November 2016

# Blockchain – en ny teknologi med potentiale

*Notat fra ATV's Digitale Vismandsråd*

Blockchain er blevet udråbt som en af tidens mest spændende teknologier. Det er blevet spået, at Blockchain vil påvirke finanssektoren på samme måde, som e-mail har påvirket postvæsenet, og mange peger på Blockchain som det mest disruptive, der er sket siden internettet. Blockchain bygger videre på den trend, der kommer til udtryk i deletjenester som Netflix og AirBnB.

I dette notat giver ATV's Digitale Vismandsråd baggrund om teknologien og peger på nogle af de muligheder og udfordringer, den indebærer. Vismandsrådet anbefaler, at vi fra dansk side opruster og eksperimenterer med, hvordan teknologien kan udvikles og anvendes – også inden for andre sektorer end finanssektoren.

**Det startede med Bitcoin**
Blockchain er den basisteknologi, der indgår i den virtuelle valuta Bitcoin, der muliggør finansielle transaktioner i et såkaldt 'peer-to-peer' system, hvor man ikke behøver mellemled som pengeinstitutter eller centralbanker.

Bitcoin blev til som en protest på baggrund af finanskrisen i 2008. Begyndelsen var den 31. oktober 2008, da Satoshi Nakamoto udgav en artikel på et internetsite for kryptografientusiaster. Det vides ikke med bestemthed, hvem Satoshi Nakamoto er. Han boede angiveligt i Tokyo, brugte en gratis e-mail registreret i Tyskland og kommunikerede på perfekt engelsk. Navnet bag pseudonymet er stadig ikke afsløret, men facts peger mod en australsk professor.

Nakamoto protesterede over den uigennemsigtighed, der førte til finanskrisen og mod finanssektorens monopol på betalingstransaktioner. Hans artikel beskriver i detaljer en ny form for betalingssystem baseret på kryptografiske algoritmer, og han kaldte konceptet: "Bitcoin: A Peer-to-Peer Electronic Cash System". Altså et system, der er fuldt peer-to-peer, uden nogen tredjepart eller nationalbank. Året efter lagde han programmet bag algoritmen ud på nettet, frit tilgængeligt for alle – og forsvandt så ud af historien. Men hans opfindelse har fået medvind.

**Hvad kan Blockchain?**
Blockchain er en relativt ny teknologi, der gør det muligt at have et delt og fælles register for deltagere i et netværk.

Teknologien tillader, at netværket kan være fuldt åbent, men anonymt som i Bitcoin eller et mere lukket netværk med et afgrænset sæt af kendte deltagere. Alle deltagere i netværket har som udgangspunkt adgang til den samme information i hver sin lokale kopi – og alle ændringer indføres "samtidigt" og med integritet, så de enkelte transaktioner er uafviselige.

Det gør systemet sikkert, at den samlede Blockchain ikke ligger fast et enkelt sted, men er kopieret ud på de servere, der er en del af netværket. Det er netværket, der godkender, om en transaktion er valid eller ikke. Hvis en enkelt transaktion bliver manipuleret, passer den efterfølgende checksum ikke længere med kopierne på de andre computere og markeres som fejlagtig. Så hackerangreb skal op på et andet niveau af sofistikering for at bryde ind i Blockchain-baserede systemer.

Blockchain indeholder et andet interessant element – nemlig ”smarter contract”, som er en forretningsregel, der gemmes og udføres sammen eller på indikativ af transaktionen. Et eksempel kunne være, at betaling udløses i det øjeblik, en last når en bestemt havn.

Blockchain-teknologi har potentielt meget brede anvendelsesmuligheder. Den kan bruges til at registrere ting på sikker vis. Det kan være en identitet, en titel, en licens, en IP-rettighed og stadig med samme uafviselighed som et mere traditionelt centralt system, men med fuld gennemsigtighed til data og processerne.

Det fælles og delte register, som Blockchain leverer, giver mulighed for, at den enkelte deltager kan træffe beslutninger på baggrund af et (mere) fuldstændigt overblik. De kendte anvendelser af Blockchain som eksempelvis Bitcoin er bygget for at kunne udveksle værdier anonymt og uden for de traditionelle værdinetværk, men teknologien kan bruges alle steder, hvor man har gavn af et sikkert fælles, delt register.

Blockchain er en teknologi, der ændrer på magtforholdet omkring, hvem der ejer data. Det er som sådan farvel til, at for eksempel en offentlig myndighed eller en bank har enekontrol over ”den store bog”, hvori ”sandheden” står – for det samme register ligger på de enkelte interessenters PC eller server. Teknologien giver altså i sig selv mulighed for at opbygge og sikre tillid mellem partnere i et netværk uden brug af en mellemmand, der fungerer som den centrale koordinator.

