6018

6002

Emnekode: BAO347

Emnenavn: Bacheloroppgave (Digital Markedsføring)

Innleveringsdato: 07.06.2021

Bacheloroppgave

Høyskolen Kristiania

Blokkjede - en fremtidig løsning for dataregulering og personvern

Vår 2021

Forord

Dette er en bacheloroppgave på 15 studiepoeng ved Høyskolen Kristiania, og markerer slutten på vår bachelorgrad i digital markedsføring. Vi ønsker å takke alle informantene som stilte opp i en travel hverdag, og for all kunnskap dere har delt med oss.

Vi vil også si takk til alle forelesere og medstudenter for tre givende og uforglemmelige år. En spesiell takk til veilederen vår, Annette Kallevig. Som har hjulpet oss med å prioritere og holde fokus på riktig ting underveis i avhandlingen. Dette bidro med å holde motivasjon oppe gjennom en krevende tid. Til slutt ønsker vi også å takke familie og venner som har oppmuntret og støttet oss gjennom hele oppgaveskrivingen.

Vennlig hilsen
6018 og 6002

Sammendrag:
Kryptovalutaer som Bitcoin og Ethereum har blitt sentrale temaer rundt om i verden når vi snakker om teknologisk innovasjonen. Teknologien som står bak disse kryptovalutaene er blokkjede. De fleste er mest kjent med teknologien i sammenheng med overføring og loggføring av disse digitale valutaene. Blokkjede teknologien er likevel bygget på en digital infrastruktur som potensielt kan revolusjonere flere fremtidige innovasjoner på tvers av bransjer. Flere forskere og teknologientusiaster har i imidlertid begynt å se på hvordan denne teknologien kan benyttes for å optimalisere måten vi samler inn og bruker data. Selskaper som Facebook og Google har lenge sittet med makt og kontroll over enorme mengder med personlig informasjon, og har i flere tilfeller misbrukt denne makten. Samtidig har datainnsamling og databehandling møtt på strengere krav for ivaretakelse av forbrukeres rettigheter og personvern, og mange har sett til blokkjedeteknologien som en mulig løsning. Diskusjonen rundt dette omhandler muligheten for å implementere deler eller hele dagens datasystem for å gi kontroll over egne opplysninger tilbake til forbrukere. Problemstillingen vår er utformet slik:

"Hva er den potensielle innvirkningen av blokkjede teknologi på bruk og innsamling av data".

Vi har i denne oppgaven benyttet oss av kvalitativ metode til forskningen ettersom primærdata er utgangspunktet i studien. Data er samlet fra 5 dybdeintervjuer der vi som forskere har hatt en eksplorativ tilnærming. Informantene som er undersøkt har god kunnskap innen blokkjede og/eller bruk og innsamling av data.

Oppgaven gir innsikt til både muligheter og utfordringer knyttet til implementeringen av blokkjede innen bruk og innsamling av data. En ny digital plattform for distribuering av data vil føre til økt gjennomsiktighet og kontroll for både forbrukere og annonsører. Det er allikevel flere sentrale lover og reguleringer som må jobbes rundt før blokkjeder kan benyttes som systemer for håndtering av personlig data. Disse systemene kan på den andre siden bidra til et helt ny verdiskapning hvor data kan kjøpes og selges mellom forbruker og databehandler.

Innholdsfortegnelse

1.0 Innledning

1.1 Introduksjon

Den åpne hemmeligheten innen markedsføring er at det er bygget på å utnytte vår data. Alt vi gjør på internett blir sporet, for å følge våre bevegelser og forstå våre atferdsmønstre. Denne dataen blir samlet inn og videre solgt og distribuert til utallige selskaper på tvers av internett. Data har blitt den nye sentrale valutaen for teknologiselskaper, og med svært lite innsikt og gjennomsiktig er det lett for oss forbrukere å bli utnyttet. Det har kommet til et punkt hvor vi nesten ikke har noe valg lenger. Enten må vi gi fra oss vår data, eller så må vi unngå å bruke internettet i sin helhet.

Parallelt med denne utviklingen har kryptovalutaer som Bitcoin og Ethereum i det siste blitt store snakkiser ettersom de har endret hvordan vi ser på tradisjonell valuta. Disse formene for digitale valutaer er ikke regulert av myndigheter eller sentrale autoriteter, men styres av et såkalt "peer-to-peer" system. Makten ligger dermed hos brukerne, og ingen eksterne autoriteter. Bitcoin var det første store systemet bygget på et blokkjede nettverk, men denne teknologien kan ha revolusjonerende egenskaper for utallige andre bransjer. Innen markedsføring har det lenge vært de store aktørene som Facebook og Google som har dominert, ettersom de sitter på enorme datamengder om forbrukerne. Fler og fler har likevel begynt å stille seg kritiske til disse monopol gigantene for hvordan de både samler og bruker disse sensitive dataene til å påvirke oss forbrukere. Regelverkene blir stadig strengere, og det krever at vi tilpasser oss og kommer med nye og bedre teknologiske løsninger. Blokkjede teknologien har potensiale til å skape store endringer, og totalt endre hvordan vi både samler inn og bruker data for å bedre nå forbrukerne. Det fundamentale konseptet bak blokkjede teknologi er at det tilbyr total gjennomsiktighet, og at det ikke er noen eksterne autoriteter som kan kontrollere og manipulere informasjon som ligger på kjeden.Vi ønsker derfor i denne oppgaven å undersøke hvilket potensiale slik teknologi vil ha for fremtiden av datainnsamling, og de største utfordringene som står i vente før blokkjede teknologi kan integreres som en ny standard for datainnsamling og databruk.

1.2 Bakgrunn for valg

I løpet av studiet digital markedsføring har særlig stordata/personvern og de etiske dilemmaene som utspiller seg som en konsekvens vært av stor interesse for oss begge. Vi har begge lagt merke til hvordan kommunikasjon på digitale flater har føltes mer påtrengende og overvåkende enn noen gang før. Nesten alt vi gjør på nettet spores og lagres i store databaser, som senere blir brukt til å påvirke atferden til forbrukerne. I denne oppgaven ønsker vi å se på blokkjede teknologien som en potensiell løsning på dette problemet, og hvilke fordeler og ulemper denne teknologien kan tilby. Vi er begge veldig interessert i innovative løsninger og teknologi. Blokkjede teknologien er derfor noe som virkelig har fanget vår oppmerksomhet. Ettersom blokkjede teknologi er et såpass nytt konsept og vi enda ikke har sett de reelle innvirkningene det har for næringslivet, er dette noe vi ønsker å se nærmere på i denne oppgaven.

Vi tror denne teknologien kan ha et enormt fremtidig potensiale og kan bli en ny standard for hvordan flere bransjer opererer. Vi vet begge at det er utrolig viktig å være tidlig ute når det kommer til ny teknologi, og mener vi vil ha stor nytte av denne kunnskapen når vi skal ut i næringslivet. Vi har begge blitt veldig fascinert av kryptovaluta, og ønsker derfor å videre undersøke teknologien bak.

1.3 Problemstilling

Ved bruk av relevant teori og pensum fra studieretningen vår ønsker vi å se nærmere på hvordan denne teknologien fungerer, og hvilket potensiale den har for fremtiden. Vår problemstilling er derfor:

“Hva er den potensielle innvirkningen av blokkjede teknologi på bruk og innsamling av data”.

Ved bruk av kvalitative metoder som dybdeintervju, ønsker vi å få en klarere innsikt fra fagpersoner om hvordan blokkjede teknologi kan benyttes som en løsning på data/personvern utfordringer, og hvilke hindringer som står i vente før blokkjede kan bli integrert som en ny standard.

Ettersom problemstillingen er relativt åpen ser vi det hensiktsmessig å ytterligere avgrense problemstillingen under følgende hovedkategorier, med tilhørende temaer.

- ***Blokkjedes datapotensiale: gjennomsiktighet, kontroll, og datasystem.***
- ***Blokkjedes datautfordringer: Tilgjengelig, sletting/retting, og ansvarlig part.***
- ***Blokkjede - Veien videre: Bedrifters nytte, De store aktørene, regulatoriske endringer.***

1.4 Formål

Formålet med studien er å kartlegge det reelle potensiale for blokkjede teknologi når det kommer til bruk og innsamling av data. Resultatene fra studien vil gi oss en bredere forståelse for hvordan slik teknologi fungerer teoretisk, men også de praktiske implikasjonene som kan forekomme. Ettersom blokkjedeteknologi er et nytt felt under stadig utvikling vil det være vanskelig å komme med konkrete operative løsninger eller fasitsvar. Oppgaven vår vil derfor ha en eksplorativ tilnærming for å avdekke potensielle muligheter innen fagfeltet. Vi ønsker at resultatene fra denne oppgaven kan bli benyttet som et fundament i videre forskning, samt å gi en bedre forståelse for blokkjede teknologien og hvilke muligheter teknologien kan gi innen bruk og innsamling av data.

1.5 Avgrensning

Ettersom blokkjede er et såpass bredt fagfelt med utallige bruksområder ser vi det nødvendig å avgrense oppgaven. Studien vår vil av den grunn fokusere kun på potensiale blokkjeder vil ha for bruk og innsamling av data. Det er allerede gjort mye studier på det mer generelle bruksområdet av blokkjeder, så vi ser det derfor hensiktsmessig å ikke gå i dybden på disse i denne oppgaven. Denne studien ønsker å utforske det bredere potensiale og aktuelle løsninger innen bruk og innsamling av data. Vi vil derfor ikke gå i dybden på det teknologiske oppsettet av de aktuelle løsningene som blir presentert, men heller drøfte disse fra et teoretisk standpunkt.

1.6 Begrepsforklaring

Gjennom oppgaven kommer vi til å bruke sentrale fagbegreper for å forklare ulike konsepter innen blokkjede og data/personvern. Dette er begreper som er viktige å forstå for å få en

korrekt oppfattelse av oppgaven og de diskuterte temaene. Under er en liste med de aktuelle begrepene som benyttes regelmessig i oppgaven.

Cookies - Er en liten mengde data som genereres av nettsiden man besøker, og lagres av nettleseren din. Formålet er å huske informasjon om deg, for å gi bedre brukeropplevelser, men også data til nettsidene (Techterms, 2011).

Data controller - En person som (enten alene eller i fellesskap eller til felles med andre personer) bestemmer formålene for og måten personlige data blir behandlet på, eller som skal behandles (Ico, 2021).

Data processor - Enhver person (bortsett fra en ansatt av data kontrolleren) som behandler dataene på vegne av data kontrolleren (Ico, 2021).

Digital lommebok - også kalt "e-wallet" er et programvarebasert system som lar brukere oppbevare finansielle midler, gjennomføre transaksjoner og spore betalinger digitalt. Dette er en sikker løsning, og lommebøkene kan også skape sterke passord for deg uten at du må bekymre deg om å glemme de senere (Kagan, 2021).

Distributed ledger - Er er en database som er spredt mellom flere enheter. Det fungerer som en oversikt for transaksjoner og kontrakter mellom ulike aktører i en desentralisert form (Majaski, 2018).

GDPR - General Data Protection Regulation. I 2018 kom denne nye personopplysningsloven. Loven består av nasjonale regler og EUs personvernforordning, og ble kalt GDPR (Datatilsynet, 2019).

Hashverdi - Ved å hashe noe vil den hashen få en kode (verdi) som angir den hashen. Dette er en metode man bruker for gjøre en melding ugjenkjennbar så den ikke kan dekodes (Jaatun, 2018)

Hyperledger - Er en open source blokkjede-løsning som ble til for å skape stabile rammeverk, og som et nøytralt hjem for distributed ledgers (Hyperledger, 2021).

Kryptografi - Dette opererer som et hemmelig språk, og det er kunsten til å utarbeide hemmelig informasjon som kun den som skal forstå det, kan løse det (Knapskog og Eilertsen, 2018).

Lukket blokkjede - På engelsk kalt **private blockchain** er et lukket nettverk hvor selektivt utvalgte for lov til å delta, og gjennomføre transaksjoner. Folk som ikke er i nettverket har ikke mulighet til å se på transaksjoner utført (Seth, 2021).

Miner - Er en som kjører algoritmer på en spesifikk programvare for å sørge for at transaksjonen mellom person A og person B blir registrert på en ledger. I gjengjeld får vedkommende en ny-skapt coin (kryptovaluta) (Ethos, 2021).

Noder - En blokkjede eksisterer av blokker av data, og disse datablokkene er lagret på noder. Det kan være datamaskiner, serverer, eller en telefon, og de former hele infrastrukturen til blokkjede. Alle noder på en blokkjede er tilkoblet hverandre, og de utveksler konstant den nyeste dataen med hverandre. De lagrer, sprer og vedlikeholder blokkjede dataen. En full node er for eksempel en datamaskin som inneholder en full kopi av transaksjonshistorikken til en blokkjede (Jimi, 2018).

OBT (Online Behavioral Targeting) - en teknikk benyttet for å levere relevant kommunikasjon til forbrukere, ved bruk av data og analyse av forbrukeratferd på nett. (Li, Nill, 2020)

Peer to peer - (P2P) Er en desentralisert løsning hvor to individer kan samhandle direkte med hverandre uten noe form for involvering av en tredjepart. Transaksjonene vil da skje umiddelbart fra person til person (Hayes, 2021).

Proof of concept - Også kalt PoC er en måte å teste om en forretningside er gjennomførbar og levedyktig på markedet. Det fokuserer på det tekniske aspektet bak gjennomførbarheten til et produkt eller en app (Medium, 2020.

Proof of stake - Også kalt PoS er en funksjon som stiller krav til personer som skal mine eller validere blokk-transaksjoner avhengig av hvor mange coins (krypto) de har. Dette betyr at desto mer coins en miner eier, desto mer mining-muligheter har de (Frankenfield, 2021).

Proof of work - Også kalt PoW er en desentralisert konsensus mekanisme som krever at brukerne av nettverket må løse vilkårlige matematiske utfordringer for å forhindre at noen misbruker systemet (Frankenfield, 2021).

Stordata - Er en mengde data som er så stor at tradisjonelle analyseverktøy ikke er kapable nok, men at statistiske modeller må til for å hente ut relevant data. (Datatilsynet, 2017)

Åpen Blokkjede - På engelsk kalt **public blockchain** er et nettverk som er åpent for alle som ønsker å bli med uten å få tillatelse. Her kan alle gjennomføre transaksjoner, og de er transparente for alle (Seth, 2021).

2.0 Teorigrunnlag

Gjennom teorigrunnlaget henviser vi til relevant teori undersøkt i forbindelse med bacheloroppgaven. Målet her er å først etablere en forståelse for aspektene knyttet til problemstillingen. Deretter vil vi benytte oss av denne kunnskapen i metoden, og videre reflektere over informasjonen i diskusjonen og konklusjonen.

Vi starter først med å presentere de ulike mekanismene for bruk og innsamling av data i dag, samt hvordan de største dataselskapene opererer. For å forstå blokkjedes potensielle innvirkning er det viktig å forstå hvordan mekanismer for innsamling og bruk av data fungerer i dag, og de potensielle fallgruvene ved dagens system.

Deretter vil vi vi gå mer i dybden på forbruker aspektet av disse systemene. Dette er for å kartlegge den nåværende kunnskapen til forbrukere, men også for å bedre forstå hvordan forbrukere kan bli utnyttet med dagens system, og hvilke muligheter de har for å unngå dette.

Videre vil vi forklare hvordan blokkjeder fungerer, og de viktigste mekanismene blokkjeder tilbyr. Senere går vi i dybden på forskning som allerede er gjort på området, hvor vi tar for oss forskjellige artikler funnet gjennom litteratursøk. Dette er for å avdekke potensialet blokkjede teknologi har for bruk og innsamling av data, men også sentrale utfordringer.

2.1 Stordata (Innsamling og bruk).

I korte trekk beskrives stordata som "en mengde data som er så stor at tradisjonelle analyseverktøy ikke er kapable nok, men at statistiske modeller må til for å hente ut relevant data" (Datatilsynet, 2017). Stordata kan bli benyttet til mange gode formål. Det blir som regel brukt til å analysere anonymisert data for å identifisere og forutse fremtidige trender og korrelasjoner. I prinsippet utfordrer ikke stordata personvern, men i visse tilfeller kan det bli brukt på måter hvor det påvirker enkeltindivider direkte.

Vi etterlater oss data overalt, og det blir da generert mye data fra oss forbrukere. Eksempler: Facebook, lokasjon fra mobilen/applikasjoner, YouTube, Musikktjenester, søk på google, kjøp i nettbutikker, treningsapplikasjoner osv. Det er uendelig med ulike tjenester vi benytter oss av hver dag som samler inn data om oss som videre blir brukt, og i flere tilfeller også solgt videre. Flere kommersielle virksomheter har funnet ut at man kan bruke denne dataen strategisk for å oppnå mer salg, promotering av kampanjer, og hva som treffer forbrukeren hvor og på hvilke tidspunkt. Stordata leter etter mønstre og sammenhenger, noe som blir ekstremt verdifullt for markedsføring, salg og ikke minst myndigheter som får bedre innsikt i befolkningens mønstre. Dette blir benyttet til både godt og vondt. Det bidrar til at det blir lettere for merkevarer og øke salg basert på bedre innsikt i forbrukernes kjøpsmønster og interesser. Det bidrar også til et klarer overblikk over sykdommer, og kriminalitet, noe som er en klart stor ressurs for enhver myndighet (Datatilsynet, 2017).

På den andre siden fører dette også til flere utfordringer i henhold til vedlikehold av dagens personvernlovgivninger. Hver for seg er ikke dataene samlet inn sensitive og skadelige, men når man begynner å slå sammen dataen kan man ende opp med et sensitivt resultat. Prosessen bak hvordan dataene om deg blir hentet inn er som regel ikke gjennomsiktige. Noe som medfører at forbrukerne ikke vet hvem eller hva dataen om de blir brukt til (Datatilsynet, 2017).

2.2 Ulike aktører og deres rolle

De to største aktørene i dag innen tjenestebasert innhenting er Google og Facebook. De samler inn all dataen sin ved hjelp av forbrukeren selv, og trenger ikke å bruke pengeressurser for å innhente all den verdifulle informasjonen andre selskaper er sultne etter å få tak i.

2.2.1 Google

Mange nettsider og apper bruker Google sine tjenester for å forbedre innholdet sitt og holde det så gunstig som mulig. Når disse nettsidene/appene integrerer Google sine tjenester, godtar de å dele all dataen de henter inn til Google. På denne måten får google konstant samlet inn enorme mengder data forholdsvis uten noe spesiell kostnad.

Et eksempel er hvis man besøker en nettside som benytter seg av Google analytics, Google Ads eller har en YouTube video inkorporert på siden, så vil den informasjonen nettsiden samler inn om deg også gå til Google. Dette inkluderer IP adressen din, og Google vil også ofte benytte seg av egne Cookies på siden, hvis ikke det allerede ligger noen der fra før. Uavhengig så vil den hente opp data herfra også. De bruker all informasjonen de får delt til å utbedre sine egne tjenester og alle tredjeparter som benytter seg av de, vedlikeholde og forbedre, utvikle nye tjenester, måle effektivitet av reklamer, beskytte mot svindel og ikke minst personalisere innhold og reklamer rettet mot deg som forbruker. (Google, 2021)

Google har noen måter hvor man selv kan være med å kontrollere hva slags data man deler, gjennom tjenester hvor Googles tjenester står for innsamlingen. De fleste innebærer at man har logget inn på Google-kontoen sin for å få tilgang til. Inne på google brukeren sin kan man gå inn på "Ad Settings" hvor man kan kontrollere om man skal motta personaliserte ads basert på dataen din, og man kan velge å blokkere spesifikke annonsører. Man har en funksjon som heter "My Activity" hvor man kan se over, samt kontrollere dataen som har blitt samlet inn på deg via Googles tjenester. Dette inkluderer data hentet fra andre sider og applikasjoner som benytter seg av Google sine tjenester. Her har man faktisk mulighet til å få full oversikt via dato, tema, og man kan slette deler man ikke vil ha liggende. Når det er sagt så er ikke disse tjenesten akkurat informert ut til mannen i gata, og de fleste har ikke noe form for kjennskap til at disse mulighetene eksisterer (Google, 2021).

