en stor gruppe el-bilejere. I begge tilfælde skal batterierne til solcellesystemerne og i elbilerne indgå i balancering af el-nettet ved at lade op, når der bliver produceret for meget strøm, og aflade, når der produceres for lidt. Ejerne af batterierne får til gengæld en økonomisk kompensation for at sætte deres batterier til rådighed. Pilotprojekterne løber i cirka et halvt år indtil sommeren 2018 og involverer nogle hundrede aktører.

Hvordan indgår blockchain i løsningen?

De tekniske detaljer omkring løsningen er ikke tilgængelige, før pilotprojekterne er færdige, men det er offentligt, at blockchainen indgår som en del af en større digitaliseringsproces, og at det er Hyperledger Fabric, der bliver brugt som blockchain-teknologi.

Den nye løsning



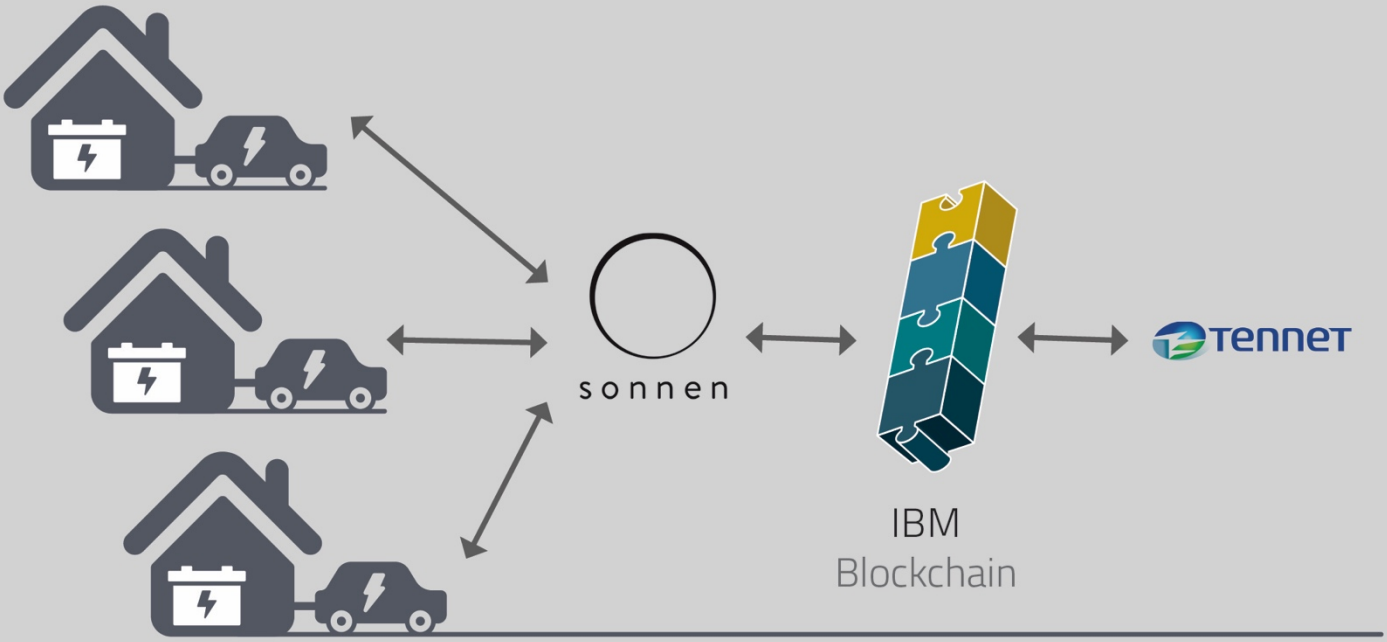
Blockchainen fungerer som en markedsplads for batterikapacitet. Ejerne af batterianlæg eller el-biler kan sætte kapacitet til salg sammen med betingelser for salget, fx hvor meget kapacitet der er, hvornår det kan udnyttes, og hvad prisen er. Det gøres i form af en såkaldt *smart kontrakt*, som TenneT kan aktivere, hvis de vurderer, at det er nødvendigt at udnytte batterikapaciteten hos nogle batteriejere. I praksis er det Sonnen eller Vandebron, der laver kontrakterne på vegne af deres kunder. Det bliver gemt på blockchainen, hvor meget kapacitet TenneT har brugt og hvornår, så batteriejerne kan aflæse det og kan få den rette betaling.

Hvorfor en blockchain?

I løsningen indgår blockchain-teknologi'en Hyperledger Fabric, der er en teknologi til at lave private blockchains, og IBM er leverandør af den nødvendige software. En privat blockchain er valgt af TenneT på grund af de lave transaktionsomkostninger sammenlignet med offentlige åbne blockchains som fx Bitcoin. Ydermere ønsker TenneT ikke at stå som en central aggregator i løsningen, som de ønsker skal være så decentral som mulig. TenneT ser ikke løsningen som værende *peer-to-peer*, hvilket vil sige en decentral løsning, hvor udveksling af værdi sker direkte fra bruger til bruger uden et centralt mellemled. Forskellige aktører har netop forskellige roller på netværket, men de forestiller sig, at andre blockchains, der netop fungerer som peer-to-peer, kan indgå som en del af netværket.

Da alle oplysninger om hvor meget batterikapacitet der bliver benyttet hos hvilke batteriejere bliver gemt på blockchainen, og dermed er tilgængelige for alle parter, er der en forventning om, at det vil være fleksibelt og nemt at afregne med batteriejerne og at afgøre eventuelle tvister.