**Et konkret eksempel**

Et eksempel kan være med til at tydeliggøre værdien og nogle af de potentielle fordele. Lad os forestille os en byggesag. Her involveres en række offentlige instanser, en arkitekt, en projektansvarlig ingeniør og en række håndværkere med forskellige kompetencer og roller.

I dagens situation resulterer det i, at der sendes dokumenter, tages kopier af dokumenter, afholdes byggemøder for at sikre koordinering – alt sammen fordi de enkelte kun har adgang til den information, der ligger på vedkommendes egen lille informations-ø. Måske sidder der en koordinator, som forsøger at fordele informationen så godt som muligt, men det sker ud fra koordinatorens indsigt.

Med et delt register vil alle have adgang til den samme information, der hele tiden vil være fuldt opdateret. Det vil sige, at tømreren kan se, når mureren er færdig – og derfor ikke behøver at vente på det næste byggemøde. Arkitekten og projektledel-

sen kan løbende følge med i fremskridtene og koordinere, og de offentlige myndigheder kan lave en løbende opfølgning på, at tingene bliver som forventet og godkendt. Alle kan se godkendelserne og færdigmeldingerne og eventuelle aftalte ændringer. Der er næppe nogen tvivl om, at en sådan løsning vil kunne bidrage til større effektivitet og sikkerhed. Og de fleste vil nok nikke genkendende til, at en proces bliver forbedret med en større gennemsigtighed.

Og kunne denne løsning så ikke være lavet uden Blockchain? Svaret er, at det kunne den selvfølgelig. Man kunne lave en central database og dele/fordele informationen. Men her melder spørgsmålet om ejerskabet sig som det første punkt – og dernæst spørgsmålet om integritet og uafviselighed. Hvis der efter fem år pludselig kommer en diskussion om, hvorvidt kommunen gav sin godkendelse, så er det med Blockchain ikke et spørgsmål om et centralt register mod en delvis kopi - eller hvem der har den rigtige/endelige version, men om præcis de samme data.

Her har vi brugt en tænkt byggesag som eksempel. Vi kunne i stedet have brugt et eksempel omkring en personskadesag eller en sygdomsjournal eller noget helt fjerde – og gevinsterne vil være de samme. Om end der her nok ville rejse sig et yderligere niveau af spørgsmål omkring *privacy*.

**Blockchains potentiale**

Blockchain-teknologi kan blive fundamentet for en række af nye løsninger, hvor komplekse processer kan forenkles samtidig med, at der skabes større gennemsigtighed og dermed tillid. Og det er ikke kun i finanssektoren, at Blockchain-teknologien kan finde anvendelse. Det gælder også andre sektorer og ikke mindst inden for det offentlige. Med Blockchain og dens indbyggede sikkerhed åbnes nye muligheder for gennemsigtighed omkring offentlig sagsbehandling og for borgerservice, der kan involvere transaktioner med følsomme oplysninger.

Konkret kan man forestille sig, at man gemmer sundhedsdata, stemmesedler, ejerskabsdokumenter, ægteskabsattester og retssagsdokumenter i Blockchain-form, så de hverken kan slettes, manipuleres eller mistes.

Blockchain er selvfølgelig ikke svaret på alle problemer omkring proces og transaktioner. Der er use case, hvor teknologien kan forbedre effektiviteten eller give andre fordele, mens der er andre, hvor det ikke er et godt match.

Man skal heller ikke undervurdere de tekniske og organisatoriske udfordringer, der er ved at bygge et delt system. Det er ikke lettere at lave en god datamodel for det fælles register, end det er at lave en for sin egen lille del - snarere tværtimod.

Og endelig er det klart, at teknologien ikke kun kan bruges i det godes tjeneste. Det har vi set med Bitcoin, som bl.a. er blevet brugt til hvidvaskning og andre lyssky aktiviteter.

**Udfordringerne og balancen**
For at sikre den udbredelse, som er kritisk ved en peer-to-peer løsning, er det nødvendigt, at der skabes en åben teknologi, som sikrer interoperabilitet mellem forskellige systemer, sådan som vi kender det fra internettet.

Det er nødvendigt, at der etableres en standardiseret måde at implementere teknologien, at overføre data og at opbevare data på. Standardiseringen skal som minimum være på plads internt i det enkelte netværk, men ideelt på tværs af netværk ligesom internettet og intranet deler den samme teknologi. Blockchain giver ikke mening uden interoperabilitet.

Grundteknologien skal udvikles, så den adresserer de sikkerhedsmæssige og privacy-mæssige krav, der vil være, hvis det fælles register har forskellige interessenter med forskellige accessrettigheder, som det ville være tilfældet i eksemplet med byggesagen, hvor en offentlig instans har brug for egen specifik information.