Sjefsarkitekten i Google har skrevet at *"the only way in which Google reveals information about users are when we receive lawful, specific orders about individuals."* (Zunger, 2013). Google sier selv at de ikke selger personopplysningene dine til noen, men det betyr ikke at de ikke selger dataen. Som de selv skriver: "Vi gir annonsørene data om resultatene for annonse deres, men uten å avsløre noen av personopplysningene dine. I hvert ledd av annonse prosessen holder vi personopplysningene beskyttet og private." (Google, 2021). Det blir ikke spesifisert hvordan, men her faller utfordringen inn hvor som tidligere nevnt i avsnittet om

stordata. Når dataene blir samlet sammen og analysert, kan den etterhvert føre til at man blir identifiserbar.

2.2.2 Facebook

Facebook samler inn mye mer data enn bare informasjonen man har valgt å dele med de på profilen sin. De sporer folk på andre sider og applikasjoner, og samler inn biometrisk ansiktsdata uten noe ordentlig samtykke fra brukerne. Innhenting av data fra forbrukerne kan gå inn på et ganske personlig nivå, og innen ulike målrettede grupper tilbyr Facebook annonsører opp til 1,5 millioner mennesker som sitter på interessene/preferansene til å engasjere med de gitte tjenestene. *"Facebook can learn almost anything about you by using artificial intelligence to analyze your behavior. That knowledge turns out to be perfect both for advertising and propaganda"* (Eckersley, 2018).

Facebook bruker flere ulike programvarer for å samle inn data, blant annet noe som heter Facebook Pixel. Pixel er usynlige koder som liker skjult på nettsider, slik at den siden og Facebook har muligheten til å spore forbrukernes aktiviteter (Singer, 2018). Det er utallige med selskaper som samler inn data på brukerne sine for markedsføringsformål, men Facebook får mest kritikk da de de er markedslederne. Det er også den største inntektskilden deres (85,965 USD i 2020), som selvfølgelig fører til diskusjon om hvor etiske hele prosessen er (Statista, 2021).

Facebook tilbyr en plattform der brukerne får fri tilgang til det meste man vil anse som nyttig, og hjelpsomt. Mange bruker plattformen for å holde kontakt med venner, jobbgrupper, hobbygrupper, og som nyhetskanal. I bakgrunnen av alt dette skjer det konstante analyser, profileringer, og algoritmiske prosesser som samler inn data uten at vi er klar over det (Johannes Caspar, 2018).

2.2.3 Stordatas fallgruver

I flere år nå har det vært konvensjonelt at den smarteste måten å bygge opp et svært selskap er å samle inn store mengder data på kundene dine. Men etter hvert har man begynt å se at det også kan påføre en stor risiko og skade på selskapene. (John D. Stoll, 2018). Selskaper møter nå mangel på tillit fra kundene sine da folk begynner å bli mer oppmerksomme på hvor mye data som faktisk samles inn på hver enkelt forbruker. Da flere av de store aktørene som

benytter seg i aller høyeste grad av stordata har opplevd databrudd, skaper det en naturlig redsel for hva som kan skje med all dataen som man har lagt fra seg.

"De scanner ikke legitimasjonen på grunn av alderen min, skjegget mitt er eldre enn 21" (Roy Hewitt, 2018. Roy er en 71 år gammel mann som er veldig bevisst på at han ikke liker å legge igjen data hos verken butikker eller banker fordi han er redd for at informasjonen skal bli misbrukt og komme i feil hender. Han er et noenlunde ekstremt eksempel på skeptikere, men som John D. Stoll påpeker i denne artikkelen. Så er dette forholdet vi vanlig forbukere av sosiale medier og lignende begynner å få til de større plattformene vi benytter oss av som Facebook, Youtube/Google og Twitter.

Cambridge Analytica var et mining selskap som sto for Facebooks største datalekkasje gjennom tidene i 2014. Selve data lekkasjen skjedde når forskere fra Cambridge Analytica tilbød å betale Facebook brukere for å kjøre tester på de. Når man godtok å være med i undersøkelsen fikk man beskjed om at din personlige Facebookbruker ville bli brukt. Det som også skjedde var at alle vennene man hadde knyttet til Facebookbrukeren sin også ble samlet inn komplett informasjon på, men dette ble ikke formidlet. *"Facebook should have never disclosed this data to a third party"* (Marc Rotenberg, 2018). Facebook mislykket å beskytte dataen sin, og selskapet fant ikke ut om dette før i 2015. Da spurte de Cambridge Analytica om å slette all data de hadde samlet inn på feil måte, men i følge forskning utført av the New York Times, så skjedde aldri dette (Rash, 2018).

Det var ikke før i mars 2018 at det kom frem for offentligheten at denne datalekkasjen faktisk hadde skjedd. Cambridge Analytica hadde brukt data fra 87 millioner ulike Facebookbrukere og laget psykografiske tilpassede annonser rettet mot å påvirke folks stemmepreferanser inn mot USAs presidentvalg i 2016. Dette har ført til mange debatter rundt de etiske kravene rundt datainnsamling, og krav som bør stilles til regulering av kunstig intelligens. (Hern, 2018). Forskning har vist at det ikke er så lett å få implementert nye standarder for slike krav, da folk på tross av irritasjon knyttet til all datalekkasje stiller seg i en konflikterende rolle når løsninger skal implementeres. Folk vil ikke at dataen deres skal lekkes eller misbrukes, men de vil heller ikke at plattformene de benytter seg av daglig skal endres på. (Choi et al., 2018)

2.3 Personalisering og Online Behavioral Targeting.

OBT, også kjent som online behavioral targeting, er en teknikk benyttet for å levere relevant kommunikasjon til forbrukere, ved bruk av data og analyse av forbrukeratferd på nett. informasjon samles inn om den enkelte forbrukers internett- og mobilaktiviteter for å få et bredere bilde av forbrukeren. Den innsamlede dataen om forbrukeren består ofte av: hvilke nettsider forbrukeren har besøkt, hvilke søkeord de bruker, og deres kjøpshistorikk. Denne informasjonen kombineres ofte med demografisk og geografisk data, samlet fra andre mediekilder som for eksempel GPS lokasjon på mobile enheter. Når dataene analyseres, vil den samlede informasjonen gi markedsførere muligheten til å levere målrettet og relevant kommunikasjon til forbrukeren (Nill and Aalberts, 2014). OBT har økt effektiviteten til digital markedsføring eksponentielt, ettersom det nå er mulig å målrette seg til kun de forbrukerne som vil ha nytte av våre produkter og tjenester (Tucker, 2012).

Den økte inntekten disse annonsene har generert har tillatt utgivere og produsenter muligheten til å publisere digitalt innhold gratis. Betalingen derimot blir nettopp at kunder - ofte uvitende - betaler i form av å gi digitale annonsører tilgang til sin personlige informasjon. Vi har nådd en ny historisk høyde i hvilken grad forbrukerdata kan samles inn, analyseres, lagres og utnyttes (Li, Nill, 2020). Det har allikevel blitt strengere reguleringer knyttet til datainnsamling og personvern, som vi kommer tilbake til senere i oppgaven. Allikevel er det vanskelig å benytte seg av mangfoldet av de digitale tjenestene som har integrert seg i hverdagen vår, uten å gi fra seg tilstrekkelige mengder med data. Det finnes ulike verktøy man kan bruke for å beskytte seg mot datasporing, men svært få som gjør det på en sømløs måte, og tilgangen til tjenestene som bruker datasporing blir ofte blokkert. For brukere som ønsker å beskytte sin personlige informasjon blir ofte den beste løsningen å ikke benytte seg av internett, eller mobile tjenester i det hele tatt (Li, Nill, 2020).

De fleste forbrukere er bevisste på at digitale tjenester samler og bruker data for å levere personaliserte annonser, men er ofte uvitende om bredden og dybden av denne prosessen. (Smit et al. 2014; Milne et al. 2008; Turow et al.2008). De forstår ofte ikke omfanget og alvoret av de nye datainnsamlingsteknikkene, og vet heller ikke hvordan de kan begrense tilgangen til deres personlige data. Alt i alt har de fleste forbrukerne et tilsynelatende negativt syn på OBT, så fort det blir forklart for dem. (Boerman et al. 2017; Turow et al. 2012; Smit et

al. 2014). Opplyste forbrukere benytter seg også oftere av verktøy for å begrense tilgangen til deres personlige data (Redondo and Aznar, 2018).

Samtidig som OBT har muligheten til å gjøre annonser mer effektive og dermed mer profitable, så kan teknikken slå tilbake hvis forbrukere oppfatter annonsører som for påtrengende og inngripende (Tucker 2012; Aguirre et al. 2015; Bleier and Eisenbeiss 2015). Videre kan personalisert kommunikasjon, som er det endelige målet for OBT, også føre til personverns bekymringer. Schwaig et al. (2013) undersøkte sammenhenger mellom enkeltpersoner og deres holdning til personvern. De fant ut at angst for ny teknologi og mangel på opplevd kontroll, bidrar til en mer negativ holdning til personvern for informasjon. I sin tur kan denne negative holdningen være skadelig for helheten av digitale tjenester (Martin og Smith 2008). Personvern og sikkerhetsproblemer er i gjengjeld negativt korrelert med forbrukernes tillit til annonsører og Internettet generelt (McCole et al. 2010; Sarathy og Robertson 2003).

2.3.1 Gjennomsiktighet, og oppfattet kontroll:

Forskning viser at å gi forbrukere mer kontroll over egen data eller i det minste oppfattet kontroll over egen data kan redusere bekymringer relatert til personvern. (Malhotra et al. 2004; Tucker 2014). Wang and Wu (2014) utviklet en modell som støtter argumentet for at hvis forbrukere er informert, ikke i form av en ansvarsfraskrivelse, men gjennom informasjon om den faktiske nytten og verdien av datainnsamlingen, så er forbrukere mer villig til å samtykke med innsamlingen.

2.4 Regulering og restriksjoner for datainnsamling og databruk (GDPR)

EU sier at GDPR var laget for å "harmonisere" datasikkerhets lover for alle EU/EØS land, samt gi en bedre beskyttelse av rettigheter for individer. GDPR ble også skapt for å endre på hvordan virksomheter og organisasjoner kan håndtere informasjonen til de som interagerer med dem. Det er potensiale for store bøter, og omdømmeskade for de som bryter reglene (edps.europa, 2018) (Geradin, 2020).

I 2018 kom denne nye personopplysningsloven. Loven består av nasjonale regler og EUs personvernforordning, og ble kalt GDPR (General Data Protection Regulation) (Datatilsynet, 2019). Loven handler om behandling, altså innsamling og bruk av personopplysninger. Reglene gir virksomheter en rekke plikter, mens den gir enkeltpersoner rettigheter. Det

gjelder for så og si alle virksomheter, med noen få unntakstilfeller. Hvis norsk lov går i konflikt med GDPR så vil GDPR gå foran. Dette betyr at alle norske regler om behandling av personopplysninger bør passe inn i GDPR systemet for å være gyldige.

Personvernforordningen er lik i alle EU/EØS-land, noe som fører til at virksomheter fra andre EU/EØS-land må følge samme fordringer som norske virksomheter i forhold til innsamling og bruk av data. Loven gjelder når virksomheter benytter seg av automatisk (elektronisk) behandling av personopplysninger. Den gjelder også når virksomheten ikke utfører automatisk behandling, men hvis personopplysningene skal inngå i et strukturert register. I noen tilfeller vil loven også gjelde for virksomheter som ikke er fra EU/EØS hvis de skal behandle personopplysninger knyttet til personer i f.eks. Norge. Virksomheten har da en plikt til å utpeke en representant i EU/EØS.

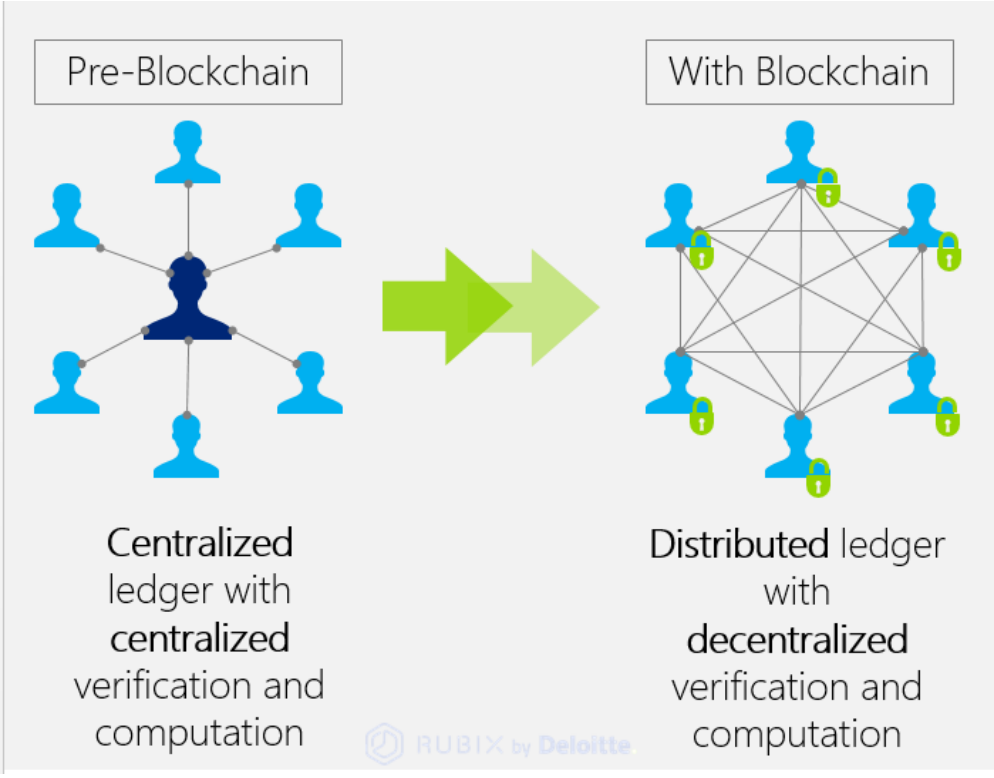
GDPR-loven gjelder ikke hvis fysiske personer som er på familiebesøk, eller kameraovervåkning av eget hus. Det gjelder heller ikke hvis det bistår myndighetene med å forebygge, etterforske eller straffeforfølge straffbare forhold, og for utelukkende journalistiske, akademiske, kunstneriske eller litterære formål. (Datatilsynet, 2019)

2.5 Teknologien bak blokkjede

Ideen bak blokkjede ble først utforsket av Stuart Haber og W. Scott Stornetta i artikkelen "How to timestamp a digital document" i 1991. De så at det var en utfordring med tidsstempling av digitale dokumenter, og at informasjonen enkelt kunne endres. I artikkelen introduserte de en ide om et system bygget på en kjede med hashes og kryptografisk nøyaktighet for verifisering og tidsstempling av et voksende sett med digitale dokumenter, som ville være sikrere enn å stole på en tredjepart. (Harber & Stornetta, 1991). Ideen forble kun en idee, frem til 2008 når den ble reintrodusert og henvist til i et "whitepaper" av den mystiske figuren Satoshi Nakamoto for et digitalt Peer-to-Peer (P2P) system for digital valuta kalt Bitcoin. Satoshi Nakamoto er et pseudonym og det er fortsatt ikke klart hvem denne mystiske figuren er. Nakamoto ble dermed den første til å introdusere en digital tjeneste bygget på et blokkjede nettverk.

"Distributed ledger technology", også kalt DLT er et sentralt begrep innen blokkjede teknologi. DLT betyr i hovedsak at et nettverk er desentralisert. Det er ingen sentral autoritet

som modererer eller administrerer data. Vi refererer ofte til dette som et Peer-to-peer nettverk (P2P). Ordet "Peer" er ofte brukt som en node. En node refererer til hver enhet som er koblet til nettverket. I et slikt system bidrar hver enhet i nettverket til å dele internett dekning, prosessorkraft, og lagringsplass, enten det er en mobil enhet eller en datamaskin. Dette øker igjen hastigheten av informasjonsflyten i nettverket, i motsetning til et sentralisert nettverk hvor informasjonsflyten blir tregere ved at flere benytter seg av det samme systemet.



Figur 1. Illustrasjon av Hossein Abbaspour

Generelt sett lagres det ikke noe faktisk innhold på en blokkjede. Digitale dokumenter, musikk, bilder, kontrakter, transaksjoner og annet innhold blir tildelt en såkalt "hash" som er en kryptografisk kode bestående av 64 bokstaver og tall, som representerer innholdet. Tenk på en hash som et fingeravtrykk for innholdet ditt. Hver hash er unik, og representerer en unik bit med informasjon. En eneste endring i den originale informasjonen vil generere en helt ny hash (Williams 2019, s. 64).

Et blokkjede nettverk er sammensatt av en rekke med datapakker også kjent som blokker. Hver blokk inneholder kryptografisk data som enda ikke er registrert på nettverket, et bestemt tidsstempel, hashverdien fra den forrige blokken i kjeden, og en såkalt nonce som er et

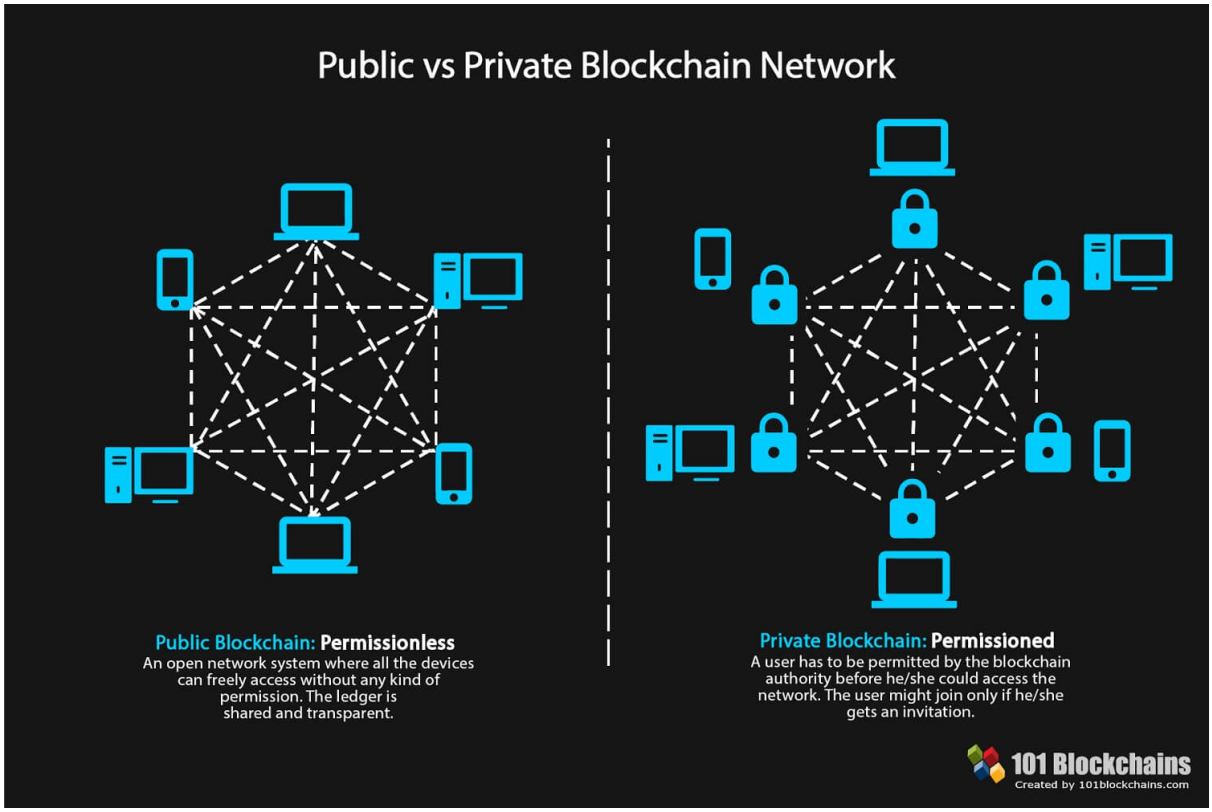
randomisert nummer for verifisering av blokken. Hashverdien forhindrer svindel og endring av materialet i blokken, ettersom en endring av blokken vil gi en ny hashverdi.