Blockchainens funktion



Blockchainen bruges i dette projekt som markedsplads for køb og salg af batterikapacitet. Blockchainen sikrer transparens og dataintegritet i samspillet mellem energiselskab og de private batteriejere. Data ligger direkte på blockchainen og er tilgængelig for alle parter. Som noget særligt har man valgt at håndtere den faktiske salgstransaktion i Blockchainen. Dette gøres gennem en smart kontrakt, som energiselskabet kan aktivere, når det ønsker at købe ekstra batterikapacitet.

Opmærksomhedspunkter i implementeringen af blockchain

Nøgleord
Systemintegration
Transaktion af værdi
Standardisering
Nye roller
Transition af el-nettet

Løsningen skal integreres med de eksisterende systemer
El-nettet er allerede i dag i høj grad digitaliseret, og de apparater der allerede nu er en del af det komplekse netværk af decentrale systemer skal kunne interagere med løsningen. Det har fra TenneT's side krævet en del arbejde og udviklertimer at lave en sådan integration til det eksisterende system og energinet.

Behov for skalering og udvikling af standarder
TenneT håber, at deres løsning kan blive en standard for energisektoren til at skabe større fleksibilitet og løse balanceringen af el-nettet. De skal dog først teste, om løsningen skalerer så godt, som de håber, den vil. For hvis det skal bruges i stor skala, vil det være mange tusinde eller millioner brugere, der kommer til at indgå i løsningen. Behovet for udvikling af tekniske standarder har også meldt sig, da løsningen kommer til at indgå i et større system, som den skal kunne fungere i.

Særlige potentialer

Når vi ser på tværs af de fem cases, er der en række potentialer, der træder frem som særlige i de konkrete anvendelser. Det er dog forskelligt, hvordan potentialerne udfolder sig og for hvem. Det er vigtigt at bemærke, at vi tager perspektivet *indefra.* Det vil sige, at vi følger projektejernes egne definitioner og beskrivelser af blockchain i deres løsning. Det ligger således ikke inden for denne rapport at bedømme, hvorvidt en implementering er blockchain eller ej. Det er vigtigt pointere at potentialerne er meget kontekstafhængige og i høj grad præget af at alle casene er det man kalder lukkede blockchains. En vurdering af potentialerne ved anvendelsen af blockchain i den offentlige digitale infrastruktur vil derfor afhænge af en konkret analyse af anvendelsesområdet.

Effektivisering

Et tema, der træder frem som et potentiale på tværs af flere cases, er effektivisering. Det forhold at blockchain-løsningen giver mange forskellige parter *overblik* over en transaktionsproces forventes at give en hurtigere og mere effektiv proces. Mens effektivisering i casen om validering af persondata (case 1) handler om et skift fra manuel håndtering til fuldautomatisk verificering, handler effektiviseringen i andre cases om det, der må betegnes som reelle digitaliseringsprojekter. Her spiller blockchain-teknologien en rolle i samspil med en udvikling, der handler om digitalisering. I casene om tracking af containere (case 3) og registrering af ejerskab (case 4) ligger der i dag – særligt i forbindelse med containerfragt – tunge arbejdsprocesser med store mængder analoge dokumenter og ressourcekrævende manuel håndtering af sagsgange. Når parterne i de to cases vurderer, at den økonomiske værdi er høj, er det derfor vigtigt at huske på, at det i høj grad også er selve digitaliseringen, der giver en stor del af gevinsten. Det er således tydeligt, at blockchain ikke gør det alene – i cases som disse udgør teknologien et element i en større digitaliseringsøvelse.

Effektiviseringspotentialerne ligger således i høj grad i aspekter af digitalisering så som automatisering, bedre transparens og hurtigere udveksling af oplysning mellem parter i processer. I nogle tilfælde kan blockchain dog være en afgørende komponent idet teknologien giver mulighed for at digitalisere processer og systemer, hvor mange parter er involveret, men hvor ingen af disse oplagt kan fungere som en betroet part. I hvor høj grad dette er relevant i offentlige digitaliseringsprojekter vil afhænge af den konkrete situation.

Dataintegritet

I hovedparten af casene spiller blockchain-teknologiens særlige egenskaber i forhold til at sikre dataintegritet en afgørende rolle. Forsøg på at hacke systemet eller manipulere data vil i et distribueret system skulle rette sig mod alle kopierne af blockchainen, der ligger hos parterne i netværket. Selvom der kan være fejl, nedbrud og forsøg på hacking i systemet, har blockchain en stor 'resistens' over for uautoriserede ændringer, fordi parterne i systemet hurtigt vil kunne spotte uautoriserede forsøg på ændringer.

Dataintegritet sikres i mange af casene netop ved, at hashes af databasen er distribueret enten hos udvalgte aktører eller blandt alle parterne i netværket. Det gør sig gældende i casen, der handler om at beskytte bankkunders persondata (case 1). Her vil banker indgå i netværket sammen med en autoritet, der forventes at indgå som en ekstra kontrolinstans for at sikre, at der ikke ændres i blockchainen. Noget tilsvarende gør sig gældende i forhold til registrering af ejerskab (case 4), hvor blockchainen – ud over at ligge hos Läntmateriet, der driver blockchainen – er distribueret i et netværk af betroede virksomheder og myndigheder. Distributionen af blockchainen indgår også som et vigtigt element i casen, der handler om tracking af containere i global handel (case 3), hvor ambitionen netop er at sikre dataintegritet, ved at kopier af blockchainen ligger hos toldmyndighederne og de store spillere i branchen.