Bitcoin har nogle karakteristika, der ikke passer med de krav, der gælder for et reguleret område som eksempelvis tingbogen. Bitcoin er anonym og ”permissionless”, og hvis man vil bruge teknologien til at registrere meget værdifulde assets, for eksempel en ejendom, ønsker man ikke anonymiteten – tværtimod.

Anonymitet kan erstattes af en pseudonym struktur, der slører den enkelte aktørs ægte identitet – og med en kobling til NemID vil man kunne etablere forbindelse til den enkelte aktør. Men man kan også have en implementering af Blockchain med fuldt identificerbare aktører.

Der er også et behov for at kunne rulle transaktioner tilbage i tilfælde af svig eller fejl – og der skal være en juridisk ramme for konfliktløsning.

I Bitcoin er de kryptografiske processer så tunge, at svartider og skalering er en udfordring. Hvis man derimod bruger Blockchain inden for et netværk med kendte aktører, så kan processerne simplificeres, svartiderne afkortes, og skalerbarheden øges. Der er behov for yderligere udvikling af teknologi, herunder specialiseret hardware, hvis man skal kunne håndtere meget store transaktionsmængder.

Omkostningerne ved infrastrukturen vil selvfølgelig også være en afgørende faktor – ikke mindst hvis en IOT-løsning skal gøre brug af Blockchain. Her har man måske brug svartider på millisekunder, og det kan man ikke i dag.

Det betyder imidlertid ikke, at en Blockchain ikke kan skabe betydelig værdi i visse sammenhænge. For eksempel kan smarte kontrakter, der holdes på en Blockchain, give enheder mere selvstændighed og give dem mulighed for at finde modparter til at understøtte midlertidige behov. Et godt eksempel kunne være en smart lås, der kan overføre ejerskabet af fysiske varer eller anmodning om service uden behov for et centralt styringssystem.

Et design af en IT-løsning skal altid vurdere, hvilke teknologier der løser en given opgave bedst med passende hensyn til de investeringer, der er gennemført. Derfor vil de første egentlig produktions Blockchain-løsninger formentlig være private/lukkede med et sæt fælles regler, som anvendes i tæt sammenhæng med eksisterende løsninger. Som teknologi er Blockchain ikke et alt eller intet, men kan forstærke eksisterende netværk med synlighed, deling og dermed tillid.

Det vil være vigtigt at anvende Blockchain i områder, hvor der er et reelt problem at løse – men man skal ikke overse de juridiske og datamodelmæssige udfordringer. Processer, der er tunge, men ikke for juridisk komplicerede, kan være gode kandidater til at indlede forsøg med Blockchain-teknologi.

**Skal Danmark være en frontløber, en fast follower eller en lagger?**
Blockchain er et klassisk eksempel på en ny teknologi, som indeholder en række fordele og nye muligheder – og derfor bør undersøges aktivt og ikke bare bør overlades til en "vent og se"-tilgang.

Det er ATV's Digitale Vismandsråds opfattelse, at man hos danske myndigheder og virksomheder bør overveje, hvordan man kan drage fordel af teknologien, så Danmark kan bevare og udbygge sin position omkring IT-infrastruktur til gavn for både private og offentlige aktører. For eksempel kunne man forestille sig at Nationalbanken – eventuelt i samarbejde med en række nordiske eller private banker afsøgte muligheden for at udvikle en kryptocurrency.

Danmark skal med en stærk vidensbaseret økonomi være på forkant med, hvad teknologier kan og ikke kan – og det er derfor væsentligt, at universiteter og uddannelsesinstitutioner aktivt eksperimenterer med teknologien - meget gerne i samspil med den private sektor og offentlige myndigheder. Men Blockchain er så meget i rampelyset, at der er en risiko og fare for, at teknologien bliver placeret som et universalmiddel mod alle dårligdomme og derfor næsten uundgåeligt vil skuffe. Det er derfor væsentligt, vi forholder os kritisk til anvendelsen.

Hvis de, der ser Blockchain som lige så potentielt disruptiv som internettet – og hvis det holder stik – så bør vi ruste os på bedste vis. Der er regeringer i Europa og i den øvrige verden, der allerede er i fuld gang med at undersøge, hvordan offentlige centrale registre som en tingbog kan flyttes til Blockchain-teknologien.

ATV's Digitale Vismandsråd ser Blockchain som en teknologi med store muligheder for det danske samfund, herunder virksomheder og myndigheder. Men der skal en aktiv og koordineret satsning til, hvis teknologiens potentiale skal blive en realitet.