2.5.1 Konsensus

For at en node skal validere (eller ugyldiggjøre) en transaksjon i nettverket, må datamaskinen løse et komplekst matematisk problem som krever enorm gjetting. Dette matematiske problemet er så komplekst at det ville tatt en enkelt datamaskin flere år å løse. For å endre eller validere transaksjonen, må hver node arbeide med andre noder i nettverket for å løse problemet kollektivt. Når problemet er løst av en av nodene, må datamaskinen dele sitt "proof of work" med de andre datamaskinene i nettverket for å validere problemløsningen. Dette betyr at en potensiell hacker eller svindler vil måtte manipulere tilsynelatende utallige datamaskiner for å kunne legge til falsk eller uekte informasjon i blokkjeden. (Fandl, 2020) Dette er den såkalte konsensus mekanismen mange av disse blokkjedene er bygget på, som gjør det nesten umulig for en enkeltaktør å manipulere kjeden.

2.5.2 Åpen og lukket blokkjede.

Blokkjeder kan skilles mellom åpne og lukkede, også kjent som private og offentlige blokkjeder (Williams 2019, s. 73). I en åpen blokkjede kan alle i nettverket, både se gjennom og verifisere blokker. Alle kan også delta i prosessen for å få konsensus om validiteten til en blokk. Det er en slik plattform kryptovalutaene Bitcoin og Ethereum er bygget på, og tilbyr total gjennomsiktighet for alle deltakere av kjeden.



Figur 2. Illustrasjon fra 101-Blockchains

En lukket blokkjede derimot krever tilgang før du kan se gjennom og delta i blokkjeden. Slike nettverk brukes ofte av større bedrifter, som vil holde sin informasjon og data privat. Linux Hyperledger er et rammeverk som anvendes for bruk av disse private blokkjedene. Disse rammeverkene er essensielle for bedrifter som behandler store mengder sensitiv data.

Begge blokkjedene har sine respektive fordeler og ulemper. I noen tilfeller er total gjennomsiktighet nødvendig, som i åpne blokkjeder som Bitcoin, mens i andre tilfeller er kontroll av data viktigere, som for eksempel offentlige systemer som behandler sensitiv persondata. Hva som er best avhenger helt av hva vi bruker systemet til og hvilke tjenester det er snakk om.

En annen ganske stor ulempe med en åpen blokkjede er den betydelige mengden prosessorkraft som kreves for å opprettholde en hovedbok i stor skala, for å oppnå konsensus. Enhver node i nettverket konkurrerer og samarbeide i beregningen av komplekse kryptografiske problemer kalt “proof of work”. (Jayachandran, 2017). Når disse matematiske problemene løses belønnes det med et sett andel bitcoin, eller annen kryptovaluta. Dette er en såkalt “mining reward.” Problemet er at det krever enorme mengder strøm for at

datamaskiner kan løse disse komplekse problemene. Kinas bitcoin-utvinning driver nær 80 prosent av verdens kryptovalutahandel. Denne utvinningen krever enorme mengder strøm, og når strømmen hovedsakelig kommer fra kullkraftverk, kan dette føre til store miljøskadelige konsekvenser (NTB-AFP, 2021).

Et av de store løftene med blokkjede teknologi er den totale gjennomsiktigheten et slikt nettverk tilbyr. Det at all informasjon i nettverket er tilgjengelig for enhver deltaker i kjeden er ofte sett som den store fordelen med blokkjede teknologi. Det at den tilbyr total gjennomsiktighet for brukerne, uten kontroll og manipulasjon av en sentral autoritet. Etterhvert som flere selskaper tar i bruk private blokkjeder, frykter mange at det store løftet om gjennomsiktighet sakte vil visne bort, og at det igjen er de store private aktørene som sitter på kontrollen. Disse store aktørene vil allikevel måtte forholde seg til de åpne/offentlige kjedene som igjen vil være nesten umulig å kunne kontrolleres av enkelte aktører. (Williams 2019, s. 74)

2.5.3 Smartkontrakter

Smartkontrakter er et begrep som brukes til å beskrive datakode som automatisk utfører hele eller deler av en avtale og lagres på en blockchain-basert plattform. (*Stuart. ET al, 2018.*) Du kan tenke på en smart kontrakt som en avtale mellom 2 eller flere parter som utføres automatisk hvis transaksjonen oppfyller kontraktens gitte krav, uten behovet for en tredjepart (Ertemel, 2019). Blokkjede giganten Ethereum var den første til å utvikle en infrastruktur til å produsere smartkontrakter i blokkjeden. Vitalik Buterin som var med å starte Ethereum påpekte at smartkontrakter var krevende å skrive i Bitcointeknologien. Buterin utviklet dermed en teknologi for å skrive smartkontrakter på en enklere måte, og det var slik Ethereum ble startet. Smartkontrakter har stort sett blitt benyttet i utføring av transaksjoner eller overføring av eiendeler, men kan ha flere andre bruksområder. Når det kommer til datadeling mellom forbruker og annonsører kan smartkontrakter komme godt til nytte. En avtale for datadeling kan inngås mellom begge parter, nemlig at data kun deles med databehandler hvis gitte krav er møtt. Slike kontrakter kan være essensielle for å gi forbrukere bedre kontroll over egen persondata. De kan dermed bestemme hvilke data de deler, når de deler dem, og med hvilke parter. Hva som er best for en forbruker, kan være totalt forskjellig for en annen forbruker. Disse smartkontraktene kan tillate oss å sette våre egne regler, og ikke følge en standard som gjelder alle.

2.6 Sentrale utfordring med blokkjede som personvernløsning

Ettersom flere data skandaler har blitt offentlige, og fler forbrukere har sett omfanget av hvordan store bedrifter bruker og utnytter deres data, har det vokst frem flere bekymringer tilknyttet data og personvern. Mange har derfor begynt å se til blokkjede teknologi som en potensiell løsning på dette problemet, ettersom det ikke er en tredjepart som sitter på kontrollen. Blokkjede teknologien tilbyr sikkerhet og anonymitet for å muliggjøre beskyttelse av vår personlige informasjon. Et sentralt aspekt av personvern i blokkjede er bruken av tilfeldige tall stringer kalt offentlige og private nøkler. Disse nøklene brukes til å identifisere en person i en transaksjon uten å måtte avsløre identiteten. Dette gir potensielle muligheter for blokkjede å sikre personvern og sikkerhet. (Rawal, 2020)

Kombinasjonen av offentlige og private nøkler og hash-funksjonen gjør det mulig å sikre opprinnelsen til en bestemt melding ved å garantere hemmelighold, ekthet og integritet, som også strekker seg til metadataene og dataene i blokkene. Systemet skaper et hash-fingeravtrykk for den aktuelle transaksjonen, som det tildeler et ikke-modifiserbart tidsstempel til. Som et resultat kan dataene som er lagt inn i blokkjeden, så fort validert av nodene, ikke lenger endres eller slettes. Dataene blir registrert på ubestemt tid, og det er ikke mulig å slette disse dataene (Riva 2020).

2.6.1 Artikkel 17: Rett til sletting

Som man fort ser er ikke blokkjede teknologi av natur direkte egnet for å løse spesifikke personvernutfordringer. En av hovedkarakteristikkene til blokkjede er at så fort data/informasjon blir lagret i kjeden, kan den ikke lenger endres eller slettes. Dette er et rammeverk som er i direkte strid med lovdata spesifisert i GDPR, og da særlig Artikkel 17: *Rett til sletting («rett til å bli glemt»).* Loven spesifiserer at: *"den registrerte skal ha rett til å få personopplysninger om seg selv slettet av den behandlingsansvarlige uten ugrunnet opphold under gitte forhold"* (Lovdata, 2021). Som det står nå finnes det ingen gjennomførbar juridisk løsning på dette problemet. Det er viktig å notere at i utvikling av GDPR ble slik disruptiv teknologi som blokkjede ikke tatt til betraktning. Det er derfor nødvendig at det kommer nye regelverk som omfatter data og personvern i blokkjeder, eller at nye blokkjedetjenester tilpasser seg regelverket og kommer med potensielle løsninger. (Riva, 2020).

2.6.2 Artikkel 16: Rett til retting

En av de første problemene angående personvern er muligheten til å endre uriktig persondata. Artikkel 16 i GDPR spesifiserer at : *Den registrerte skal ha rett til å få uriktige personopplysninger om seg selv rettet av den behandlingsansvarlige uten ugrunnet opphold.* (Lovdata, 2021). Teknisk sett, i blokkjede-arkitektur, er dette bare mulig ved å endre den siste blokken som inneholder feilen. Denne prosedyren endrer imidlertid ikke de forrige blokkene, noe som betyr at feil informasjon forblir i settet med gamle blokker i kjeden uten mulighet til å slette eller endre denne informasjonen. For å endre alle blokkene i kjeden som inneholder feilinformasjon, ville det være nødvendig med full kontroll over flertallet av nodene i nettverket, sammen med den tilhørende beregningskapasiteten som kreves for å endre alle blokkene. Derfor, hvis blokkjede følger den typiske distribuerte arkitekturen, er det ikke praktisk gjennomførbart eller økonomisk levedyktig. Dette viser både styrken og svakheten til blokkjede, da det sikrer både en permanent ikke-modifiserbar logg, men ikke en fleksibel metode for å oppdatere informasjonen i blokkene samtidig (Riva, 2020).

2.6.3 Fullstendig gjennomsiktighet

En av de store fordelene med blokkjeder er at de tilbyr fullstendig gjennomsiktighet. Det betyr at enhver node i nettverket kan se innholdet i alle blokkene. Selv om data kan være anonymisert, vil det fortsatt være mulig for noder å se gjennom data på kjeden. Dette er selvfølgelig ikke optimalt når det er snakk om sensitiv persondata. Fra et juridisk perspektiv fungerer derfor blokkjeder essensielt som et offentlig kommersielt register, der alle har muligheten til å hente ut informasjon anonymt (Pollicino and De Gregorio, 2017). Denne ukontrollerte og anonyme tilgjengeligheten utgjør en av hovedtruslene mot individuell personvern fordi det fører til at sensitiv informasjon kan spres offentlig. (Riva, 2020). Lukkede (private) blokkjeder kan i teorien løse dette problemet, ved å kun gi tilgang til autoriserte noder i nettverket. I tilfelle med for eksempel en digital helsetjeneste kan blokkjeden lagre sensitiv data som pasientjournaler, og gi tilgang kun til autorisert helsepersonell. Det oppstår allikevel en etisk problemstilling. Når det er en sentral autoritet som sitter på kontrollen av flertallet av nodene i nettverket, vil de ha muligheten til å kunne modifisere og endre data lagret i blokkene.

2.6.4 Den ansvarlige part

Den klassiske blockchain-distribusjonens karakter tillater imidlertid ikke at den registrerte kan håndheve sine rettigheter, da det ikke er noen behandlingsansvarlig som personvernforespørsler kan sendes til. Det vil si at det er ingen juridisk ansvarlig part eller representant som kan behandle individuelle forespørsler, ettersom kjeden av natur er offentlig og uten en direkte eier (Riva, 2020). Flere studier har påpekt dette problemet. At det er nødvendig for en juridisk enhet å kunne bestemme hvem som er ansvarlig for et bestemt blokkjede nettverk. Dette betyr at alle blokkjeder som oppbevarer eller behandler persondata vil være avhengig av en ansvarlig tredjepart i posisjonen som en datakontroller og databehandler. Denne databehandleren vil i gjengjeld være ansvarlig for validiteten til persondata som er introdusert til kjeden for at blokkjede nettverket skal kunne samsvare med betingelser klarert i GDPR.

2.6.5 Data controller og Data processor

Det er viktig å kunne identifisere og skille mellom disse to rollene når det kommer til behandling av persondata. Dette er fordi de respektive rollene ikke har de samme gradene av ansvar når det kommer til behandling og håndtering av persondata.

En "Data controller" kan defineres slik: *"a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed"* (Ico, 2021).

En "Data processor" i relasjon til personlig data derimot defineres slik: *"any person (other than an employee of the data controller) who processes the data on behalf of the data controller."* (Ico, 2021).

Dette betyr at hvis en blokkjede skal kunne oppbevare persondata er det nødvendig å tilskrive en ansvarlig tredjepart som rollen av datakontrolleren (Riva, 2020). Buocz, et al spesifiserer også at en offentlig distribuert blokkjede innebærer at ingen av GDPR sine regler om ansvarlighet kan utfylles grunnet den diffuse naturen av "distributed ledgers" og dens anonyme tilgjengelighet (Buocz, et al, 2019). På den andre siden hvis nodene i nettverket ikke hadde vært anonyme kunne de blitt klassifisert som "data processors", men ettersom det ikke finnes noen "data controller", er det ingen ansvarlig entitet som kan delegere denne prosessor rollen. Så hvis det ikke finnes noen "data controller", så er det heller ingen part som

kan bestemme“data processor” rollen.

Uavhengig av hvor vanskelig det kan være å identifisere disse rollene som “controller”, og “processor”, så er det helt nødvendig hvis blokkjeder skal kunne utfylle de juridiske kravene om ansvarlige entiteter når det kommer til lagring og behandling av personlig data. Som det står i dag er det ingen direkte løsning på dette problemet, men det er allikevel mange som jobber med løsninger som jobber rundt disse problemene.

2.7 Bruke blokkjede for å beskytte persondata

Kontroll

Forskning har gjentatte ganger vist at forbrukere bekymrer seg for deres transaksjoners anonymitet og konfidensialitet på nett (Ratnasingham, 1998). Disse bekymringene stammer mye fra den økte risikoen knyttet til selskapers innsamling, misbruk, og spredning av personlig informasjon. Personvern bekymringer har fortsatt å øke ettersom nettside “cookies” har gjort det lettere å både samle inn og lagre personopplysninger. (McParland and Connolly, 2007). Store forbedringer innen datainnsamlingsteknikker har gjort det lettere for selskaper å identifisere, spore, samle, og prosessere forbrukeres personlige informasjon. Dette har i gjengjeld ført til at forbrukere oppfatter kommunikasjon på nett som mer påtrengende enn noen gang før (Rejeb, 2020). En studie gjennomført av Harris Poll viser at forbruker har et sterkt behov for kontroll av deres personlige informasjon. Studien viste at 87% av respondentene valgte å beskytte deres personlige informasjon ved å forespørre trekk av personlig informasjon fra selskapers databaser (Harris Poll, 2004).

Ettersom forbrukeres behov for beskyttelse av personlig informasjon stadig øker, kan blokkjeder være en sentral brikke i utviklingen av systemer som øker forbrukerens kontroll. Forbrukeres personlige informasjon kan beskyttes i stor grad på blokkjeder. Dette kan gjøres med flere ulike teknikker og mekanismer bygget inn blokkjedene. En av de viktige mekanismene blokkjeder tilbyr er muligheten til å kryptere informasjon. Dette hindrer at informasjon deres kan bli benyttet som en handelsvare av ikke ønskelige parter (Rejeb, 2020). Videre som diskutert i kapittelet om smartkontrakter har brukere også muligheten til å sette egne regler for distribusjon av deres data. På denne måten kan kontrollen over egne opplysninger gis tilbake til forbrukeren. Det har også ved hjelp av blokkjedeløsninger som

Wibson, og Brave vokst frem muligheter for forbrukere å byttehandle deres data med selskaper som vil ha nytte av den.

Kontrollen over personopplysninger, og sensitive data generelt sett, burde ikke ligge i hendene til tredjeparter, der de er utsatt for angrep og misbruk. I stedet bør brukerne eie og kontrollere deres egen data uten at det går på bekostning av sikkerheten, og samtidig ikke fjerner muligheten for selskapers mulighet til å tilby personaliserte tjenester. Bedrifter kan i gjengjeld fokusere på å bruke data uten å være altfor bekymret for riktig sikring, lagring og distribuering av data.

Flere innovative selskaper jobber for øyeblikket med blokkjede baserte løsninger på disse utfordringer. The Enigma Project ledet av MIT setter ut for å løse disse utfordringene. Teamet i Enigma har utviklet "The Secret Network", som er en "open-source" blokkjede, som tillater desentraliserte tjenester å lage personvern-fokuserte smartkontrakter for håndtering av sensitiv data. Applikasjoner bygget på Secret Network bruker en protokoll med 2 lag av kryptering. Dette betyr at nodene i nettverket kan behandle kryptert data uten at dataen blir avslørt for nodene. Problemet vi ofte ser ved å gi tilgang til data i dag, er at selskaper som Facebook og Google har muligheten til å selge denne informasjonen videre til andre selskaper. The Secret Network fjerner denne muligheten for redistribusjon av persondata, ettersom data aldri blir avslørt for nodene. De får kun en midlertidig mulighet til å behandle kryptert data, uten å faktisk vite hva denne dataen er. Dette gjøres altså ved bruk av krypterte inputs og outputs, samt ved hjelp av hemmelige smartkontrakter (Secret Network, 2020).

3.0 Metode.

Her skal vi ta for oss hva slags metode vi har brukt for å svare på problemstillingen vår:

> "*Hva er den potensielle innvirkningen av blokkjede teknologi på bruk og innsamling av data".*

For dette forskningsprosjektet har vi sett det mest hensiktsmessig å benytte oss av kvalitativ metode. Gjennom denne seksjonen skal vi begrunne hvorfor vi har valgt denne metoden, og hvordan vi har brukt den for å besvare vår problemstilling.

Kvalitative metoder har den egenskapen at man kan gå i dybden for å forstå. Man kan si at kvalitative metoder har sin styrke når det gjelder spørsmål av typen "hva, hvorfor og hvordan?" (Gripsrud, Olsson og Silkoset 2016, s. 103). Det å ta en kvalitativ tilnærming egnes til forskning som er i en tidlig fase i teoriutvikling, og når nye begreper eller fenomener skal utvikles, og det er høy kompleksitet. Blokkjede teknologi innenfor datainnsamling og bruk er i en tidlig fase av dets potensiale, og i forhold til hvor mange som sitter med en god dybdeforståelse av temaet. Vi ønsker derfor ved hjelp av kvalitative metoder å få et dypere innblikk i blokkjede sin potensielle innvirkning på datainnsamling og bruk.

I økende grad blir kvalitativ forskningen sett på som en sterk og givende metode for å få et innblikk i hvordan temaer fungerer i praksis. Vi er ute etter en dypere forståelse av blockchain ved å bruke andres erfaringer. Kvalitativ forskning har fått en del kritikk for å være tidskonsumerende (Vaivio, 2008), men i et slikt prosjekt som dette hvor det er såpass høy kompleksitet i teknologien og forståelsen rundt den og problemstillingen vi skal ha svar på er innenfor et forholdsvis nytt tema med lite tidligere forskning, ser vi det hensiktsmessig å benytte oss av dybdeintervjuer.

3.1 Kvalitative intervjuer

Intervju er primært en datainnsamlingsmetode brukt i kvalitativ forskning. Det er som regel en omfattende og tidkrevende prosess, som krever mye oppmerksomhet og mye forberedelser. Savin-Baden og Major har delt inn de kvalitative intervjuene i fire ulike varianter. Strukturerte, semistrukturerte, ustrukturerte og uformelle intervjuer (Savin-Baden & Major, 2013). I vår forskningsprosess kommer vi til å benytte oss av semistrukturerte intervjuer.