Dataintegritet i den elektroniske patientjournal i Estland (case 2) skiller sig ud fra den distribuerede model i de øvrige eksempler. I den estiske løsning er der ikke noget netværk af aktører omkring selve blockchainen. Her fungerer den udelukkende som en ekstern kontrolinstans i forhold til myndighederne og er særligt med til at sikre, at der ikke manipuleres med data.

De seneste år er cybersikkerhed kommet stadig højere på dagsordenen, også i forhold til den offentlige digitale infrastruktur. I situationer, hvor det vurderes, at der kan være aktører der kunne have interesse i at manipulere med data, kan blockchain i kraft af den øgede dataintegritet teknologien understøtter, være en komponent i en sikring mod dette. Som det er tilfældet i én af casene, kan dette også gøres som et ekstra lag ovenpå et eksisterende ikke-blockchain-baseret system.

Sporbarhed

Sammen med dataintegritet er sporbarhed et nøgleelement, der træder frem i alle fem cases. Udsagn der går igen, når projektejerne forklarer, hvad der gør blockchain-løsningen særlig i forhold til sporbarhed, er, at transaktioner tidsstemples, og transaktionshistorikken kan følges tilbage. I denne optik sikrer løsningerne provenance og transparens for parterne i netværket.

I casen om validering af persondata (case 1) er det netop muligheden for at sikre provenance (oprindelse) med den indbyggede beviselighed, der er den væsentligste årsag til implementering af blockchain. I en række cases handler sporbarhed om, at mange forskellige parter får overblik over en transaktionsproces, hvor der er en indbyrdes afhængighed mellem parterne. I tracking af containere på tværs af lande (case 3) og i registrering af ejerskab (case 4) vil løsningen gøre processen transparent for de involverede parter. Parterne udgør hver især en form for informations-ø, og de vil blive bundet sammen i en blockchain-løsning, så et fællesskab af aktører kan få overblik. Sporbarhed træder også frem som nøgleelement i casen om beskyttelse af persondata (case 2) og leverer her et vidnesbyrd om provenance. Her er det ikke et netværk af mange aktører, der få et overblik. Her er det myndighederne, der har mulighed for at spore ændringer, da der for hver ændring er registeret tidspunkt og hvem, der har lavet opdateringen. Projektejere fremhæver endvidere sporbarhed som værdifuldt, hvis noget går galt mellem parterne i en transaktionsproces. Eftersom blockchain-systemet fungerer som en såkaldt 'single source of truth', vil det eksempelvis kunne bruges til at afgøre eventuelle tvister og svindelsager (fx case 3 og case 5).

Blockchain giver en meget stærk transparens, en egenskab der umiddelbart kan virke uønsket, hvis de data der indgår i systemet er følsomme, fx forretningsfølsomt data eller persondata. Det er dog muligt at bruge

blockchain alligevel og få værdi ved at gøre det. Selve dataene kan være gemt i en beskyttet database, og der kan så blot gemmes hashværdier af dataene, eller adgangsrettigheder på blockchain. På den måde er det muligt at have transparens og sporbarhed over integriteten af data, om den er blevet ændret, eller hvem der har adgang til data, mens selve dataene forbliver hemmelig. Her er det vigtigt at skelne mellem datatransparens og procestransparens.

I forhold til den offentlige digitale infrastruktur kunne muligheden for at lave systemer, der sikrer transparens, have et demokratisk potentiale, da sådanne kunne bruges til at give f.eks. borgere, journalister eller ngo'er automatisk indsigt i dele af myndigheders processer.

Nye roller – samtykke, kontrol og ejerskab

Ser man på tværs af de fem cases er det tydeligt, at aktørerne omkring blockchain-løsningerne vil få nye roller. Et potentiale der træder frem handler om ejerskab og kontrol i forhold persondata og datadeling, mens et andet potentiale knytter an til nye forretningsmodeller, hvor producent-, leverandør- og forbrugerroller er under forandring.

I en række cases forholder aktørkredsen omkring blockchain-løsningen sig eksplicit til EU's Persondataforordning (GDPR) og ser netop, at set-up'et omkring en blockchain er med til at løse udfordringen med at beskytte personfølsomme data – en opgave der i dag varetages centralt af en myndighed eller af private virksomheder. Casen omkring validering af persondata (case 1) er bemærkelsesværdig set i forhold til en række af de øvrige cases, da den giver bankkunderne ejerskab og kontrol over deres egne persondata. I løsningen vil kunden få et samlet overblik over, hvilke personlige oplysninger forskellige banker ligger inde med, og kunden kan give samtykke og inddrage adgang til data.

Casen om balancering af el-nettet (case 5) peger på potentialet i forhold til udvikling af nye forretningsmodeller, hvor kunderne indtager nye roller og et ejerskab af værdier i forhold til producenter/leverandører. I balanceringen af el-nettet afprøves blockchain som en teknologi, der kan understøtte en udvikling, hvor rollerne er under forandring, og forbrugere i stigende omfang bliver *prosumers*, dvs. de konsumerer og producerer strøm i et marked for vedvarende energi. I balanceringen af el-nettet arbejdes der specifikt med en *crowd balancing* model, og TenneT, der er en hollandsk/tysk TSO, hvilket svarer til Energinet i Danmark, nævner, at de også ser et fremtidigt marked, hvor denne model sameksisterer med *peer-to-peer*-løsninger. Det vil sige decentrale løsninger hvor udveksling af værdi sker direkte fra bruger til bruger uden et centralt mellemled. I sådanne systemer får (for)brugerne potentielt større kontrol og magt over den værdi, der udveksles – sælges og købes.

I forhold til den offentlige sektor åbner casen, der handler om validering af persondata (case 1) interessante perspektiver, da den løser problemstillingen omkring datadeling og samtykke og tilbyder en brugervenlig adgang fra forbrugerside.

Distribueret tillid

At tilliden er distribueret i et netværk er en helt central faktor. På tværs af de fleste af casene er det tydeligt, at distributionen af systemet blandt deltagerne – med den *dataintegritet* og *sporbarhed* det giver – afføder tillid mellem parterne. Samtidig virker tilliden til systemets distribuerede karakter som incitament

blandt nogle af parterne til at ville indgå i en fælles løsning. At det ikke blot er en enkelt part, der sidder med myndigheden og kontrollen over systemet, skaber tillid mellem parterne.

At tillid som faktor går igen på tværs af alle cases er ikke overraskende, da blockchain-teknologien har egenskaber, der gør det muligt at skabe en sikker, fælles transaktionshistorik i et netværk af aktører, der kan udveksle sikkert uden et enkelt centralt mellemled. Blockchain er netop derfor blevet betegnet som en slags tillidsteknologi.

Selv om teknologien åbner for store potentialer, da den kan befordre tillid mellem parter i et distribueret netværk, er det vigtigt at have for øje, at teknologien indgår i en kompleks organisatorisk kontekst. Som led i implementeringen af blockchain-løsninger er der omfattende udfordringer, der skal løses i forhold til organisering og ejerskab – hvad gør man for eksempel, hvis der opstår uenigheder, eller hvis kontrol og myndighed imod hensigten samler sig på få hænder. Analysen af de fem cases viser, at der ofte er en vis form for tillid tilstede mellem parterne i forvejen, for at der er vilje til at indgå i en fælles løsning. Samtidig rummer dette et paradoks – for har en kreds af aktører først har formået at få organiseringen og samarbejdet på plads, vil det i praksis overflødiggøre nogle af blockchains særlige teknologiske potentialer.

Centrale forudsætninger

Når man ser på tværs af de fem cases, er det tydeligt, at der er en række faktorer, der påvirker mulighederne for at indfri potentialerne ved blockchain. Det handler ikke alene om udviklingen af de teknologiske løsninger. Det handler i lige så høj grad om udviklingen af den organisatoriske og forretningsmæssige virkelighed, løsningerne skal fungere i. I vurderingen af anvendelsen af blockchain i den offentlige digitale infrastruktur er det derfor afgørende have et helhedsorienteret fokus på det tekniske og organisatoriske samspil blockchainen-løsningen skal indgå. i.

Fokus på organisering og samarbejde

Alle casene er kendetegnet ved, at løsningerne bevæger sig på tværs af forskellige juridiske enheder og med komplekse organisatoriske set-ups. Det er for så vidt ikke så overraskende, for blockchain har netop sit store potentiale i muligheden for at håndtere distribueret tillid. Derfor vil mange blockchain-løsninger også fremover være født i en kompleks organisatorisk virkelighed, og det betyder, at blockchain-løsninger typisk vil kræve ekstra fokus på organisation og samarbejde. Det er her vigtigt at understrege, at udfordringen ikke ligger i selve blockchain-teknologien, men i de muligheder teknologien giver for at etablere distribuerede løsninger.

Fælles for casene (bortset fra den estiske case) er, at man investerer rigtig meget energi i at få etableret en solid tværgående samarbejdskonstruktion. Uden den, ingen blockchain-løsning. Der ligger et stort arbejde i at få andre parter med og få skabt en løsning, der er værdifuld for alle på trods af de interessekonflikter, der naturligt måtte forekomme mellem parterne. Dette ser ud til at være en stor udfordring, uanset om man er en privat virksomhed (New Banking, Mærsk) eller en offentlig myndighed (Lantmäteriet).

Omend teknologien synes at være lidt i baggrunden i flere af casene, så fremhæves blockchain paradoksalt nok samtidig som en løftestang for at få skabt det tværgående samarbejde. Man udnytter simpelthen den hype, der er omkring blockchain, til at få skabt opmærksomhed om og interesse for projektet. Det er også en af forklaringerne på, hvorfor flere af vores cases fremhæver sig selv som blockchain-projekter, til trods for at teknologien måske kun spiller en birolle i den overordnede løsning, og det teknologiske set-up er på grænsen af, hvad man vil definere som blockchain.

Fokus på offentligt-privat samspil

I etableringen af tværgående samarbejdskonstruktioner ligger også et arbejde i at finde ud af, hvilken rolle de enkelte parter skal have i samarbejdet – og måske i særlig grad hvilken rolle offentlige myndigheder tager i denne type projekter. Et gennemgående træk i casene er udviklingen af nye samspil mellem offentlige myndigheder og private virksomheder. De offentlige myndigheder indtager i casene groft sagt tre forskellige roller.