Gjennom et semistrukturert intervju vil vi ha friere tøyler rundt spørsmålene vi stiller. Vi har en satt intervjuguide, og målet er å få dekket alle spørsmålene i en gitt rekkefølge. Men det vil være en lettere flyt i samtalen, med oppfølgingsspørsmål og kommentarer. Fordelene med semistrukturerte intervjuer er at intervjuer kan sørge for at fokuset blir spisset inn og

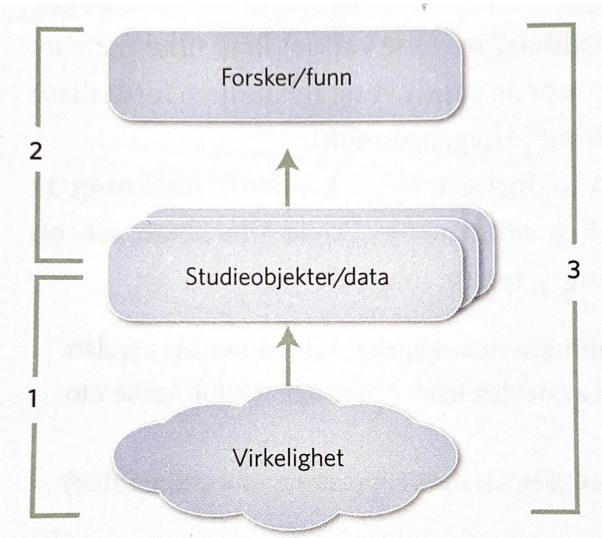
kontinuerlig holder seg innenfor tema. Det vil da også bli muligheter for å analysere intervjuobjektene sine svar basert på tema (Savin-Baden & Major, 2013). Dette gir oss en mulighet til å fordype oss i utvalget, og hva de sitter på av kunnskap. En nedside av dette er at det blir vanskeligere å analysere svar, da det ikke er like direkte sammenligninger. Vi har derfor valgt å begrense oss til 5 intervjuobjekter, da det er en omfattende og tidkrevende prosess å analysere intervjuene.

3.2 Reliabilitet og validitet

Reliabilitet også kalt pålitelighet går ut på i hvilken grad studien kan etterprøves. I dette spørsmålet ligger det også en anerkjennelse av at undersøkelsesopplegget, datainnsamlingen og analysen kan påvirke resultatet. Alle undersøkelser med unntak av de som holdes skjult for de som blir undersøkt, vil utsette undersøkelses objektene for stimuli og signaler. Informantene som intervjues blir påvirket av intervjuet, og intervju forholdene (Jacobsen 2018, s. 241). Det er viktig at informantene er i en naturlig setting som ikke endrer holdningene deres, da dette kan påvirke resultatet og gi feilaktige svar (Jacobsen 2018, s. 242).

Validitet også kalt intern gyldighet går ut på om resultatene oppfattes som riktig. Hvorvidt noe er riktig eller feil avhenger av mange forhold, men det viktigste er om beskrivelsen er sanne, og om sammenhengene er reelle. Ved en pragmatisk tilnærming stiller man spørsmål

om i hvilke grad det samsvar mellom virkeligheten og forskerens beskrivelse, og dette kaller vi for validering (Jacobsen 2018, s. 228). Illustrert i **figur 3:**



Figur 11.1 Validering som relasjon mellom tre nivåer

Et viktig spørsmål innen validitet er "gir studieobjektene en sann representasjon av virkeligheten?". Mats alvesson (2011) er en sterk kritiker av det han kaller en naiv holdning mange forskere har til kvalitativ datainnsamling, og spesielt med tanke på intervjuer. Han hevder at for mange forskere tar det for gitt at menneskene de intervjuer forteller sannheten, og da den reelle virkeligheten. Dette mener han er feil, fordi mennesker verken kan eller vil avsløre virkeligheten (Jacobsen 2018, s. 229). Dette er noen essensielle spørsmål man bør stille seg selv for å kontrollere validitet:

- Har vi fått tak i de riktige kildene?
- Gir kildene riktig informasjon?
- Hvordan kommer informasjonen frem?
- Gir forskerne en sann representasjon av data?

(Jacobsen 2018, s. 229-233).

Når man skal gjennomføre intervjuer er det viktig å hindre store ringvirkninger den potensielle effekten av intervjue kan ha på informanten. Dette oppnås med å trå frem varsomt å tenke seg nøye om rundt hvordan man skal gjennomføre intervjuet, og bevissthet rundt effekten ledende spørsmål kan ha. Ikke alle som godtar å være med i et intervju har en interesse av å bli påvirket, eller at samfunn skal få en forandring. Derfor er det viktig at

forskerne har fokus på hva som er av verdi når det er til forskningsprosjekter (Brinkmann 2013, s. 80; Golafshani 2013, s. 598)

For å gi informantene mulighet til å utdype om eventuelle saker de mener er relevant opp mot spørsmålene vi stiller, har vi lagt inn åpne spørsmål innenfor temaene våre så informantene kan snakke fritt om ønskelig (Seidmann 2005, s.86). Vi ga de en kopi av transkriberingene våre slik at kunne se over, redigere og bekrefte at informasjonen vi har skrevet ned stemmer overens med deres synspunkter. Dette er med på å øke reliabiliteten til intervjuene (Carlson 2010, s. 1105). Målet med validitet er at dataen vi henter inn er av direkte nytte og gyldig for det vi ønsker å finne ut (Gripsrud, Olsson og Silkoset 2016, s. 72).

Etter Brinkmanns anbefalinger har vi valgt å inkludere refleksjoner om reliabilitet og validitet i metoden (Brinkmann 2013, s. 146). På bakgrunn av teorien vi har undersøkt har vi valgt å benytte oss av følgende tiltak som vi mener bidrar til å stryke reliabilitet og validiteten. Vi har derfor gått for å stille ikke ledende spørsmål, og hvis det er spørsmål informantene ikke er komfortable med å svare på så har vi sagt klart i fra om at man ikke må svare på alt. Dette er for å sikre kvaliteten på svarene, slik at det ikke blir overfladisk refleksjon fra informantene. Vi har også prøvd å kontrollere omgivelsene slik at det blir naturlige settinger og at det er et åpent felt for diskusjon innenfor temaene våre. Og som tidligere nevnt at informantene har fått mulighet til å se over transkripsjonene fra intervjuene deres. Vi har også laget en intervjuguide og valgt utvalg basert på teori. Dette vil vi presentere nærmere videre i oppgaven.

3.3 Intervjuguide

Vi har laget en intervjuguide som vi har tatt utgangspunkt i. For å ende opp med gode og dekkende spørsmål begynte vi tidlig med å utforme et utkast til intervjuguiden (Andersen og Krumsvik 2017, s. 81). Vi tok utgangspunkt i teorien fra validitet og reliabilitet for å oppnå godt formulerte spørsmål som er åpne for diskusjon innen temaene vi er inne på.
Vi ble enige på forhånd at én av oss sto for å være intervjuer, og stilte dermed alle spørsmål og styrte intervjuet. Mens den andre sa minst mulig, transkriberte primært og stilte bare spørsmål hvis noe var uklart. Dette var for at intervjuet skulle bli ryddig organisert, og at man fikk mest mulig utbytte av transkriberingen.

3.4 Utvalg

I dette forskningsprosjektet har vi valgt å danne utvalget basert på forventinger om kunnskap informantene kan dele med oss, dette kalles et informasjonsorientert utvalg (Brinkmann 2013, s. 57). Kravene vi hadde til informantene var at de hadde god kunnskap om blokkjede, data og personvern eller begge deler. Da denne oppgaven har et eksplorativt forskningsdesign har vi prøvd å finne gode og relevante informanter for å oppnå mest mulig innsikt i deres tanker og ideer. For at vi kunne oppnå et bra datagrunnlag til analysen valgte vi å se på bakgrunnen (stillingstittel, bedrift, prosjekter) til vedkommende. Dette var for å unngå at vi bare intervjuet folk med samme bakgrunn, da vi kunne ha risikert å sitte igjen med litt for homogene svar.

Vi begynte med å sende ut mail til personer vi tenkte var aktuelle, og som kunne sitte på god kunnskap om blokkjede. Vi benyttet også linkedin for å finne gode kandidater, og videre den såkalte "snøballeffekten", ved å gå gjennom de aktuelles nettverk og bekjentskaper (Andersen og Krumsvik 2017, s. 81). Mailen/meldingen vi sendte ut var nøye formulert, og med hensikt om å vekke interesse hos mottakerne. Det er som oftest foretrukket å utføre færre, men grundige intervjuer fremfor mange enkle intervjuer. Vi har også bestemt utvalg basert på tidsperspektivet vårt som tidligere nevnt i oppgaven. Utvalget vårt består da av fem informanter med ulik bakgrunn og erfaringer med blokkjede (Brinkmann 2013, s. 59).

3.4.1 Tilstrekkelighet og Metning

Dette er to viktige faktorer å se på når man skal vurdere hvor mange intervjuobjekter som er hensiktsmessige for det gitte prosjekt. Tilstrekkelighet går ut på at man intervjuer nok mennesker til at personer som ikke er en del av utvalget kan gjenkjenne opplevelser og erfaringer som kommer frem. (Brinkmann 2013, s. 58). Metning oppnås ved punktet i prosessen hvor flere intervjuer ikke vil gi noe ny essensiell informasjon for prosjektet ditt (Glaser og Strauss 1999, s. 61).

Informant 1 - Front-end og blockchain utvikler
Informant 2 - College professor, underviser blockchain
Informant 3 - IT konsulent, utvikle IT-tjenester
Informant 4 - Regnskapskonsulent
Informant 5 - Digital markedsfører

3.5 Etiske handlinger

Når man skal forske på personer er det en del etiske krav forskerne må forholde seg til. Gjennom denne seksjonen skal vi forklare våre roller som forskere i henhold til etiske handlinger. Loven om forskningsetikk er slik: *"Loven skal bidra til at forsking i offentlig og privat regi skjer i henhold til anerkjente forskningsetiske normer"* (Forskningsetikkloven, 2006, §1).

Forskere har en plikt om å tenke nøye gjennom hvordan forskningen kan påvirke de det forskes på, og hvordan forskningen vil oppfattes og bli brukt. Vi som forskere kan være med på å påvirke studien etter våre personlige egenskaper, og derfor følger det med en grad av ansvar under forskningen (Jacobsen 2018, s. 45). Hva slags type spørsmål som blir stilt, vinkling og formulering er avhengig av forskeren. Som forsker må man alltid ta hensyn i forhold til hendelser som kan oppstå underveis. Da det er flere utfordringer ved kvalitativ forskning så må forskerne være selvkritiske. Som forsker kan man være bias, noe som medfører mindre tillit til dataene samlet inn. Å ha et kritisk syn gjennom hele prosessen bidrar med å redusere risikoen for bias (Johnson, 1997). Utvalget vårt består av dyktige fagpersoner, samtidig som vi to har vært kritiske til hverandres oppfatninger og tolkninger, for å minske denne risikoen .

Før hvert intervju har vi informert om hensikten bak intervjuet og hva forskningsprosjektet omhandler. Vi har sendt informasjonsskrivet (se vedlegg 2), og her står det beskrevet hva det går ut på, problemstilling, anonymisering og transkribering. Dette er for at informantene skal ha kontroll og forståelse for hva de deltar på.

4.0 Analyse

4.1 Datasortering:

I denne seksjonen skal vi presentere vår fremgangsmåte for både tolking og analyse av data. Etter datainnsamlingsprosessen kom vi til punktet for hvordan man effektivt sorterer data for å finne ut av hva som kan brukes og hva som må forkastes. I følge Savin-Baden og Major (2013) er de vanligste utgangspunktene for analyse av kvalitativ data: karakterisering, koding, kutting, kategorisering, konvertering og oppretting. (Savin-Baden og Major, 2013, s. 219).

Alle intervjuene ble transkribert samtidig som intervjuene tok sted, og vi endte med mye rådata. Det var derfor nødvendig for oss å karakterisere data som var mest relevant for vår studie. Vi begynte med å lese gjennom transkriberingene våre gjentatte ganger for å få en bedre forståelse for data som skulle analyseres. Videre når vi leste gjennom kuttet vi ut informasjon som ikke var relevant for vår studie og lagde fargekoder for informasjon som var av interesse. Fargekodene benyttet vi for å kategorisere de ulike temaene vi ønsket undersøke. Vi benyttet oss av "google docs" for å gjennomføre denne prosessen av karakterisering, kutting, koding, kategorisering, og konvertering for dataene før vi gjennomførte analysen. Dette la grunnlag for en mye enklere dataanalyse ettersom vi satt igjen med mer organisert, strukturert og relevant data.

Det finnes flere forskjellige programvarer man kan ta i bruk for å organisere data fra kvantitative undersøkelser. NVIVO 12 er et program vi vurderte å ta i bruk for analyseprosessen, men ettersom ingen av oss har noe erfaring med programmet fra før valgte vi å bruke en løsning vi begge var kjente med. "Google docs", ga oss samtidig muligheten til å utføre alt organiseringsarbeidet vi var ute etter. For koding og kategorisering benyttet vi oss av fargekoder. Hver enkelt kategori ble representert med en tilhørende farge, og relevant tekst ble gitt farger som samsvarte med kategorien vi mente det tilhørte. Til slutt brukte vi fargen rød til å markere alt av sitater. Disse sitatene benyttet vi videre for å bekrefte funn i analysen. Ifølge P. Burnard, Et al, er prosessen for tematisk innholdsanalyse essensielt den samme enten man gjør det manuelt eller ved hjelp av en programvare. Prosessen består av å identifisere temaer og kategorier som regelmessig dukker opp i dataen, for så å organisere et sammendrag av de relevante funnene (P. Burnard, Et al, 2008).

4.2 Funn

I denne delen av oppgaven ønsker vi å analysere datamaterialet vi har samlet inn og presentere våre funn. Deretter ønsker vi å besvare oppgavens problemstilling ved å ta utgangspunkt i disse hovedkategoriene.

- ***Blokkjedes datapotensiale: gjennomsiktighet, kontroll, og datasystem.***
- ***Blokkjedes datautfordringer: Tilgjengelig, sletting/retting, og ansvarlig part.***

- ***Blokkjede - Veien videre: Bedrifters nytte, De store aktørene, regulatoriske endringer.***

Ifølge P. Burnard, Et al, er det flere enkle fremgangsmåter for å presentere funn i kvalitativ forskning. Den første metoden er rett å slett å rapportere hovedfunnene under hvert tema eller kategori, ved bruk av relevante ordrette sitater for å illustrere funnene. (P. Burnard, Et al, 2008).

Funnene fra intervjuene vil bli kategorisert under det tilhørende temaet under hver hovedkategori. Når flere av respondenten mener det samme, vil vi vektlegge disse utsagnene mer og trekke frem sitatene som forklarer meningen på best måte. Under sitatene vil vi undersøke og forklare meningen til respondenten i mer detalj, i henhold til relevant teori. Hvis det er eventuelle begrensninger ved forskningsspørsmålet vil dette også bli presentert under. Etter vi har presentert alle funnene våre, vil vi ha et avsnitt med diskusjon og oppsummering av hvert hovedtema, og samtidig knytte disse opp mot relevant teori.

4.3 Respondenter

Vi har laget en tabell over de 5 respondentene som har blitt intervjuet under. Respondentene vil holdes anonyme, og vi har tildelt hver respondent et nummer, som de vil bli referert til i avhandlingen. Vi har også valgt å kategorisere respondenter etter bakgrunn, samtidig som vi tilfører en kommentar som beskriver kunnskapsnivået de har. I kommentaren vil det også forstås hvorfor de respektive respondentene er interessante å se på for vår forskning.

Respondenter	Bakgrunn/bransje	Kommentar
Respondent 1	Innovasjonsstudio	Grunnleggende kompetanse med blokkjede.
Respondent 2	Professor	Veldig god kompetanse med blokkjede.
Respondent 3	Teknologiselskap	God kompetanse med blokkjede. Har jobbet med prototyping av blokkjede løsninger
Respondent 4	Regnskap	God kunnskap, men mindre teknologisk kompetanse.
Respondent 5	Markedsførings konsulent	Veldig god kompetanse med blokkjede, men ingen praktisk erfaring

Figur 4 – Skjermdump fra Excel

4.4 Blokkjedes datautfordringer

Flere teknologientusister har sett til blokkjedeteknologi som en potensiell løsning for utfordringer vi møter med den stadige digitaliseringen av det moderne samfunn. En av de sentrale utfordringene vi har sett som særlig relaterer til vårt studie er måten vi i dag samler og bruker data på. Som diskutert i teoridelen, blir mer og mer av våre handlinger på nett sporet og lagret, ofte uvitende for forbrukere. Vi har i denne oppgaven satt ut for å utforske hvordan blokkjede teknologien kan benyttes som en alternativ løsning, som kan gi mer gjennomsiktighet og kontroll tilbake til forbrukerne. Det er likevel store utfordringer denne teknologiske infrastrukturen har møtt på når det kommer til lagring og behandling av data i henhold til reguleringer spesifisert i GDPR. Som diskutert i teorikapittel er det tre sentrale problemstillinger vi har møtt på ved bruk av blokkjede teknologi og ivaretakelse av personvernsrettigheter. Disse er tilgjengelighet, sletting/retting, og den ansvarlige part. Gjennom intervjuene har vi diskutert disse utfordringene, og hva som kan være en potensiell løsning på disse problemene. Vi vil under presentere hvert tema, og funnene fra intervjuene våre på hva som vil være den aktuelle løsningen.

4.4.1 Tilgjengelighet.

Som diskutert i teorikapittelet tilbyr blokkjeder fullstendig gjennomsiktighet for alle nodene i nettverket. Denne ukontrollerte og anonyme tilgjengeligheten utgjør en av hoved truslene mot individuell personvern fordi det fører til at sensitiv informasjon kan spres offentlig. (Riva, 2020). Gjennom intervjuene ønsket vi å utforske denne problemstillingen og hva som eventuelt kunne være en løsning.

Det er et enstemmig konsensus blant deltakerne at dette stemmer for offentlige/åpne blokkjeder. I private/lukkede blokkjeder derimot kan kun autoriserte noder i nettverket få tilgang til informasjonen. Det kan derfor virke som at den naturlige konklusjonen vil være å kun oppbevare sensitiv data på private kjeder. Informant nummer 2 spesifiserer derimot at private blokkjeder ofte blir for like vanlige databaser.

> *"I think that the deal with private chains is that they're a little bit too close to just databases. And is it worth the expense of a Blockchain to use a private chain."*

Flere av informantene poengterer også at sensitiv data ikke nødvendigvis er egnet til å ligge tilgjengelig på en kjede, men at vi heller må utforske løsninger som kombinerer blokkjede

mekanismer for innhenting og behandling av data sammen med eksterne databaser.

Informant 2 og 3 foreslår begge en lignende løsning hvor man kombinerer blokkjede mekanismer for innhenting og behandling av data, mens selve lagringen skjer på en ekstern database.

> Informant 2: "*I think in the long run, the way it's going to be set up is that each person sort of has like a private server of some sort which maybe you're hiring a company that you trust for that private server. (...) and the Blockchain is really more the gatekeeper for access to that server. I think that's going to be a model that We'll see 10 years from now."*

> Informant 3: *"man kan utforske et design som kombinerer både blockchain med database lagring. Så for eksempel kan du sette opp en kontrakt som henter ut kryptert data fra en database, under gitte forhold. Men persondata i seg selv burde ikke oppbevares kjeden."*

Informant nummer 5 foreslår også en løsning som tar utgangspunkt i krypteringsmekanismer med offentlige og private nøkler. På denne måten kan man sikre at informasjon kun er tilgjengelig for autoriserte parter.

> *"Den store løsningen vil ligge i krypteringer, og private og offentlige krypteringsnøkler. På denne måten kan vi sikre at sensitiv informasjon kun er tilgjengelig for spesifikke personer eller selskaper."*

Informanten spesifiserer også at sensitiv data ikke er egnet til å oppbevares på blokkjeden, men at vi heller må sette klare forhåndsregler for hva som kan ligge på kjeden og ikke.