Den offentlige myndighed som driver
I casen om registrering af ejerskab (case 4) indtager de offentlige myndigheder hovedrollen i projektet. Det er dem, der har ejerskabet og driver projektet. De har en stor interesse i at effektivisere processen omkring handel af ejendomme og skabe øget transparens på tværs af de involverede parter. Her får de private virksomheder mere en rolle som leverandører af teknisk ekspertise.

I casen om beskyttelse af persondata (case 2) forholder det sig lidt anderledes. Her fungerer den private virksomhed samtidig også som kontrolinstans – altså en form for garant. Det kan måske synes irrelevant i et dansk perspektiv, hvor tilliden til de offentlige myndigheder er høj. Men i et estisk perspektiv, hvor man arbejder på at konsolidere tilliden til de offentlige myndigheder, er dette et vigtigt element. Det kunne være interessant at overveje, om der vil være tilfælde, hvor denne rolle som garant kunne være værdifuld i en dansk kontekst – evt. på tværs af offentlige myndigheder.

Den offentlige myndighed som garant
I casen om validering af persondata (case 1) er forskellige offentlige myndigheder tiltænkt en rolle som garant, både i forhold til verificering af personoplysninger og som deltager i blockchain-netværket. Rollen som garant er både vigtig i forhold til virksomhedens fremtidige kunder, da dette skaber tillid og sikkerhed for, at løsningen er compliant. Det er også potentielt vigtigt for myndighederne, fordi man herigennem får mulighed for at overvåge, at processerne foregår som de skal.

Den offentlige myndighed som aktiv part
I casen om tracking af containere (case 3) er de offentlige myndigheder tiltænkt en mere aktiv part i samarbejdet som brugere af løsningen. I dette projekt har de offentlige myndigheder en direkte interesse i løsningen, som på den ene side vil effektivisere arbejdsgangene og skabe transparens og på den anden side lette mulighederne for at afgøre tvister.

For at indfri potentialerne i blockchain er det vigtigt, at de offentlige myndigheder arbejder proaktivt med, hvordan de bedst indgår i sådanne offentligt-private samarbejder. Ikke kun i forhold til at udforske de praktiske muligheder men også for at skabe klarhed over, hvilke udfordringer og faldgruber der kan være i etableringen af denne type samarbejder.

Fokus på kontrol og ejerskab

Et tema der går igen på tværs af de fem cases er spørgsmålet om, hvem der har ejerskabet – og i sidste ende kontrollen – over blockchainen. For at skabe ekstra tillid og opbakning til løsningen har man i flere af casene valgt at lægge både udviklingen og driften af blockchainen hos en ekstern softwareleverandør. Softwareleverandøren fungerer her som en neutral part, der ikke har egen interesse i de data, der lægges på blockchainen eller i den tilhørende krypterede database. Tanken er, at det vil være med til at bevare den distribuerede tillid og sikre, at alle parter indgår på lige fod. Men flere af de virksomheder og offentlige myndigheder, der fungerer som projektejere i casene, peger samtidig på, at der kan være et problem i, at magten i stedet centraliseres hos softwareleverandøren. For hvordan forholder man sig, hvis softwareleverandøren går konkurs, eller man af andre årsager ønsker at skifte leverandør? Kan man så reelt det? Eller

bliver man i virkeligheden bundet til den konkrete softwareleverandør? Flere taler også om nødvendigheden af at udvikle modeller, der sikrer decentralisering af magten, så de databaser og administrationssystemer, der kobler sig til blockchainen, ikke ender med at underminere hele grundtanken med blockchain.

Fokus på modenhed og standardisering

Blockchain er stadig en ny og forholdsvis uprøvet teknologi. I alle fem cases har projekterne været præget af en høj grad af udforskning af, hvad teknologien består i, og hvordan den kan anvendes i praksis. Men flere af projekterne er også nået til et stadie, hvor der er behov for klarhed og konsolidering. Spørgsmål rejser sig om teknologiens modenhed, og hvordan man sikrer en professionel drift af løsningen. I flere af vores cases spiller behovet for standardisering en vigtig rolle i realiseringen af projekterne. Det er særligt tydeligt i casen om validering af persondata (case 1). I et gennemregulereret område som den finansielle sektor er det helt afgørende at kunne dokumentere, at systemet er compliant og driftes på en forsvarlig måde. Tillid til teknologien er helt afgørende for at sikre opbakning fra banksektoren. I flere af de andre cases taler man også om behovet for at sikre fælles tekniske standarder, der skaber tryghed om håndteringen af teknologien og sikrer større fleksibilitet i valg af platforme og leverandører.

For at sikre at blockchain-løsningerne kan udvikles ud over proof-of-concept-stadiet er det afgørende at sætte fokus på standardiseringsprocessen inden for dette område.

Teknologiske alternativer

Blockchain er en ny teknologi, der tilbyder nogle unikke muligheder. Men det er ikke den eneste teknologi, man kan bruge, hvis et antal parter vil dele data på tværs af organisationer på en sikker måde. I dette afsnit vil vi forsøge at placere blockchain i det landskab teknologiske løsninger, der allerede eksisterer, og vurdere på hvilke parametre blockchain adskiller sig fra disse.

Specifikt vil vi sammenligne blockchain med en *centraliseret database*, der meget ofte vil være det oplagte alternativ. Derudover vil vi diskutere, hvordan blockchains potentialer og egenskaber forholder sig til dem, man kender fra *Public Key Infrastructures* (PKI) og *linkede databaser*.