> *"Vi må sette klare regler for hva som kan legges til og hva som ikke kan legges til, og heller bruke en ekstern database for oppbevaringen av mer sensitive opplysninger."*

4.4.2 Sletting/retting

I teorikapittelet diskuterte vi artikkel 16 og 17 fra GDPR, som spesifiserer at enhver registrert skal ha muligheten til å trekke informasjon, og/eller endre feilaktig informasjon. En av

hovedkarakteristikkene til blokkjeder er derimot at så fort data blir lagt til i kjeden, kan den ikke lenger slettes eller endres. Den kan kun oppdateres ved å legge til en ny blokk. Dette er også en av de sentrale utfordringene med blokkjeder, når det kommer til oppbevaring av personinformasjon. Gjennom intervjuene ønsket vi å høre synspunkt på denne problemstillingen og hva som kunne være en potensiell løsning.

Alle informantene diskuterer seg frem til at sensitive personopplysninger ikke er egnet til å ligge på en blokkjede. Informant 2 spesifiserer at dette rett og slett er for risikabelt:

> *"It's out there forever. So the risk of that I think is just too high for that to be the way Blockchain is used."*

Informant 1 konkluderer også med at løsningen vil ligge i å kombinere blokkjeder med en ekstern database, som også tar utgangspunkt i krypteringsmekanismer. Informant 1 stiller seg likevel kritisk til dette med å ha en ekstern database, og hvem som skal være ansvarlig for denne.

> *"man hadde typ en nøkkel, så hvis man hadde personnummer så var det ID som var linket til en database. Så uten den ID'en ga ikke dataen noe mening. Men så igjen blir det enda en database og holde styr på, også kan man diskutere hvor desentralisert det er, og hvem er det som skal være ansvarlig for den databasen."*

4.4.3 Den ansvarlige part

Den siste store utfordringen vi diskuterte i teorikapittelet er behovet for en ansvarlig entitet. Ettersom en åpen blokkjede ikke har noen ansvarlig part, men er kontrollert og regulert av nodene i nettverket finnes det ingen enkelt entitet å holde ansvarlig for brudd på personvern. Det er altså ingen juridisk ansvarlig part eller representant som kan behandle individuelle forespørsler om trekk eller endring av data (Riva, 2020). Gjennom intervjuene diskuterte vi behovet for en ansvarlig part, og behovet for å identifisere de ulike datarollene, og hva som eventuelt kan være en løsning.

Alle informantene er godt kjente med GDPR, og behovet for en ansvarlig part for behandling av personlig data.

> *Informant 3: "med tanke på lover og regler vil man jo måtte ha en person eller bedrift å holde ansvarlig hvis det skjer uventede lovbrudd."*

> *Informant 4: "Men for at datahåndtering sånn som lovbildet ser ut i dag skal fungere med GDPR, må det være en tredjepart ja som har ansvar for at dataen blir behandlet riktig".*

Informantene hadde likevel litt forskjellig forslag på hvordan vi kunne identifisere disse ansvarlige entitetene, og hva som ville være den naturlige løsningen på dette problemet. Informant 5 trekker frem mulighetene for å selv velge sin egne ansvarlige entitet som lagrer data på en ekstern database.

> *"Jeg tror rett og slett vi må finne en løsning hvor hver person velger sin ansvarlige part for deres data, på en annen ekstern database. Også kan vi bruke blokkjeden som en mekanisme for å hente denne dataen, og distribuere til de rette mottakerne. "*

Dette er teoretisk sett en god løsning som tar hensyn til reguleringene fra GDPR. Basert på denne modellen vil vi kunne identifisere denne tredjeparten som "data controller". Dette selskapet kan da altså spesifisere alle regler for hvordan persondata skal håndteres og brukes sammen med brukeren, og kunne stilles ansvarlig for eventuelle brudd. Denne dataen kan da videredistribueres til andre selskaper i kjeden som vil ha nytte av den under gitte vilkår. Disse selskapene som henter ut data fyller da rollen som "data processor". Vi har dermed en mulighet til å kunne identifisere begge rollene "controller", og "processor".

Informant 2 trekker også frem at det kommer til å være ulike modeller for hvem en bruker velger som sin ansvarlig part, ettersom ikke alle stoler like blindt på store selskaper.

> *"Well, so I think it's going to be each individual chooses who they trust for that third party. So some people are fine with a really big company, other people are less trusting and they're going to want something like a cousin that they know or trust. I think there's going to be different models for this third party. It won't be a centralized 3rd party, that I'm sure of."*

4.5 Blokkjedes data potensiale

En av blokkjedes store potensielle fordeler når det kommer til data er muligheten til å vite hvem som har tilgang til dataen din. Dagens dataløsninger har flere problemer, og et av de større som omtalt i teorien er når det forekommer databrudd. Det har dessverre vært flere slike tilfeller hvor de store aktørene og da blant annet Facebook ikke har klart å holde dataene våre trygge. Som har ført til at de har falt i feil hender, og blitt utnyttet til uetiske formål (Rash, 2018). Dette fører til skeptisisme hos forbrukerne, og behovet for nye innovative løsninger er absolutt til stedet. Det er her smartkontrakter kommer inn i bildet. Smartkontrakter er et begrep som brukes til å beskrive datakode som automatisk utfører hele eller deler av en avtale og lagres på en blockchain-basert plattform (*Stuart D. ET al, 2018).* Med denne teknologien får brukeren mulighet til å kontrollere hvem som har tilgang til sin data, og alltid ha oversikt over hvem som eventuelt har hentet ut dataen deres. Dette skal vi gå mer inn på i punktene nedenfor. Gjennom intervjuene har vi forhørt oss om informantenes tanker rundt eventuelle løsninger, og kommer videre til å diskutere funnene fra intervjuene.

4.5.1 Gjennomsiktighet

En av de store fordelene med blokkjeder er at de tilbyr fullstendig gjennomsiktighet. Det betyr at enhver node i nettverket kan se innholdet i alle blokkene (Pollicino and De Gregorio, 2017). Som forsket på i vår teori har vi sett at et av de store problemene med nåværende datainnsamling og bruks løsninger er mangelen på gjennomsiktighet. Brukere har så og si null oversikt over hva slags data som blir samlet inn om de, og spesielt ikke hva de blir brukt til. Ved å ta i bruk en løsning som smartkontrakter kan dette medføre en transparent oversikt over hvem som har samlet inn data på deg, og hva slags prosjekter og formål de har blitt brukt til.

Informant 5 har kommet med innspill fra to sider. Vedkommende snakker om egnet bruk for både forbruker og annonsør, og hvordan det kan gi nytte til begge parter.

> *"Med en blokkjede løsning kan forbrukere enkelt se alle parter som har tilgang til deres data, hvilke data som er registrert av dem, og eventuelt sette egendefinerte regler for deres data."*

> *"Med et blockchain system derimot kan vi totalt fjerne denne "middelmannen", og analysere og validere enhver kundereise som tar plass, som igjen vil gi oss*

> *markedsførere mye mer presis og pålitelig data. Dette kan redusere kostnader, øke annonse effektiviteten, og samtidig gi en mye mer gjennomsiktig løsning for annonsører."*

Informant 4 har et eksempel på en annen måte å benytte seg av gjennomsiktig på ved at folk fra utviklingsland som ikke er registrert i noe databaser får muligheten til dette i en blokkjede for å forhindre misbruk og muligheten til å være en del av et sivilisert samfunn med et register, lån, reising o.l. En slik løsning kan funke da blokkjede er en transparent teknologi, som gjør at det kan funke som et register.

> *"FN driver å tester ut hvordan man få ID på folk i utviklingsland som ikke nødvendigvis er identifiserbare. Dette for å hindre mennesektraffikering, og gi fattigere tilgang på flere tjenester de ikke har den dag i dag. Selv om noe som først er lagt til i en blockchain blir der for alltid, så har det også sine fordeler som i slike scenarioer."*

Informant 1 tar opp bruksområde dette kan ha for supply chains, og hvordan det kan gi oversikt for både bedriftene og kjøperne.

> *"Muligheten til å spore produkter, hvor det kommer fra, mulighet til å dra typ en digital tvilling av ting, sånn at brukerne kan se hvor produktet kommer fra og spore det."*

Informant 2 snakker om hvordan dette kan benyttes av lov systemene for en gjennomsiktig løsning på å avgjøre om en regel har blitt brutt.

> *"So I think getting the legal system to sort of use Blockchain more often and use them as transparent ways of proving that yes you set up these rules and they have violated the rules you set up with. I think that's going to be key."*

4.5.2 Kontroll

Forskning viser at å gi forbrukere mer kontroll over egen data eller i det minste oppfattet kontroll over egen data kan redusere bekymringer relatert til personvern (maholtra et al. 2004; Tucker 2014). Som nevnt i teorien så utviklet to forskere en modell som støttet denne

påstanden med at hvis forbrukere blir informert over nytten og verdien av datainnsamlingen så er de mer villig å til godta det. Brukerne burde ha mulighet til kontrollere egen data uten at det går på bekostning av sikkerhet eller selskapers mulighet til å tilby personaliserte tjenester.

Informant 2, 3 og 4 mente at smartkontrakter var en velegnet løsning på å gi kontroll tilbake til forbrukeren, da man kan sette regler for hvem som har tilgang til dataen, og kun hvis de møter de og de kriteriene. Informant 2 hadde et godt eksempel på hvordan det kan benyttes i helsesektoren:

> Informant 2: *"Let's say you have a rare disease and you want your data to be available to researchers who are researching people like you, it's super private data. You won't put your medical data on a Blockchain but you'll have some sort of smart contract that says okay if people meet these criteria which might be like they have five researchers with a PhD in medicine or Biology or something like that. If they have these, then it can automatically dispense my data to those people"*

> Informant 3: *"Man kan for eksempel sette opp smartkontrakter mellom 2 parter som for eksempel spesifiserer at man vil kun gi fra seg data til aktører som ikke vil lagre det og benytte det i en senere anledning, eller også til kun profesjonelle aktører som har en mastergrad osv, hvis du skjønner."*

> Informant 4: *"Men hvis det skulle vært noe måtte det vel ha blitt en form for løsning ved bruk av smart kontrakter som ga tilgang basert på krav bestemt av eieren av dataen."*

Løsningen Brave ble diskutert med informant 2 og 3. Her diskuterte de hvordan man kan kontrollere hvem som har rettighet til dataene dine og at man kan bruke blokkjede som en måte å forhandle data på. Begge reflekterte at det vil være sånn flere fremtidige løsninger kan se ut.

> Informant 2: *"Who has the right to this private stuff. I can negotiate that. I can sell it on the market. I can use this block team to sort of transact you know, access to my data. I think that absolutely will happen."*

> Informant 3: *“ de kan altså sette opp regler for hvem de vil dele dataen sin med, og motta goder for dataen de gir fra seg.”*

Informant 5 snakker om at blockchain kan funke som en slags åpen markedsplass for salg og kjøp av data. På denne måten løser man problemet med at forbrukerne ikke har kontroll over egen data, samt gir et større utbytte i retur av dataene de deler.

> *“Det er her jeg tror den store løsningen på dette dataproblemet ligger. Nemlig at forbrukerne er de som sitter på makten over deres egen data. (...) Det blir nesten som en åpen markedsplass for kjøp og salg av data, hvor begge parter kan sette sine egne regler for hvordan denne dataen forveksles.”*

4.5.3 Blokkjede som dataløsning

Mye av informantenes svar som omfavner dette temaet er allerede trukket inn i analysen ovenfor, da gjennomsiktighet og kontroll er direkte forbundet med potensielle dataløsninger. Blokkjede teknologi innenfor datainnsamling og bruk er i en tidlig fase av dets potensiale. Vi er i en tid hvor dataverden er moden for nye løsninger. Gjennom denne delen av intervjuet skal vi se på informantenes formeninger rundt fremtidige blokkjede datainnsamlings og bruk løsninger, samt hvordan det kan påvirke sensitiv databehandling.

Informant 2 ser på det som god bruksverdi for et register. Som tidligere nevnt i analysen i forhold til medisinske logger, og ha oversikt over hvem som har tilgang. En annen type løsning var at hver person har en privat server, hvor man selv velger hvem som lagrer data, hvor bare en person eller et selskap du stoler på har tilgang.

> *“I think that's going to be the big early use of Blockchain and security is just keeping accurate records of permissions.“*

Informant 1 og 2 har begge tatt opp hvordan blokkjede kan funke som en nøkkel til dataen i stedet for å oppbevare selve dataen.

> Informant 1:*“man hadde typ en nøkkel, så hvis man hadde personnummer så var det ID som var linket til en database. Så uten den ID’en ga ikke dataen noe mening.”*

> Informant 2: *"I also think there's a possibility that block chains may have information that is not the data itself but it is essentially a key to the data so that it's sort of like all these letters that are stored on the Blockchain when you take that set of data, you can kind of mix it with this other data base two undo information that is truly personal"*

Informant 3 ser for seg en løsning som kombinerer offchain og onchain tjenester, hvor brukerne kan sette forhåndsregler ved hjelp av smartkontrakter.

> *"I teorien må det bli en generell løsning som kombinerer både onchain og offchain tjenester. Vi kan for eksempel ha en desentralisert app hvor brukere kan sette forhåndsregler for deling av deres data, kombinert med en ekstern database som brukeren har full kontroll over."*

Informant 4 poengterer at en egnet dataløsning ved bruk av blokkjede teknologi er en åpen markedsplass for kjøp og salg av data mellom forbruker og bedrift.

> *"det blir som en åpen markedsplass hvor data forhandles mellom forbrukere og bedrifter."*

4.6 Blokkjede veien videre

Det er fortsatt utrolig mye teknologisk innovasjon som må på plass før vi kan se det fulle potensiale av blokkjede teknologi. Tiden har fortsatt mye å vise før vi kan se denne teknologien operere til sitt fulle potensiale. Gjennom denne delen av intervjuet har vi utforsket hvordan blokkjede kommer til å påvirke ulike industrier, hvem som vil ha mest nytte av å ta i bruk denne teknologien, og hvilke endringer som må til før blokkjeder kan integrere seg mer og mer i den digitale utviklingen.

4.6.1 Bedrifters nytte

I denne delen av intervjuene har vi hatt formålet å kartlegge det fremtidige potensiale av blokkjede teknologi. Det er viktig å forstå hvilke bedrifter som vil ha størst utbytte av teknologien, så vi lettere kan predikere fremtiden av blokkjeder. Hvor vil blokkjeder ha størst og mest signifikant påvirkning,

De fleste av informantene er enige i at blokkjeder er en viktig teknologisk kunnskap som vil

være til stor nytte for mange bedrifter. Flere mener allikevel at det ikke er alle bedrifter som vil ha like stort utbytte av å investere i denne teknologien med det første.

> Informant 2: *"I think it depends on the business. I think blockchain is going to kind of infiltrate different industries at different rates."*

> Informant 4: *"Så jeg ser ikke for meg at det blir første prioritet for alle bedrifter og vie så store mengder av tid, penger og ressurser generelt til å ta i bruk blockchain teknologien. Det blir rett og slett for komplekst til at alle bedrifter har tid til å forstå og få bruk for prosessene i dag. "*

> Informant 3: *" Det kommer egentlig helt an på bedriften og hva de driver med. For noen bedrifter vil ikke blockchain være like relevant, mens andre vil kunne ha enorm nytte av det."*

Det kommer også frem fra intervjuene hvilke bedrifter som vil og burde være tidlig ute når det kommer til å integrere blokkjede teknologi før andre. Disse er både økonomi og såkalte "supply chains".

> Informant 2: *"Supply chains are sort of the next wave where blockchain is taking over, where 5 years from now most supply chains will be blockchain based."*

> Informant 5: *"Vi har allerede sett en stor innflytelse av blokkjede teknologi i finans, og det tror jeg bare kommer til å fortsette. Essensielt offentlige systemer hvor informasjon loggføres."*

4.6.2 De store aktørene

Google og Facebook er i dag blant de største datagigantene, og har i nyere tid investert mye ressurser i blokkjede teknologi. Vi ser det derfor som svært hensiktsmessig å undersøke hvordan disse selskapene vil ta i bruk slik teknologi, og hvordan det eventuelt kan påvirke utviklingen.

Informantene er generelt ganske usikre på hvordan teknologien vil anvendes i praksis, men hovedkonklusjonen er at disse selskapene investerer ressurser i blokkjede teknologi som et konkurransefortrinn, rett å slett for å ikke havne bak sine konkurrenter.

> Informant 3: *"hvis denne teknologien kommer for å bli er det nødvendig at de har tilstrekkelig med kunnskap om fagfeltet så de ikke havner bakpå og lar konkurrenter overta dem."*

> Informant 5: *"Jeg tror for Facebook og Google handler alt om å være tidligere ute enn rivalene sine. Du kan rett og slett ikke havne bakpå når det kommer til slik teknologi."*

Informant 5 trekker også frem hvordan Facebook har utviklet sin egen kryptovaluta, som de potensielt kan bruke for å lage blokkjede baserte belønningsintensiver, lignende de åpne data markedsplassene som er diskutert tidligere i analysen.

> *"Facebook blant annet har jo også utviklet sin egen kryptovaluta "Libra", så det er mulig de utforsker blockchain baserte belønning insentiver som tar i bruk Libra."*

4.6.3 Regulatoriske endringer

Med dagens lovverk, og EUs personvernforordning (GDPR) er det vanskelig å få maksimalt utbytte av blokkjedes potensiale. Det er regelverk som er til for å beskytte oss forbrukere, men disse lovene har også en tendens til å henge et stykke bak den teknologiske utviklingen. Vi har derfor valgt å se på informantenes tilnærming til temaet, og hvordan de kan se for seg blokkjedes funksjon med dagens gjeldende lover.

Det er generelt konseus mellom informantenen om at man foreløpig må forholde seg til dagens regelverk, men ideelt sett ønskes det en oppdatering i regelverket for at blokkjede teknologien skal bidra til noe ordentlig stort utbytte.

Informant 1 poengterer at dagens regelverk er til for å beskytte brukerne, og at de ikke burde vike for noen teknologi, og at det heller er opp til selskapene og jobbe rundt disse.

> *"Det er jo viktige regelverk som ikke kan vikes for, for noen teknologi. Da må heller vi som jobber med teknologi finne en måte på hvordan man kan gjøre det, og selskaper teste seg fram."*

Informant 2 nevner at det er problematisk at de regulatoriske systemene ligger såpass langt bak, og at de ideelt sett vil oppdatere seg i samsvar med blokkjede. Vedkommende fortsetter med å si at utviklere må fortsette utviklingen av teknologien med forutsetning om at lovene ikke vil endres på en stund, og at det heller ikke er noe mulighet for de å vite hva slags lover som må integreres for å få systemet til å funke. Vi må akseptere utdaterte lover, å finne en vei rundt.

> *"I think I tend to be more on the side of we kind of have to accept the given laws which are outdated and don't take into account what Blockchain is. Work for a while and then 10 years down the road, the policymakers will catch up."*

> Informant 3: *"Vi har jo fortsatt ikke sett den reelle innvirkningen av blockchain enda, og hvis det ved et senere tidspunkt blir en teknologi som tar helt over er det nødvendig at regelverkene oppdateres til disse nye teknologiene. "*

> Informant 4: *"Ja, slik som lovverket ser ut i dag, og spesielt da i europa med GDPR så må det eventuelt skje en del forandringer før blockchain vil fungere"*

Informant 5 trekker frem at det må skje endringer i regelverket hvis blokkjede skal fortsette å vokse i like stor grad som det har gjort frem til nå, og at folk trenger mer kunnskap rundt teknologien.

> *"Så det må nok gjøres noe arbeid her for å kunne simplifisere denne teknologien så folk flest kan få en bedre forståelse av hvordan det fungerer."*

5.0 Diskusjon

5.1 Blokkjedes data utfordringer

Vi begrenset oss til å se på de 3 utfordringene vi mener er mest sentrale, og som utviklere må ta hensyn til i utviklingen av nye blokkjede løsninger. Disse utfordringene er tilgjengelighet av informasjon, rett til sletting/retting, og den ansvarlige part. Basert på våre funn kan vi oppsummere med at disse vil prege utviklingen av blokkjeder, men at det også finnes ulike fremgangsmåter for å jobbe seg rundt disse.