Det er værd at bemærke, at man typisk kan bygge nogle ekstra egenskaber oven på en traditionel database og dermed få nogle af de samme egenskaber, som en blockchain har. Det vil ikke altid være oplagt, hvornår disse udbyggede systemer krydser den grænse, der gør, at de kan anses for at være en blockchain. Da grænsen mellem en blockchain og andre teknologier derfor er lidt flydende, giver det ikke nødvendigvis mening at se en blockchain som en modsætning til eksisterende teknologier.

Centraliseret database

I de tilfælde hvor et antal parter skal kunne skrive til og læse fra en fælles database, vil det oplagte alternativ til at bruge en blockchain være at bruge en centraliseret database. I en centraliseret database vil kontrollen med databasen være hos én part, som vi her vil kalde databasens *ejer*. I et system baseret på en centraliseret database vil det være ejeren, der sørger for at vedligeholde databasen, mens de øvrige parter i systemet tilgår databasen for at læse eller skrive data via et interface stillet til rådighed af ejeren. Den primære forskel på en blockchain og en central database er altså, at tilliden til systemet er centraliseret og hviler fuldstændig på databasens ejer, men så længe parterne i systemet kan have tillid til databasens ejer, kan vi opnå mange af de samme egenskaber som med et blockchain-system.

Ejeren vil således kunne sørge for at overholde på forhånd aftalte regler, såsom *immutabilitet*, og sikre, at nye tilføjelser til databasen bliver valideret. *Sporbarhed* kan sikres ved at lade ejeren logge al adgang og opdateringer af databasen. *Konsensus* omkring databasens indhold og *dataintegritet* kan opnås mere eller mindre trivielt, da ejeren kan diktere den korrekte udgave af databasen. Dataintegritet kan ydermere sikres ved løbende at offentliggøre signerede hashes af databasens indhold eller via regulering, fx at kun meget få brugere har adgang til at ændre i databasen.

Generelt er fordelen ved et centraliseret databasesystem, at det typisk vil performe bedre end et blockchain-system, da ejeren egenhændigt overholder systemets regler. Da ejeren egenhændigt står for vedligeholdelsen af databasen og for at overholde systemets regler, og de øvrige parter spiller en mere passiv rolle, vil systemet kunne implementeres med mindre kompleksitet og mindre ressourceforbrug både i form af beregningskraft og lagring af data. Bl.a. undgår man at skulle anvende en konsensusprotokol for at blive enige om indholdet af databasen, og at alle parter skal have en kopi af databasen, som det er tilfældet med

en blockchain. Derudover er centrale databaser en teknologi, der har været anvendt i årtier, så der er tale om langt mere modne og gennemtestede produkter.

I et centraliseret databasesystem vil man kunne fjerne afhængigheden af den tillid, der tillægges databasens ejer. Ved fx at replikere databasens indhold til flere parter vil man kunne sikre, at databasen er tilgængelig uafhængigt af ejeren. Ved at lade ejeren offentliggøre hashes af databasen, eller ved at lade de øvrige parter digitalt signere deres opdateringer, vil man kunne garantere et vist niveau af dataintegritet (case 2 er et eksempel herpå). Med disse tilføjelser vil man dog bevæge sig tættere på den grå zone, hvor man kan begynde at tale om et blockchain-system.

Den primære ulempe ved en centraliseret database i forhold til en blockchain er, at det er nødvendigt at have fuldstændig tillid til ejeren af databasen. Ejeren af databasen kan uden videre bryde systemets regler og evt. helt stoppe med at give adgang til databasen. Om det er hensigtsmæssigt med et sådant set-up, afhænger fuldstændig af situationen. I systemer med (mange) parter, der ikke umiddelbart har indbyrdes tillid mellem hinanden, kan dette være en stopklods for overhovedet at tage systemet i anvendelse. I andre tilfælde kan den distribuerede tillid, der fx kan opnås med blockchain, netop være hovedformålet for systemet, således at databaseejeren ikke alene har kontrollen og ansvaret for at vedligeholde databasen.

Public Key Infrastructure

En *Public Key Infrastructure* (PKI) er et system, der kan bruges til at udveksle og verificere kryptografiske nøgler i et netværk af parter. Via disse nøgler kan parterne i systemet udveksle beskeder, der er digitalt signerede og/eller krypterede. En PKI vil ofte være en integreret del af en blockchain-løsning, der gør det muligt at autentificere parterne og deres tilføjelser til blockchainen, især i lukkede *(permissioned)* blockchain-løsninger. En PKI kan dog også bruges alene til at give nogle af de samme sikkerhedsegenskaber som en blockchain.

En PKI implementerer ikke en database, som et blockchain-system eller en central database. Til gengæld kan en PKI være tilstrækkelig, hvis et system udelukkende er beregnet til sikkert at distribuere data og beskeder i netværket af parter. Via digitale signaturer vil parterne kunne opnå en høj grad af *dataintegritet,* da signerede data ikke kan forfalskes. En PKI kan kombineres med en central database, hvor parter kan lægge signerede dokumenter, som andre kan tilgå.

Som med en central database er en PKI en gennemtestet teknologi, der er afprøvet i stor skala, fx med NemID. Der er udfordringer ved at drive en PKI, men da det som nævnt er en integreret del af en blockchain, vil det ikke være mere vanskeligt at drive en PKI, end det er at drive en blockchain. En udfordring med en PKI er, at alle parter skal kende hinandens offentlige nøgler og være sikre på, at de er udstedt korrekt. Det kan løses ved at have en central autoritet, der udsteder nøglerne, hvilket giver en centraliseret tillidsmodel, hvor alle parter skal have tillid til, at den centrale autoritet gør dette korrekt. Det er den mest praktiske løsning, men det er ikke nødvendigvis hensigtsmæssigt, hvis man ønsker et distribueret, decentralt set-up. Alternativt kan hver part udstede sin egen nøgle (som det kendes fra åbne blockchains, fx Bitcoin) og derefter udveksle offentlige nøgler med de andre parter i systemet, men da antallet af udvekslinger vokser ekspotentielt med antallet af parter, er det ikke altid praktisk muligt.

Linkede databaser

En linket database er en database, der indeholder dokumenter, der kan linke til hinanden. Data kan ligge på forskellige servere, men det skal være muligt og nemt at finde et dokument ud fra et link. Internettet er et eksempel på noget, der kan betragtes som en linket database: Her kan websites ligge på et utal af forskellige servere verden over, men de kan linke til hinanden, og internettet er konstrueret således, at det er nemt at finde den rigtige website på den rigtige server ud fra et link.

En linket database tillader, at data og dokumenter kan være distribueret på mange servere, men at det alligevel er nemt at tilgå dem. Distributionen er dog af en anderledes type end i en blockchain, hvor data er duplikeret, så hele databasen er gemt på alle servere. Til gengæld skal der i en linket database være tillid til, at et link fører til det rigtige dokument. På internettet kan den tillid brydes fx ved såkaldt DNS hijacking, hvor en hacker sørger for, at en internetadresse leder til et andet dokument eller website, end den plejer.

Hvis alle parter kan stole på, at links leder til de rigtige dokumenter, giver en linket database en meget effektiv måde at dele dokumenter på mellem et stort antal parter. Da data som udgangspunkt kun ligger på én server, er der dog ikke samme garanti for *dataintegritet* og *immutabilitet* som på en blockchain, men det kan man opnå, ved at de forskellige servere fx løbende offentliggør hash-værdier af de dokumenter, de har liggende. Dermed vil det være muligt at verificere, at et dokument stemmer overens med det oprindelige, men hvis der er en uoverensstemmelse mellem et downloadet dokument og den forventede hash-værdi, er det som udgangspunkt ikke muligt at finde frem det oprindelige dokument, da der ikke er nogen transparens over for ændringer på de forskellige servere, som det gør sig gældende for blockchain. Forskellen på blockchains og linkede databaser vil i denne sammenhæng være at der i den linkede database ikke nødvendigvis vil være konsensus om hvilke hash-værdier der er de gældende.

Risici og sikkerhed

Blockchain er ikke nogen såkaldt 'silver bullet', der kan løse alle sikkerhedsproblemer for en løsning. En blockchain vil altid være en del af et større system og er blot en teknologi i et landskab af forskellige teknologier. Ovenfor har vi diskuteret nogle af de alternativer, man kan implementere i stedet for en blockchain, og hvilke forskellige egenskaber det giver. I dette afsnit vil vi diskutere, hvilke risici og sikkerhedsimplikationer en blockchain kan give.

Risici

Det skal bemærkes, at alt, der kan digitaliseres, i princippet kan lægges på en blockchain, og at en blockchain derfor kan bruges i alle situationer, hvor en løsning skal bruge en database, men om det giver mening at gøre det, afhænger af use-casen. De potentialer og sikkerhedsfordele en blockchain giver skal vurderes op imod de omkostninger og risici, der følger med at anvende en meget ung teknologi. Og de løsninger, der findes, er ikke fuldstændig gennemprøvede – især ikke i stor skala.

Da en database (hvad enten den er baseret på blockchain eller en mere gennemprøvet teknologi) er helt central for enhver it-løsning, kan det være risikabelt at lade den afhænge af en relativt uprøvet teknologi som blockchain. Dog vil denne risiko blive mindre, efterhånden som blockchain bliver afprøvet i flere og flere projekter, hvilket bidrager til at teste og styrke eksisterende blockchain-produkter og gøre det klart,

præcis hvilke styrker og svagheder en blockchain-løsning har. Det vil alt sammen være med til at sikre, at valget mellem blockchain og et alternativ vil kunne foretages på et mere informeret grundlag.