Som nevnt i teorikapittelet om total gjennomsiktighet er en av hoved truslene mot individuell personvern i blokkjeder den ukontrollerte og anonyme tilgangen blokkjeder tilbyr (Riva 2020). Ifølge funnene våre vil den beste fremgangsmåten være å kombinere blokkjedefunksjoner for distribusjon og deling av data sammen med en ekstern database. Denne type løsning gir fordelen ved at man kan skjerme informasjon fra uønskede parter. Som informant nummer 5 nevner kan dette gjøres ved å kryptere informasjon slik at kun de som har behov kan få dette gjennom en krypteringsnøkkel. Dette kan sees på som en mulig løsning for å løse problemet med den ukontrollerte og anonyme tilgjengeligheten blokkjeder utgjør. Zyskind, et al presenterte også i 2015 en slik løsning i deres forskningsartikkel: "*Decentralizing Privacy: Using Blockchain to Protect Personal Data".* Som spesifisert i artikkelen vil selve dataen lagres på en ekstern database, mens blokkjeden vil oppbevare en krypteringsnøkkel til dataen. På denne måten kan man sikre at informasjon ikke er tilgjengelig for feil parter (Zyskind, Et. al, 2015).

En slik løsning vil også kunne løse problemet med retten til å få informasjon slettet. Det kommer frem fra intervjuene at sensitiv data rett og slett ikke er egnet å oppbevare på en blokkjede. Informant 2 trekker frem at det utfører en for stor risiko å lagre sensitiv data på kjeder, og at vi heller må finne andre løsninger. Å ikke oppbevare de sensitive opplysningen på en kjede fjerner den permanente tilgjengeligheten av informasjon. Ved bruk av en ekstern database vil forbrukere ha muligheten til å slette informasjon om seg selv, samt å korrigere feilaktig detaljer om seg selv. Dette er derfor en løsning som tar hensyn til artikkel 16 og 17 i GDPR, som diskutert i teorikapittelet.

Ved å oppbevare individuelle personopplysninger på en ekstern database kan vi samtidig løse utfordringen om den ansvarlige part. Et slikt system gjør det mulig å identifisere rollene som datacontroller, og dataprocessor. Selskapet som står ansvarlig for den eksterne databasen vil kunne identifiseres som datacontroller, mens selskaper som henter ut og behandler data vil kunne identifiseres som dataprocessor. På denne måten har vi muligheten til å tilskrive ansvarlige parter, slik at vi kan utfylle de juridiske kravene om ansvarlige entiteter. Skulle det skje brudd på personvernrettigheter, så vet vi hvem som skal holdes ansvarlig. Men igjen oppstår da denne debatten om makt og manipulasjon av data. Hvis det igjen er kun én ansvarlig entitet som sitter på makten over denne databasen vil de ha mulighet til å manipulere informasjon. Informant 2 foreslo derfor muligheten for ulike modeller for ansvarlige tredjeparter, enten det er gjennom en bekjent, eller en eventuell koalisjon av ansvarlige parter.

5.2 Blokkjedes data potensiale

Ut i fra funnene i analysekapittelet kan vi se at det er en generell enighet om at blokkjede har mye potensiale innenfor datainnsamling -og bruks universet. Gjennom intervjuene kommer det frem at løsninger kan tilby potensielle muligheter innen kategoriene gjennomsiktighet og kontroll. Til slutt har vi også utforsket informantenes forslag til potensielle dataløsninger. På bakgrunn av funnene våre kan vi sammenfatte at det er mange muligheter for å oppnå mer gjennomsiktighet og kontroll ved å implementere og ta i bruk blokkjede-teknologi i stedet for og i tillegg dagens løsninger.

Som nevnt i teorien har forskning gjentatte ganger vist at forbrukere bekymrer seg for deres transaksjoners anonymitet og konfidensialitet på nett (Ratnasingham, 1998). Gjennom funnene våre ser vi at blokkjeder kan tilby en løsning på dette problemet. En blokkjede løsning kan gi forbrukere bedre oversikt over hvem som har tilgang til deres personlige data, samt hva slags data som er registrert om dem og muligheten til å definere egne regler for bruk av deres data. Dette kan gjøres ved bruk av smartkontrakter som er datakode som automatisk utfører hele eller deler av en avtale og lagres på en blokkjede-basert plattform. (Stuart. ET al, 2018.) Smartkontrakter er der samtlige ser at mye av det fremtidige potensiale knyttet til datahåndtering ligger. Muligheten for forbrukeren å kontrollere hvem som har tilgang på data, og hva slags data som er tilgjengelig basert på forhåndssatte regler anses som en god

fremtidig løsning. En slik løsning vil gi forbrukere gjennomsiktighet over hvem som har tilgang.

På den andre siden gir dette også muligheter for annonsører. Det blir lettere å lage en personalisert kundereise, da forbrukerne selv styrer hva de ønsker å bli eksponert for. Dette bidrar til reduserte kostnader, mer effektiv formidling av budskap, og en helhetlig mer gjennomsiktig løsning for både forbruker og selskaper. Forskning viser at å gi forbrukere mer kontroll over egen data eller i det minste oppfattet kontroll over egen data kan redusere bekymringer relatert til personvern, som i gjengjeld kan styrke forholdet mellom annonsør og forbruker. (Malhotra et al. 2004; Tucker 2014).

Flere av informantene trekker også frem at blokkjeder ved hjelp av smartkontrakter kan skape en åpen markedsplass mellom forbruker og annonsør for kjøp og salg av data. Dette vil i gjengjeld gi kontrollen over data tilbake til forbrukere.

En lignende løsning på denne modellen som allerede eksisterer er nettleseren Brave. Her har man mulighet som forbruker til å kontrollere hvem som har rettighet til dataene dine, og hva slags annonser man ønsker å bli eksponert for. Denne løsningen fungerer i prinsippet likt som smartkontrakter hvor man kan sette opp regler og krav til hvem som får tilgang til dataen din, og man kan også motta goder for å gi fra seg dataen. Dette er en løsning som har hatt stor suksess, og antall brukere vokser betydelig fortløpende. Brave har nå over 25. millioner aktive brukere, og har over doblet antall brukere i løpet av det siste året (Brave, 2021).

5.3 Blokkjede - veien videre

For at blokkjede teknologi skal kunne etablere seg ordentlig innenfor dataverden er det mye teknologisk innovasjon som må på plass. Vi har derfor gjennom denne delen av analysen ønsket å se på potensiale til blokkjeder i en større sammenheng, hvilke industrier som vil bli mest preget av teknologien, og hvilke endringer som må til før blokkjeder kan integreres på tvers av industrier.

Det var generell enighet fra samtlige av informantene om at blokkjede er en viktig ny teknologi som kan være til stor nytte for mange bedrifter. På tross av enighet rundt potensiale, så presiserte noen at det ikke ville være hensiktsmessig for alle bedrifter å

investere store mengder ressurser i denne teknologien med det første. Selv om blokkjede har et bredt bruksområde, er det ikke nødvendigvis mer effektivt enn dagens allerede eksisterende løsninger, og på bakgrunn av dette påpeker flere av informantene at det ikke er lønnsomt for alle bedrifter i dag. Gjennom funnene kom det frem at den økonomiske sektoren og såkalte supply chains er de første som har begynt og burde begynne å investere ressurser i blokkjede.

Google og Facebook er to av de største aktørene innen datainnsamling og bruk. Begge selskapene har allokert mye ressurser til blokkjedeteknologi, og vi ønsket derfor å utforske potensielle bruksområder teknologien ville ha for disse selskapene. Det er generell enighet om at årsaken til at slike selskaper investerer så mye i blokkjede er rett og slett for å ikke havne bak konkurrentene sine når den tid måtte komme. Den ene informanten trekker også frem at Facebook har utviklet sin egen kryptovalua "Libra", som de potensielt kan bruke som belønningsintensiver for deling av data.

Lovene og reglene datainnsamling og bruk må forholde seg til i dag gir svært lite rom for blokkjedes fremtidige utvikling. Informantene har en generell konsensus om at man må forholde seg til lovene slik som er ettersom de er ment for å ivareta forbrukernes rettigheter. Problematikken er at lovene har en tendens til å henge langt bak den teknologiske utviklingen, og i blokkjedes tilfelle er det på et punkt hvor det betydelig sakker ned progresjonen. Ideelt sett hadde lovverket oppdatert seg i samsvar med blockchain, men det er ikke tilfelle. Det trekkes frem at de som jobber med blokkjede i dag heller må finne måter å jobbe rundt eksisterende regelverk på, da det vil da en god stund før det skjer store nok endringer i lovverket til optimal ytelse. Etterhvert som regelverk oppdateres kan lover og regler programmeres direkte inn i blokkjeden, slik at de utføres automatisk. (Zyskind, Nathan, Pentland, 2015). Dette kan i gjengjeld fjerne muligheten for bedrifter å begå brudd på regelverk, ettersom de ikke har mulighetene til å operere utenfor regelverkene som er programmert inn i kjeden.

6.0 Konklusjon

I dette kapittelet kommer vi med konklusjoner for avhandlingen vår. Vi ønsker også å sette disse inn i en større sammenheng, og se på de teoretiske og praktiske implikasjonene for

avhandlingen vår. Til slutt vil vi også presentere begrensninger og anbefalinger til videre forskning. Denne oppgaven søkte etter å svare på problemstillingen:

> ***"Hva er den potensielle innvirkningen av blokkjede teknologi på bruk og innsamling av data".***

Svaret kan oppsummeres kort med at blokkjeder vil ha en positiv påvirkning på bruk og innsamling av data, ved å gi mer gjennomsiktighet og kontroll til både forbrukere og databehandlere. Blokkjede teknologien har også muligheten til å levere mer presis og kontrollerbar data til både forbrukere og databehandlere, og samtidig skape en åpen markedsplass for distribusjon av data som kan styrke forholdet mellom databehandler og forbruker. Forskningen vår gir sterke indikasjoner på de ulike mulighetene blokkjeder kan benyttes som et datahåndteringssystem. Samtidig som vi har avdekket sentrale utfordringer med teknologien, og potensielle løsninger på disse utfordringene. Teknologien er fortsatt i en tidlig fase og det gjenstår fortsatt å se hvordan de praktiske applikasjonene av teknologien vil utvikle seg med tiden.

Blokkjede som et datasystem vil endre måten økosystemet opererer i dag. Annonsører og detabehandlere trenger ikke lenger å være avhengige av store selskaper som Facebook og Google for å levere relevant data. Ved å ta i bruk ulike mekanismer som smartkontrakter, og krypteringer kan man lage en plattform hvor annonsør og forbruker kan ha direkte forhandlinger av data uten behovet for en såkalt "middleman", som Facebook eller Google. En blokkjede løsning vil også kunne åpne muligheten for forbrukere å ha mer kontroll over deres egne personlige data. Slik systemene fungerer i dag vet forbrukere lite om data de gir fra seg og hvordan disse brukes. Kommunikasjon på nett kan derfor virke påtrengende og overvåkende. Med en blokkjede løsning derimot kan forbrukere sette sine egne regler og premisser for distribusjon av egen data, og kun dele data med ønskelige parter. Dette kan i gjengjeld føre til bedre personalisert kommunikasjon på nett, og samtidig styrke forholdet mellom annonsører og forbrukere.

Selv om teknologien kan ha en stor påvirkning på bruk og innsamling av data vil det være flere sentrale utfordringer knyttet til implementeringen av blokkjede teknologien. Som det står i dag er det fortsatt sentrale personvernutfordringer knyttet til teknologien. Slik det står i dag må utviklere finne nye kreative løsninger å jobbe rundt disse kravene, og heller vente til

regelverkene følger etter og tilpasser seg teknologien. Det er flere pilotprosjekter som allerede har kommet med forslag ment for å løse disse utfordringene, men det vil fortsatt ta tid før vi kommer frem til en ny standard. Blokkjedeteknologien kan løse problemer som andre teknologier ikke vil kunne gjøre like godt, og vi ser at teknologien kan gi stort utbytte for flere industrier. Ettersom teknologien er relativt ny og problemstillingen vår er fremtidsrettet er det vanskelig å gi noen konkrete svar.

6.1 Begrensninger og anbefaling til videre forskning:

Hvis blokkjedeteknologi skulle bli implementert som en fremtidig dataløsning ville det vært hensiktsmessig å utføre et eksperiment. Man kan da ha muligheten til å forstå hvordan systemet fungerer empirisk, og legge frem de aktuelle fordelene og ulempene som et resultat av implementering. Vi har i oppgaven vår undersøkt den potensielle innvirkningen blokkjede vil ha på bruk og innsamling av data. Det kan derfor være interessant å undersøke om det vil oppstå en økt verdiskapning for både forbrukere og annonsører som en konsekvens.

Denne studien ble gjennomført med informanter fra Norge, og andre land som opererer under EU sine databeskyttelses regelverk (GDPR). En annen vinkling kunne vært å se på land som ikke benytter seg av de samme regelverkene, og hvilke andre muligheter som kan være aktuelle. Hvis teknologien skal implementeres til bruk og behandling av data ville det vært interessant å undersøke hvordan teknologien ville fungert på tvers av landegrenser. På denne måten kan vi sette teknologien i en større sammenheng og også forstå effekten det vil ha på aktører i land med andre regelverk.

Videre vil det også være av interesse å se utviklingen av blokkjede over tid, og hvordan teknologien vil prege de nåværende aktørene og rollene innen innsamling og bruk av data. Det kunne vært av interesse å gjennomført en longitudinell studie som undersøkte utviklingen av blokkjedeteknologien over tid, og dermed gitt mer konkrete resultatet over påvirkningen blokkjeder vil ha på innsamling og bruk av data. En slik studie ville bidratt med å videre tydeliggjøre virkelighetsbildet av denne teknologien.

Begrensninger i denne oppgaven er hovedsakelig mangel på teknisk kunnskap bak de forskjellige løsningene som omhandler blokkjede og databehandling. Hadde vi sittet med mer teknologisk forståelse kunne vi gått mer i dybden på implementeringen av de aktuelle

løsningene. Dette ville gitt en god indikator på vanskeligheten av implementeringen av de ulike løsningene, og om de faktisk er praktisk gjennomførbare.

7.0 Referanseliste

Andersen, Unn C. og Arne H. Krumsvik. 2017. «Intervju som metode». I Metodebok for kreativfag, redigert av Hans Erik Næss og Lene Pettersen, 76–87. Oslo: Universitetsforlaget.

Bernal Bernabe, Jorge, Jose Luis Canovas, Jose L. Hernandez-Ramos, Rafael Torres Moreno, og Antonio Skarmeta. «Privacy-Preserving Solutions for Blockchain: Review and

Brave. (2021). Brave Passes 25 Million Monthly Active Users. Hentet fra: https://brave.com/25m-mau/

Brinkmann, Svend. 2013. Qualitative Interviewing: Understanding Qualitative Research. New York: Oxford University Press.

Buocz, Thomas, Tina Ehrke-Rabel, Elisabeth Hödl, og Iris Eisenberger. «Bitcoin and the GDPR: Allocating Responsibility in Distributed Networks». *Computer Law & Security Review* 35, nr. 2 (1. april 2019): 182–98. https://doi.org/10.1016/j.clsr.2018.12.003.

Burnard, P., P. Gill, K. Stewart, E. Treasure, og B. Chadwick. «Analysing and Presenting Qualitative Data». *British Dental Journal* 204, nr. 8 (april 2008): 429–32. https://doi.org/10.1038/sj.bdj.2008.292.

Carlson, Julie A. 2010. «Avoiding Traps in Member Checking». The Qualitative Report, 15 (5): 1102-1113. https://nsuworks.nova.edu/tqr/vol15/iss5/4.

Caspar, J. (2018). What You Don't Know About How Facebook Uses Your Data. Hentet fra: https://www.nytimes.com/2018/04/11/technology/facebook-privacy-hearings.html

Center, Electronic Privacy Information. «EPIC - Public Opinion on Privacy». Åpnet 24. Mai 2021. https://www.epic.org/privacy/survey/.

Challenges». *IEEE Access* 7 (2019): 164908–40 Hentet fra:. https://doi.org/10.1109/ACCESS.2019.2950872.

Choi et al., (2018). "It wouldn't happen to me": Privacy concerns and perspectives following the Cambridge Analytica scandal. Hentet fra: https://www.sciencedirect.com/science/article/pii/S1071581920301002#bib0046

Datatilsynet. (2017). Big Data - personvernprinsipper under press. Hentet fra: https://www.datatilsynet.no/regelverk-og-verktoy/rapporter-og-utredninger/big-data/

Datatilsynet. (2019). Om personopplysningsloven med fordring om når den gjelder. Hentet fra: https://www.datatilsynet.no/regelverk-og-verktoy/lover-og-regler/om_-personopplysningsloven-og-nar-den-gjelder/

Eckersley, P. (2021). Publicity, Sunlight and the Electrical Light. Hentet fra: https://www.policechiefmagazine.org/publicity-sunlight-and-the-electric-light/

Edps.europa. (2018). The History of the General Data Protection Regulation. Hentet fra: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

Ethos. (2021). What Are Miners? How Does Cryptocurrency Mining Work? Hentet fra: https://www.ethos.io/what-are-miners-cryptocurrency-mining

Frankenfield, J. (2021). Proof of Stake (PoS) Definition. Hentet fra: https://www.investopedia.com/terms/p/proof-stake-pos.asp

Frankenfield, J. (2021). Proof of Work (PoW) Definition. Hentet fra: https://www.investopedia.com/terms/p/proof-work.asp

Geradin, D. (2020,). How a well-intended regulation ended up favouring large online platforms. Hentet fra: https://www.tandfonline.com/doi/full/10.1080/17441056.2020.1848059

Glaser, Barney G. og Anselm L, Strauss. 1999. The Discovery of Grounded Theory: Strategie for Qualitative Research. London: Routledge.

Golafshani, Nahid. 2003. «Understanding Reliability and Validity in Qualitative Research». The Qualitative Report, 8 (4): 597–607.https://nsuworks.nova.edu/tqr/vol8/iss4/6/.

Google. (2021). Google Ads-data og -personvern - Google Sikkerhetssenter. Hentet fra: https://safety.google/privacy/ads-and-data/

Google. (2021). How Google uses information from sites or apps that use our services Privacy & Terms. Hentet fra: https://policies.google.com/technologies/partnersites?hl=en-US

Gosnell, Cymone. «The General Data Protection Regulation: American Compliance Overview and the Future of the American Business». *Journal of Business & Technology Law* 15, nr. 1 (juli 2019): 165–87.

Gripsrud, Geir, Ulf Henning Olsson og Ragnhild Silkoset. 2016. *Metode og dataanalyse: Beslutningsstøtte for bedrifter ved bruk av JMP, Excel og SPSS*, 3. utg. Oslo: Cappelen Damm Akademisk.

Guldahl, S. (2021). Slik holder du kryptoinvesteringen din trygg: En guide til kryptovalutalommebøker. Hentet fra: https://coinweb.no/lagre-bitcoins/

Hayes, A. (2021). Peer-to-Peer (P2P) Service Definition. Hentet fra: https://www.investopedia.com/terms/p/peertopeer-p2p-service.asp

Hern, A. (2018). "It wouldn't happen to me": Privacy concerns and perspectives following the Cambridge Analytica scandal. Hentet fra: https://www.sciencedirect.com/science/article/pii/S1071581920301002#bib0046

Hewitt, R. (2018). Facebook's Hard Fall Shows The Pitfalls of Big Data. Hentet fra: https://www.wsj.com/articles/facebooks-hard-fall-shows-the-pitfalls-of-big-data-1532750496

Hyperledger. (2021). Open source blockchain - What is Hyperledger? Hentet fra: https://www.hyperledger.org

Ico. (2021). Controllers and processors. Hentet fra: https://ico.org.uk/for-organisations/guideto-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/controllers-and-processors/

[1]«Implications of Blockchain Technology on Marketing by Adnan Veysel Ertemel :: SSRN». Hentet fra:. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3351196&download=yes.