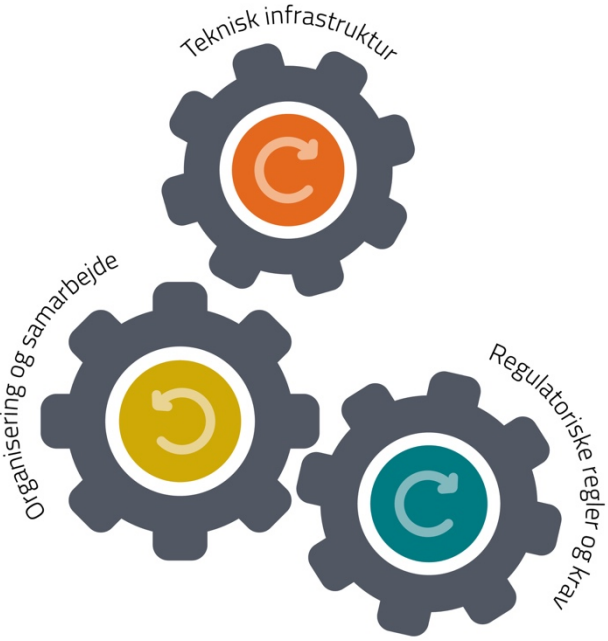
Sikkerhed

I en løsning der bruger en blockchain som database, vil blockchainen i meget høj grad sikre bl.a. immutabilitet, dataintegritet og sporbarhed for de data, der ligger på blockchainen. Men om det faktisk gør hele løsningen mere sikker, afhænger af, at de data, der bliver lagt på blockchainen, er korrekte. Det kræver, at autentifikation af brugere foregår korrekt – altså at den PKI, blockchainen baserer sig på, er implementeret og bliver vedligeholdt korrekt. Generelt gælder det, at da en blockchain er en del af et større system, afhænger sikkerheden af, at alle dele af løsningen er sikre. Blockchain kan ikke sikre en løsning, der i forvejen ikke er sikker. Derudover kan en blockchain godt give nogle garantier om sikkerhed, men hvis den ikke er implementeret korrekt, kan det resultere i fejl og sikkerhedshuller. Da næsten alle blockchain-løsninger er relativt unge, er risikoen for sådanne fejl større end med mere gennemprøvede løsninger.

Konklusion

Erfaringerne fra de fem cases viser med al tydelighed, af teknologien ikke i sig selv kan indfri potentialerne ved blockchain. Det er helt afgørende at se blockchainen-teknologien som en del af et større samspil. Både i forhold til det tekniske landskab den indgår i, og i særdeleshed i den organisatoriske, lovgivningsmæssige og forretningsmæssige virkelighed blockchainen implementeres i.

Betydningen af de forskellige aspekter og deres indbyrdes samspil vil variere. I nogle projekter vil det organisatoriske kun spille en lille rolle (som i case 2). I andre vil det være her fokus bør ligge (som i case 3 og 4). Det kan være et projekt forudsætter en hel ny samarbejdsstruktur med parter, der ikke før har samarbejdet (case 4). Måske får den offentlige part en helt ny rolle. I nogle projekter vil realiseringen af projektet kræve ændringer af lovgivningen internationalt (case 3). I andre spiller lovgivningen måske kun en begrænset rolle (case 2) med mindre justeringer i form af i sektorspecifikke reguleringer (case 5).



Den succesfulde implementering af den lukkede type blockchain sker i et komplekst tværgående samspil mellem lovgivning, teknologi og organisation. Manglende fokus på eller afkobling af blot et af elementerne kan vanskeliggøre eller helt blokere for realiseringen af blockchain-projektet.

I vurderingen af mulighederne for anvendelse af blockchain i den offentlige digitale infrastruktur er det derfor afgørende have et helhedsorienteret fokus på det tekniske og organisatoriske samspil blockchain-løsningen skal indgå i.

Det er desuden væsentligt at bemærke, at man i alle casene i rapporten har valgt at implementere lukkede blockchains. Det ser ud til, at man her har fundet en model, der passer godt ind i organisatoriske set-ups, hvor det kan være afgørende af beskytte data (f.eks. forretningskritiske eller personfølsomme data) og hvor gruppen af aktører er kendte. Dette vil formentlig også gøre sig gældende for mange digitale infrastrukturprojekter. Derfor vil det i den videre vurdering af blockchain-teknologiens potentialer være vigtigt at have særligt fokus på lukkede blockchains.

Valget af blockchain

Det kan være svært at vurdere, hvorvidt det giver teknisk mening at bruge blockchain ind i en offentlig kontekst. Blockchain giver nogle unikke muligheder for at sikre dataintegritet og sporbarhed i et set-up, hvor der ikke er fuldstændig tillid mellem de parter, der indgår i løsningen. Til gengæld er det en mere kompliceret og tungere løsning, der er meget ung og derfor baserer sig på relativt uprøvede løsninger. Nogle af de egenskaber, en blockchain giver, kan opnås med andre, mere gennemprøvede løsninger, og de kan derfor være at foretrække.

Vurderingen bliver ikke nemmere af, at det på nuværende tidspunkt er meget uklart defineret, hvad der udgør en blockchain. Desuden er vi i en situation, hvor blockchain er meget hyped, hvilket giver et incitament til at omtale egen teknologi som en blockchain, selvom den måske ikke i alles øjne opfylder kriterierne for at være det.

Den hype, der er omkring blockchain betyder dog også, at der er et utal af projekter i gang, der forsøger at implementere blockchain i mange forskellige løsninger i mange forskellige brancher og domæner. Når resultaterne af disse projekter efterhånden kommer frem, vil det gradvist blive nemmere at lave en kvalificeret vurdering af, hvilke fordele en blockchain har ift. andre teknologier, om løsningerne kan gøres anvendelige, selvom de baserer sig på kompliceret teknologi, og om de kan skalere til store løsninger med mange transaktioner. Der ligger her en vigtig teknologisk modningsproces, som er vigtig at understøtte, bl.a. gennem øget fokus på den standardiseringsproces, der er iværksat internationalt i forhold til blockchain-teknologien.

Anne Bøgh Fangel

Principal Organisation Analyst
People, Technology and Business Lab
Alexandra Instituttet

Jonas Lindstrøm

Senior Security Architect
Security Lab
Alexandra Instituttet

Peter Sebastian Nordholt

Cryptography Engineer
Security Lab
Alexandra Instituttet

Suzan Tugcu

Anthropologist
People, Technology and Business Lab
Alexandra Instituttet

ALEXANDRA INSTITUTTET