Jaatun, M. (2021). Kryptografiske hash-funksjoner. Hentet fra: https://infosec.sintef.no/informasjonssikkerhet/2018/10/kryptografiske-hash-funksjoner/

Jacobsen, D. I. (2015). Hvordan gjennomføre undersøkelser? (3. utg.). Oslo: Cappelen Damm Akademisk.

Jayachandran, Praveen. Blockchain Pulse: IBM Blockchain Blog. «The Difference between Public and Private Blockchain», 31. mai 2017. https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/.

Jimi, S. (2021). Blockchain: What are nodes and masternodes? Hentet fra: https://medium.com/coinmonks/blockchain-what-is-a-node-or-masternode-and-what-does-it-do-4d9a4200938f

Johnson, R.B. 1997. Examining Validity Structure of Qualitative Research. *Education*, 118 (2). 282-292.

Kagan, J. (2021, 17. april). What is a Digital Wallet? Hentet fra: https://www.investopedia.com/terms/d/digital-wallet.asp

Knapskog, J. S. Eilertsen Ø. (2021). Kryptografi. Hentet fra:

https://snl.no/kryptografi

Li, H., og A. Nill. «Online Behavioral Targeting: Are Knowledgeable Consumers Willing to Sell Their Privacy?» *Journal of Consumer Policy* 43, nr. 4 (desember 2020): 723–45. https://doi.org/10.1007/s10603-020-09469-7.

Lipton, Alex, og Stuart, Levi. «An Introduction to Smart Contracts and Their Potential and Inherent Limitations». *The Harvard Law School Forum on Corporate Governance* (blog), 26. mai 2018. https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/.

Lovdata. (2021). Lov om behandling av personopplysninger - Avsnitt 3 Retting og sletting. Hentet fra: https://lovdata.no/dokument/NL/lov/2018-06-15-38/KAPITTEL_gdpr-3-3#gdpr%2Fa17

Lovdata. (2017). Lov om organisering av forskningsetisk arbeid (forskningsetikkloven). Hentet fra: https://lovdata.no/dokument/NL/lov/2017-04-28-23/

McParland, C., og Connolly, R. (2007). "Online privacy concerns: threat or opportunity," in Proceedings of 2007 Mediterranean and Middle Eastern Conference on Information Systems. EMCIS2007. Citeseer. 64-1_64-11. Valencia, 24–26 June 2007. Polytechnic University of Valencia

Meholm, Lasse. 2018. "Kryptovaluta, bitcoin, ICOer og blockchain"(1. utg). Oslo: Hegnar Media AS

Majaski, C. (2021). Distributed Ledgers Definition. Hentet fra: https://www.investopedia.com/terms/d/distributed-ledgers.asp

Malhotra, N., Kim, S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. Information Systems Research, 15(4), 336–355.

NTB-AFP. (2021). Bitcoin-feber kan velte Kinas klimamål. Hentet fra: https://e24.no/boers-og-finans/i/AlndLr/bitcoin-feber-kan-velte-kinas-klimamaal

Pollicino, Oreste, og Giovanni De Gregorio. «Privacy or Transparency: A New Balancing of Interests for the Right to Be Forgotten of Personal Data Published in Public Registers». *Italian Law Journal* 3 (2017): 647.

Rash, W. (2018). Cambridge Analytica Breach Reveals Facebook's Weak User Data Defenses. Hentet fra: https://www.eweek.com/cloud/cambridge-analytica-breach-reveals-facebook-s-weak-user-data-defenses/

Ratnasingham, Pauline. «Trust in Web-based Electronic Commerce Security». *Information Management & Computer Security* 6, nr. 4 (oktober 1998): 162–66. https://doi.org/10.1108/09685229810227667.

Rawal, Yogesh. «Blockchain to Solve Growing Privacy Challenges». Medium, 24. juni 2020. https://medium.com/akeo-tech/blockchain-to-solve-growing-privacy-challenges-67fc96a42693.

Rejeb, Abderahman, John G. Keogh, og Horst Treiblmaier. «How Blockchain Technology Can Benefit Marketing: Six Pending Research Areas». *Frontiers in Blockchain* 3 (2020). https://doi.org/10.3389/fbloc.2020.00003.

Riva, Gianluigi Maria. «What Happens in Blockchain Stays in Blockchain. A Legal Solution to Conflicts Between Digital Ledgers and Privacy Rights». *Frontiers in Blockchain* 3 (2020). https://doi.org/10.3389/fbloc.2020.00036.

Savin-Baden, M., & Major, C. H. (2013). Qualitative research: the essential guide to theory and practice.London: Routledge.

Scrt.Network. (2021). Bringing privacy to Smart Contracts and Public Blockchains. Hentet fra: https://scrt.network

Seidman, Irving. 2005. Interviewing as Qualitative Research: A Guide for Researchers in Education and the Social Sciences, 3. utg. New York: Teachers College Press.

Seth, S. (2021). Public, Private, Permissioned Blockchains Compared. Hentet fra: https://www.investopedia.com/news/public-private-permissioned-blockchains-compared/

Singer, N. (2018). What You Don't Know About How Facebook Uses Your Data. Hentet fra: https://www.nytimes.com/2018/04/11/technology/facebook-privacy-hearings.html

Statista. (2021). Facebook annual revenue. Hentet fra: https://www.statista.com/statistics/268604/annual-revenue-of-facebook/

Stoll, J.D. (2018). Facebook's Hard Fall Shows The Pitfalls of Big Data. Hentet fra: https://www.wsj.com/articles/facebooks-hard-fall-shows-the-pitfalls-of-big-data-1532750496

Techterms. (2011). Cookie definition. Hentet fra: https://techterms.com/definition/cookie

Vaivio, J. (2008). Qualitative management accounting research: rationale, pitfalls and potential. Qualitative Research in Accounting & Management, 5(1), 64 - 86.

Hentet fra: https://www.emeraldinsight.com/doi/abs/10.1108/11766090810856787

Williams, Stephen P. 2019. "Blockchain - The Next Everything" (1. utg). SD Books

Zunger, J. (2013). Confronting Big Data - Applying the Confrontation Clause to Government Data Collection. Hentet fra: https://www.virginialawreview.org/wp-content/uploads/2020/12/Squitieri_Online.pdf

Zyskind, Guy, Oz Nathan, og Alex «Sandy» Pentland. «Decentralizing Privacy: Using Blockchain to Protect Personal Data». I *2015 IEEE Security and Privacy Workshops*, 180–84, 2015. https://doi.org/10.1109/SPW.2015.27.

8.0 Vedleggsliste

8.1 Vedlegg 1: Intervjuguide

Følgende intervjuer har til hensikt å undersøke forholdet fagpersoner med bakgrunnskunnskap innen blockchain har til dets potensiale og utfordringer med tanke på datainnsamling og bruk. Dette er for å kartlegge hvordan blockchain-teknologi best kan benyttes i denne sammenheng. Formålet med dette er å sitte igjen med en mer konkret forståelse av hvordan folk oppfatter at dataen deres blir håndtert av de store aktørene i dag, og hvor blockchains egenskaper best passer inn. Opplysningene fra intervjuet kan ikke knyttes tilbake til deg.

Spørsmål vi ønsker refleksjoner og svar på:

Innledning:

- Jobber du med blokkjede i dag?
- Når ble du først opplyst om blokkjede teknologi?
- Har du deltatt i noen prosjekter med bruk av blokkjede?

Blokkjede:

- Er det viktig for bedrifter i dag å ha kunnskap om blokkjede?
- Hva slags rolle tror du blokkjede vil ha for fremtiden?
- Hvilke industrier tror du kommer til å bli mest påvirket av blockchain integrasjon i fremtiden?

Over til datadeling/datasikkerhet:

- Hvordan tror du blokkjede vil påvirke fremtiden til datalagring/datahåndtering?
- Er det sånn at hvis data lagres på blokkjede, så er den tilgjengelig for alle?
- Er datahåndtering/lagring avhengig av en ansvarlig tredjepart (datacontroller)

Potensiale:

- Kan blokkjede teknologi tilby en mer gjennomsiktig løsning for bruk og lagring av personlig data?
- Kan blockchain gi kontrollen over egen data tilbake til forbrukerne, og eventuelt hvordan?
- Hvilket annet potensiale ser du ved bruk av data

Utfordringer:

- Hvis persondata lagres på en blokkjede så er informasjonen tilgjengelig for alle. Hva kan være en løsning på dette?
- Når informasjon legges til i blokkjeden kan den aldri slettes eller endres. Ser du noen løsning på dette?
- Hvilke andre utfordringer ser du med blokkjede teknologi og personvern.

Avsluttende spørsmål:

- Hvordan tror du store selskap som Facebook og Google kommer til å anvende denne teknologien i fremtiden?
- Hvordan kan blokkjede brukes som et system datahåndtering/behandling?
- Krever det endringer i nåværende datareguleringer for at blokkjede kan bli et levedyktig data håndteringssystem?

8.2 Vedlegg 2: Informasjonsskriv

Ønsker du å delta i forskningsprosjektet *"Hva er den potensielle innvirkningen av blokkjede teknologi på bruk og innsamling av data".*

Dette er et informasjonsskriv som forklarer prosessen og hva det innebærer for deg å delta. Det er et spørsmål til deg om du ønsker å delta i forskningsprosjektet med formål om å undersøke hva den potensielle virkningen blockchain teknologi kan ha på fremtiden av innsamling og bruk av data.

Formål

Målet med denne bacheloroppgaven er å forske på og komme frem til potensielle muligheter for hvordan blokkjede teknologi kan skape en mer gjennomsiktig datalagring og delings opplevelse. Vi ønsker å se på hvordan denne teknologien kan gi kontroll over egen data tilbake til forbrukerne, men også se på utfordringer som står i veien før adopsjon av slik teknologi kan være mulig.

Resultatene fra intervjuet vil bidra til å gi oss bedre forståelse innenfor temaet blockhain, og forhåpentligvis kunne trekke konklusjoner fra svarene og benytte de i vårt forskningsprosjekt.

Hvem er ansvarlig for prosjektet

Høyskolen kristiania er ansvarlig for prosjektet.

Hvorfor får du spørsmål om å delta?

Vi har valgt intervjuobjektene på bakgrunn av forskningsprosjektets problemstilling. Denne oppgaven har med hensikt å se hvordan blokkjede teknologi kan påvirke databehandling/datainnsamling. Vi har som krav til følgende intervjuobjekter om at de jobber/har jobbet innenfor fagfelt som har benyttet blockhain-teknologi i tjenesten de tilbyr, samt at de er generelt oppdatert innen temaet per dags dato.

Hva innebærer det for deg å delta?

Dette intervjuet vil for deg innebære at vi stiller åpne spørsmål for god innsikt i dine synspunkter. Det kan ta opptil 60 minutter, og det vil bli tatt notater underveis. Utover dette vil vi kunne ta kontakt på e-post hvis vi trenger noe mer oppklaring rundt eventuelle spørsmål, og dette kan medføre noe ekstra tid for deg.

Det er frivillig å delta

Dette er et prosjekt hvor det er helt frivillig å delta, hvis du først har valgt å delta så kan du trekke samtykke tilbake når som helst, uten krav om å oppgi noen årsak. Da vil alt av dine opplysninger bli slettet, og det ville ikke påføre noen negative konsekvenser for deg i ettertid om du ikke ønsker å delta.

Ditt personvern - hvordan vi oppbevarer og bruker dine opplysninger

Opplysningene dine vil bli behandlet i samsvar med personvernregelverket, og alt er konfidensielt. Vi vil ikke benytte oss av hverken lydopptak eller videoopptak, men transkriberingngene vil lagres på en privat datamaskin, passordbeskyttet og offline.

Veileder for oppgaven fra Høyskolen Kristania:
Annette Kallevig
[redacted]
[redacted]

Bacheloroppgaven kommer ikke til å gå inn på bedriftssensitiv informasjon. Hvis informasjon (sitater og eksempler) som blir gitt av intervjuobjektene kan gi antydning til bedriften, vil det bli skrevet slik at det ikke kan skade bedriftene og intervjuobjektene.

Hva skjer med opplysningene dine når vi avslutter forskningsprosjektet?
Opplysningene vi samler vil være anonyme fra innsamlingspunkt. Da det er en bacheloroppgave, må opplysningene bli lagret i oppgaven etter prosjektet er ferdigstilt. Transkriberingene blir tatt vare på i 6 måneder etter innleveringsfrist, deretter vil notatene slettes fullstendig.

Dine rettigheter
Du kan til enhver tid gjøre følgende:

- Få innsyn i personopplysningene som er registrert om deg, samt en kopi av disse opplysningene
- Du kan få disse rettet opp i hvis noe ikke stemmer
- Du kan få slettet eventuelle opplysninger du ikke ønsker at skal være med

Samtykkeerklæring

Jeg har forstått og mottatt informasjonen om forskningsprosjektet *"Hva er den potensielle innvirkningen av blokkjede teknologi på bruk og innsamling av data".,* og har fått mulighet til å stille eventuelle spørsmål.

Jeg samtykker til:

- ❑ Å delta i intervju
- ❑ At mine personopplysninger lagres til bacheloroppgaven sensur er gjennomført
- ❑ At opplysningene om meg blir publisert med bacheloroppgaven slik at jeg ikke kan bli identifisert.

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er slutt, og at jeg har mulighet for å revidere/slette opplysningene fortløpende.

Navn: _____

Dato: _____

8.3 Vedlegg 3: Transkriberte intervjuer

8.3.1 Informant 1

Front-end og blockchain utvikler

Innledning:

- **Jobber du med blokkjede i dag?**
  Nei, det gjør jeg ikke. Det har jeg ikke gjort på litt over 1 år nå. Så håper jeg har svar på spørsmålene, skal prøve så godt jeg kan.

- **Når ble du først opplyst om blokkjede teknologi?**
  Tror det var i 2017 eller 2018, da ethereum var ganske stort. Det var diskusjoner på studiestedet, der noen hadde investert i ethereum. Og det var snakk om at det skulle bli stort og "hype hype".

- **Har du deltatt i noen prosjekter med bruk av blokkjede?**
  Ja, altså jeg har jobbet på en innovasjonsstudio tidligere. Der vi fokuserte på nye teknologiker som AI, quantum computing og blockchain da blant annet. Så der lagde vi en prototype som brukte blockchain, som lagret eierskap eller bileierskap og bilforsikring på en blokkjede. Men siden det var en prototype så var det aldri noe som gikk til produksjon. Så den type perspektiv har jeg ikke.

- **Er det viktig for bedrifter i dag å ha kunnskap om blokkjede?**
  Ja, det synes jeg absolutt. Man bør ha en type forståelse for de nye teknologiene og hva de kan medføre, og da er blockchain en av de. Sånn som jeg jobbet på innovasjonsstudio er det viktig at man tester med ny teknologi, og tar med seg den kunnskapen og erfaringen bedriften får. Man får da et forhåndssteg foran de andre bedriftene, gjennom den erfaringen, og dette gjelder jo blockchain også.

- **Hva slags rolle tror du blokkjede vil ha for fremtiden? Hvilke industrier tror du kommer til å bli mest påvirket av blockchain integrasjon i fremtiden?**
  Det er jo så mange muligheter, så man kan ikke være ekspert på alle. Men jeg synes supply chain use caset med blockchain er veldig spennende. Muligheten til å spore produkter, hvor det kommer fra, mulighet til å dra typ en digital tvilling av ting, sånn at brukerne kan se hvor produktet kommer fra og spore det. Det tror jeg er

bruksområde, og det er jo allerede i produksjon.

- **Er det sånn at hvis data lagres på blokkjede, så er den tilgjengelig for alle?**
  Det kommer an på hva slags type blockchain database man har. Man har jo masse forskjellige, man har private blockchain der kan ikke alle se det. Men hvis man har det på en public blockchain der kan alle se det. Også har man permissioned, eller ikke permissioned, og det går på hvem som er tillatt til å skrive/legge til ting på blockchainen. Så hvis man har en public blockchain ja, hvis man ikke bruker noe form for kryptering av data. Men hvis man har private, så er det bare de deltakerne som er med i blockchain nettverket som ser det.

- **Med data håndtering og lagring så er man litt avhengig av en tredjepart som er ansvarlig for dataen (data controller), tenker du at dette hadde blitt gjort med en privat blockhain eventuelt?**
  Hvis det er tredjepart? Ja det er vel det som er diskusjonen rundt lukket blockchain nettverk. At det er på en måte noen som må dra i gang det, litt mer enn det andre, og hvordan men eventuelt kan jevne ut det. Gjennom kontrakt eller hvordan man jobber sammen. For uansett hvis man har lukket, kommer an på hvilke blokkjede rammeverk man bruker så kan du man på en måte distribuere en node til forskjellige bedrifter, slik at de har sin kopi og kan endre.

- **Kan blokkjede teknologi tilby en mer gjennomsiktig løsning for bruk og lagring av personlig data?**
  Det er jeg ikke helt sikker på, jeg har ikke satt meg inn i det use caset såpass mye. Jeg leste om det for noen år siden, men jeg er ikke helt inneforstått med hvordan det skulle vært satt opp og hva slags rammeverk man skulle ha brukt, og hvilke type blockchain plattform det skulle være.

- **Hvis persondata lagres på en blokkjede så er informasjonen tilgjengelig for alle. Hva kan være en løsning på dette?**
  Det blir vel en type kryptering, med private og public key og lignende. Så bare de som skal få tilgang til dataen skal ha muligheten til å kryptere eller dekryptere det. Men så har man jo GDPR også, som er ganske interessant med tanke på at man skal kunne slette dataene hvis en bruker ønsker det. Og da er spørsmålet hvordan du kan slette det

fra en blockchain, hvis ikke du skulle hatt en referanse i forhold til kryptering, og da må man likevel ha en ny database som lager den referansen.

- **Når informasjon legges til i blokkjeden kan den aldri slettes eller endres. Ser du noen løsning på dette?**
  Altså jeg har bare jobbet med ting i prototype, og da har vi heldigvis ikke prøvd å adressere problemet, men det har jo vært diskusjoner rundt det. Og sist jeg var med i de diskusjonene så gikk det ut på at man hadde typ en nøkkel, så hvis man hadde personnummer så var det ID som var linket til en database. Så uten den ID'en ga ikke dataen noe mening. Men så igjen blir det enda en database og holde styr på, også kan man diskutere hvor desentralisert det er, og hvem er det som skal være ansvarlig for den databasen.

- **Hvilke andre utfordringer ser du med blokkjede teknologi og personvern? GDPR og sensitiv informasjon, hvordan man skal sikre at ikke feil person får tilgang på dataen.**

- **Hvordan tror du store selskap som Facebook og Google kommer til å anvende denne teknologien i fremtiden?**
  Jeg tenker at jeg ikke kan så mye om den biten, men jeg føler Facebook er et så stort selskap, at hvis de ikke bruker det nå, hvorfor bruker de det ikke, og hvilke bruksområder er det de ser for seg å bruke.

- **Hvordan kan blokkjede brukes som et system datahåndtering/behandling?**
  Det kan man sikkert, men blockchain kommer også med en pris. Jeg har jobbet en del med hyperledger fabric, og det tar jo lenger tid for å utføre transaksjoner enn gjennom en vanlig database. Så jeg er litt usikker hvis det liksom er et use case, om hvilke type blockchain som kan løse det på best mulig måte, det er jeg litt usikker på.

- **Krever det endringer i nåværende datareguleringer for at blokkjede kan bli et levedyktig data håndteringssystem?**
  Nei, de regelverkene er jo til for å beskytte brukerne. Det er jo viktige regelverk som ikke kan vikes for, for noen teknologi. Da må heller vi som jobber med teknologi finne en måte på hvordan man kan gjøre det, og selskaper teste seg fram. Det tror jeg

mer på.

8.3.2 Informant 2 (engelsk)

College professor

- **Do you work with blockchain today?**

  Do I work with Blockchain? Well i'm a professor so I taught blockchain courses, but I wouldn't consider that working with blockchain. Like i don't programme. Some of my students programme, but not me.

- **When did you first start to learn about blockchain, or when did you first discover it?**

  I would say this was 2017, I think that was when it was. It was because one of my students got involved in medchain. I believe the name was, which was looking at medical records, and sort of developing systems where people could put medical records on a blockchain. Or atleast have references to your medical records on a blockchain. So he got involved in that, and then he'd just come to office hours, where we talked about the future of blockchain. How it can be used in healthcare, how it could be used in curation markets, curating information. And I got really interested, and started researching that. I had a sabbatical to do a lot of research, and then ended up teaching a course on blockchain, just as a way of exploring it with upper level undergraduates.

  So you teach a course right now?

  Well I taught it in the past, currently I'm not teaching that.

- **So you haven't worked in any projects, or anything that like uses blockchain?**

  Not really, I mean I went to a hackathon with Ethereum at one point, But our project ended up mostly being theoretical, I mean it was with some developers, and we were trying to lay out the ideas for a project. I mean it's the kind of thing you do at a hackathon which is a mini project, or the beginning of a project. Where you spend the most of the weekend just talking about it, rather than actually building it.

- **Is it important for businesses to have knowledge about blockchain today?**

  I think it depends on the business. I think blockchain is going to kind of infiltrate

different industries at different rates. So like supply chains, if you participate in supply chains and dont understand blockchain I think that's gonna put you at a huge disadvantage. With healthcare I think it's gonna take a bit longer for blockchain to take over. Mainly because healthcare is so regulated, and I mean everything in healthcare just takes a lot longer, so if you don't know about blockchain now in healthcare, it's probably not gonna put you at a huge disadvantage. But 10 years from now, yeah I think everybody will need to understand it

So who do you think will be the earliest adoptors?

The earliest adoptors. Well so it's finance, where obviously that's where blockchain is taking of right now, and I think thats a good first place for it to take off. Supply chains are sort of the next wave where blockchain is taking over, where 5 years from now most supply chains will be blockchain based.

- **How do you think blockchain will affect the future of data storage and privacy?**
  Well I think the place where it's gonna impact security is gonna have to do it having clear records of who you're giving access to private information.because that's one of the big deals like with medical records certainly and I don't think the records will happen first. I think it will be other areas that you need certain people to have access to. Like different doctors you need to have access, different medical agencies you need to have access but it's also very private and so keeping clear and accurate records of who you've given permission to, to use the data. I think that's going to be the big early use of Blockchain and security is just keeping accurate records of permissions.

- **One of the problems we saw with GDPR and the regulations in Europe. How can we protect sensitive data from being accessible to every participant on the chain?**
  I think that's one of the issues with Blockchain. I'm not convinced that the long run is going to mean everybody's private data is on the Blockchain. I think it's going to be more what's on the Blockchain. Who has control over your data and who has access and who have you given the key to your data. I think in the long run, the way it's going to be set up is that each person sort of has like a private server of some sort which maybe you're hiring a company that you trust for that private server. But it could be small companies, it could be your cousin, like different servers where this is my private server and the Blockchain is really more the gatekeeper for access to that

server. I think that's going to be a model that We'll see 10 years from now.

- **Is data privacy dependent on an accountable third party? (datacontroller).**
  Well, so I think it's going to be each individual chooses who they trust for that third party. So some people are fine with a really big company, other people are less trusting and they're going to want something like a cousin that they know or trust. I think there's going to be different models for this third party. It won't be a centralized 3rd party, that i'm sure of.

- **Can blockchain technology offer a more transparent solution for the use and storage of personal data?**
  Yeah, I think transparent methods of conveying that information. I think it's gonna be important but I think the issue here is kind of the mental infrastructure. Where it's kind of like the reason we have these centralized companies for social media and for a lot of things because it requires a little bit of knowledge to figure out how does the website work. How does the mechanism work that protects my privacy here. How do i know if my privacy is protected and centralized systems do a good job of that because you can kind of learn from your friend. Oh yeah, this company has been around for a while, all the tech aides say that it's safe and therefore you trust the third parties. But now of course once the third parties gained power, there can be an abuse of that power. And that's when the trust goes downhill. And so it's this mental infrastructure that people's understanding of how to interact with the system, of what are the risks with the system, of what kinds of things, what kinds of information to put where that it's all this stuff that is more is what I refer to as the mental infrastructure. And I think we're going to need to arrive at some standards that are this is the mental infrastructure used through this particular Blockchain. And I think that's going to evolve over time, figuring out what are the standards that are most useful. It's almost like we're going to need some sort of user design interface that has been tested and has multiple versions before we arrive at it. Okay, this is the universal for this Blockchain user design interface, but it's kept track of in a decentralized way and I think that's going to take a process. I think it will take a few years to arrive at that.

- **What other potential do you see in the terms of data privacy?**
  With data privacy, I really think it's about the rules, and I think it's gonna be sort of

here are the rules for access to my data, but I think it's connecting that with a mechanism of accountability that's not necessarily on chain. So there will be on chain mechanisms of accountability where perhaps someone who wants access to your data has to stick some money and if they don't treat your data in a secure way they don't get their money back. Things like that could be on chain. But I think there's going to be mechanisms that are off chains such as the legal system being able to sue people easily if they breach rules that are set up clearly and transparently on a Blockchain. So I think getting the legal system to sort of use Blockchain more often and use them as transparent ways of proving that yes you set up these rules and they have violated the rules you set up with. I think that's going to be key.

So do you see it being like a combination of on-chain and off-chain services?

Yeah I think both of those models are going to be out there. I don't think they'll necessarily be in the same cleans but I think we need both of those mechanisms.

- **If personal data is stored on a public chain, the information is accessible to anyone. What can be a solution to this?**

  I think that the deal with private chains is that they're a little bit too close to just databases. And is it worth the expense of a Blockchain to use a private chain. Now, there are some advantages because private chains can have parties that are sort of more socially distant to each other collaborating, and it's almost like they’re kind of in between a private and a public chain. I could see use of private chains where you have different security companies that are sort of holding each other in check. Through some sort of Blockchain system where like maybe there's 17 validated security companies in Europe or something like that. And they decided to have a private Blockchain for validation of each other's security services. And if they find bad information on a competitor. They can report that and perhaps report it to the other 16 security companies within that group and kind of police themselves to increase the security level for those 17 companies, I could see that sort of system giving the 17 companies advantage over competitors outside the Blockchain. And I think that's really the key with Blockchain. It's really about how can you help competitors cooperate. Is there something that can raise the boat of everybody in the industry. So this sort of semi, it is a private block chain technically, but it's got enough parties that are independent that they could hold each other in check and create a validation

system for each other.

- **When information is added to the chain it cannot be deleted or changed. What can be a solution to this?**
  Well so I don't think storing private personal data on a Blockchain will be like a big part of the future. I think there's so many companies where the people who are in the blockchain community will not put their personal data on a Blockchain. Which I think it makes sense for that reason. The fact that it can't be deleted if you make a mistake or if later down the road, this information becomes a liability to you. It's out there forever. So the risk of that I think is just too high for that to be the way Blockchain is used.

- **Do you see any other challenges with blockchain technology, and data privacy?**
  Well i think blockchain is the solution to one of these challenges with any technology, but especially privacy technologies that when you put a new technology out there, there's going to be problems with it and bugs for a while and when it comes to security, any bug you have really increases the risk of that technology. I think Blockchain will be used to sort of track in a transparent way the evolution of that technology as programmers come in and fix the holes in the technology. So I think what's going to happen is one of new technology is put out there for security reasons, a security technology and will be put out there knowing that it's not secure, knowing that there's problems that we haven't yet figured out, but knowing that there's going to be a certain amount of time into a certain amount of testing, before you reach the optimal levels of security of security or the level that people can trust and blockchain will keep record of how many people have used this technology. Have we had enough use of the technology that we've worked through all the bugs. What has the updates been to the technology. And are the updates strong enough that we believe we worked through the major bugs of this technology. And I think it's gonna involve tracking those changes in new technologies as they enter the system to reduce uncertainty about how much farther a new technology has to go.
- **Current data privacy regulations limits a lot of blockchains potential. Do you think these need to be changed and adapted to blockchain? Or does blockchain need to work around these regulations?**
  Ideally regulations are going to be updated in response to the development of

Blockchain. The problem is that regulators tend to be really far behind the technologists and so in some ways the time lag, I think it's an issue. Generally Blockchain developers are going to have to proceed as if the laws are not gonna change for quite a while, that and the Blockchain developers don't even know what are the laws we actually need to make this technology work. So, yeah, I think I tend to be more on the side of we kind of have to accept the given laws which are outdated and don't take into account what Blockchain is. Work for a while and then 10 years down the road, the policymakers will catch up.

- **Big companies like facebook and google have already started investing a lot of time and resources into Blockchain. How do you think they will be using this technology in the future?**
  Well I think one of the biggest reasons that they're investing in this is they need to understand the technology better than other people if they want to stay ahead. Like I think they have recognized that this technology could disrupt their business law, and one way to stay on top of that is to have projects which might not necessarily pan out is their current form but which will educate the people inside facebook and inside your role in all these places such that they really understand the strengths and weaknesses of that technology is such that they can accurately assess competitors. Perhaps that come on the scene that could disrupt their business model. So I think them involving themselves in these projects is more about making sure that there are people really know what's going on.

- **Do you think Blockchain has the potential to be used as a data storing service? If you're familiar with the Brave browser, have you heard about that?**
  No.
  So the brave browser is a new browser where you can control and manage your data settings yourself. You can choose which advertisers and stuff you want to share your information to and you earn crypto. It's called a B A T a basic attention token based on what you share and how you interact with these ads. Do you think services like this will take off more in the future?
  Okay. Yeah. I think services like that which is different than putting your information directly on Blockchain. You can sort of say okay here's my information. I have it in a safe place but who has the right to my information? Who has the right to this private

stuff. I can negotiate that. I can sell it on the market. I can use this block team to sort of transact you know, access to my data. I think that absolutely will happen. And then I think certain types of data will go on Blockchain such as credentials like especially credentials that people don't mind being public like where did they graduate from or what, what board exams have they passed. Things like that. I think that stuff will go on Blockchain. I also think there's a possibility that block chains may have information that is not the data itself but it is essentially a key to the data so that it's sort of like all these letters that are stored on the Blockchain when you take that set of data, you can kind of mix it with this other data base two undo information that is truly personal like medical did I ends DNA data and things that you would not want people to know. But I don't think personal data will be stored on block tunes but I do think there will be these other solutions that relates to our personal data.

Can we set up a system with like smart contracts, so the smart contracts rule what kind of data we share with these companies?

Yes, for sure.

How do you see smart contracts being implemented in the data privacy side of things?

I think having smart contracts that figure out who can access your data will be absolutely essential. Let's say you have a rare disease and you want your data to be available to researchers who are researching people like you, it's super private data. You won't put your medical data on a Blockchain but you'll have some sort of smart contract that says okay if people meet these criteria which might be like they have five researchers with a PhD in medicine or Biology or something like that. If they have these, then it can automatically dispense my data to those people or if a company pays me $1,000 for access to my data, then they will automatically get a key to my data which is located in a private place. So yeah, I do think the mechanisms that distribute your data or distribute access to your data and the proof that this is who you have decided, can you have it and this is who you haven't, that kind of stuff having Absolutely will be on a Blockchain.

- **You think you can have any mechanisms for you to pull that information back?**

Oh yeah, like give my data to anyone who will pay $1000 except and then have, you know, 15 exceptions, except people who are studying this thing that I don't like, or people who are belong to the Church of scientology or whatever. I definitely think the

smart contracts that give out our data, I think they're going to be pretty complex.

- **So you think the solution will be like simplifying this technology for the user, so it's easier for us to understand?**
  Yes, simplifying the technology for the users and figuring out what kinds of things should people think about when they're farming out their data. Because a lot of times people don't know like what sort of ethical violations could happen with my data, they just haven't thought through every circumstance. So having companies that are set up on block teams with smart contracts that have thought carefully about those, have experienced a lot of violations of privacy that people might want to consider and we'll have ways of like setting up interfaces that are easy for people to deal with.

8.3.3 Informant 3

IT Konsulent

Innledning:

- **Jobber du med blokkjede i dag?**
  Jeg jobber ikke med blokkjede i dag, men har tidligere vært del av et konsulentselskap som jobbet med utvikling av IT tjenester for ulike bedrifter, og har i den sammenhengen blitt fascinert av blokkjede teknologien.

- **Når ble du først opplyst om blokkjede teknologi?**
  Interessen min startet vel i 2017-2018 når Bitcoin begynte å bli populært. Jeg synes det var et veldig interessant tema, og begynte å lese mer om det på egenhånd. Så etterhvert lærte jeg om Ethereum, og begynte å se mer på teknologien bak, og ikke bare kryptovalutasiden som som regel er der vi ser blokkjede teknologi bli diskutert. Det jeg begynte å skjønne da var at blokkjedeteknologi hadde et enormt potensiale, ikke bare for digitale valutaer og finans, men også for flere andre områder som helsetjenester og særlig digitale “supply chains”. Man kan registrere enhver del av forsyningskjeden på en blokkjede, og deltakerne kan dermed til enhver tid se hvor materialer kommer fra, om materialene er av riktig kvalitet og for eksempel om de har blitt utvinnet på etiske og bærekraftige måter. Det er egentlig her i disse selskapene som tar i bruk en form for supply chain hvor jeg ser det aller største potensiale for

blockchain.

- **Har du deltatt i noen prosjekter med bruk av blokkjede?**
  Jeg har ikke laget egne blokkjede løsninger, men jeg har vært med i utviklingen av flere ulike prototyper som har tatt et utgangspunkt i blokkjede teknologi.

Blokkjede:

- **Er det viktig for bedrifter i dag å ha kunnskap om blokkjede?**
  Nja, både og. Det kommer egentlig helt an på bedriften og hva de driver med. For noen bedrifter vil ikke blockchain være like relevant, mens andre vil kunne ha enorm nytte av det. Problemet i dag er at vi fortsatt ikke helt vet hvordan denne teknologien kommer til å påvirke og brukes i bedrifter enda. Men for særlig teknologiselskaper ser jeg det som et utrolig godt konkurransefortrinn å ha i hvertfall grunnleggende kunnskap om blockchain og hvordan teknologien kan brukes.
- **Hva slags rolle tror du blokkjede vil ha for fremtiden?**
  Jeg tror blockchain kan ha ufattelig mange bruksområder, og vi er fortsatt ikke helt klare over hvor vi kan bruke det. Det vil jo også selvfølgelig ta tid før vi kan se det fulle potensiale. Mange av mulighetene ligger der, men det krever at folk generelt har mer kunnskap om temaet, og at vi tar slik disruptiv teknologi på alvor. Det er egentlig bare tiden som vil vise hvor aktuelt blockchain vil bli, men jeg personlig tror det har stort potensiale.

- **Hvilke industrier tror du kommer til å bli mest påvirket av blockchain integrasjon i fremtiden?**
  Jeg har forsåvidt nevnt det litt tidligere, men personlig tror jeg bedrifter som er bygget på en såkalt supply chain vil være de første til å ta i bruk denne teknologien. Særlig helsetjenester og offentlige sektorer som er avhengig av tilgang til korrekt informasjon og datamateriale vil ha stor nytte av blokkjeder, men som vi vet så er dette også de sektorene som bruker lengst på å tilpasse seg og ta i bruk ny teknologi.

Over til datadeling/datasikkerhet:

- **Hvordan tror du blokkjede vil påvirke fremtiden til datalagring/datahåndtering?**

Hmm, vanskelig spørsmål. Sånn teknisk sett så er det ikke all informasjon som er egnet til å ligge på en offentlig kjede. Sensitiv informasjon kan ikke være tilgjengelig for alle. Så er det annen data som kanskje burde være tilgjengelig for allmennheten. Jeg tror det er viktig at vi setter klare grenser og forhåndsregler for hva som burde distibueres og holdes privat. Spesifikk data som eierskap og transaksjoner kan ha fordel av å ligge på en offentlig kjede, mens sensitiv data som kan direkte identifisere personer burde holdes på private kjeder hvor autoriserte personer kan få tilgang til og se disse dataene, under gitte spesifiserte forhold.

- **Er det sånn at hvis data lagres på blokkjede, så er den tilgjengelig for alle?**
  De offentlige eller også kalt åpne blokkjedene vil være tilgjengelig for alle nodene i nettverket. Det betyr at alle som deltar i kjeden vil kunne gå gjennom og se over informasjonen som ligger i kjeden. Det er allikvel flere krypteringsmekanismer som er på plass for å sikre personers anonymitet. Men da kommer også denne debatten om informasjonen faktisk er anonymisert. Noe informasjon kan vi jo indirekte knytte til et individ uten at vi vet hvor informasjonen kommer fra. Så rent teknisk sett er ikke all data og informasjon egnet til å oppbevare på en blokkjede. Når det kommer til private eller lukkede kjeder derimot kan man kontrollere hvilke av nodene i nettverket som har unik tilgang til ulik informasjon. Private kjeder egner seg bedre til håndtering av sensitiv informasjon, men da kommer også dette dilemmaet om makt og manipulasjon opp. Hvis det er ett unikt selskap som sitter på makten over data og tilganger, vil de i gjengjeld også ha muligheten til å kontrollere denne dataen.

- **Er datahåndtering/lagring avhengig av en ansvarlig tredjepart (datacontroller)**
  Hmm, det er noe jeg egentlig ikke har så god kunnskap om. Men hele løftet med blockchain er jo at det er desentralisert. Men med tanke på lover og regler vil man jo måtte ha en person eller bedrift å holde ansvarlig hvis det skjer uventede lovbrudd.

Potensiale:

- **Kan blokkjede teknologi tilby en mer gjennomsiktig løsning for bruk og lagring av personlig data?**
  Det tror jeg absolutt. Men generelt sett tror jeg ikke sensitiv persondata som biometriske detaljer osv er egnet til å kunne lagres i en blokkjede. På den andre siden med data som forbrukere generelt sett ikke er redde for å offentliggjøre kan være aktuelt å registrere på en blokkjede. Man kan for eksempel sette opp smartkontrakter

mellom 2 parter som for eksempel spesifiserer at man vil kun gi fra seg data til aktører som ikke vil lagre det og benytte det i en senere anledning, eller også til kun profesjonelle aktører som har en mastergrad osv, hvis du skjønner. Så her tror jeg det er mange muligheter.

- **Kan blockchain gi kontrollen over egen data tilbake til forbrukerne, og eventuelt hvordan?**
  Ja til en viss grad tenker jeg det kan det. Med tjenester som Brave for eksempel har personer muligheten til å styre sin egen data, de kan altså sette opp regler for hvem de vil dele dataen sin med, og motta goder for dataen de gir fra seg. Jeg tror løsninger som disse kommer til å bli mer og mer populære med tiden.

- **Hvilket annet potensiale ser du ved bruk av blokkjede**
  Vanskelig å si, men føler jeg har nevnt en del muligheter tidligere. Samtidig så tror jeg også vi må la tiden vise hva denne teknologien kan gi oss av muligheter.

Utfordringer:

- **Hvis persondata lagres på en blokkjede så er informasjonen tilgjengelig for alle. Hva kan være en løsning på dette?**
  hmm, som jeg sagt tidligere så tror jeg ikke persondata er noe som burde bli overført til blokkjeder. Derimot tror jeg man kan utforske et design som kombinerer både blockchain med database lagring. Så for eksempel kan du sette opp en kontrakt som henter ut kryptert data fra en database, under gitte forhold. Men persondata i seg selv burde ikke oppbevares kjeden.

- **Når informasjon legges til i blokkjeden kan den aldri slettes eller endres. Ser du noen løsning på dette?**
  Dette er jo en av de store utfordringene med blockchain. Nemlig at man ikke kan slette informasjon på kjeden. Jeg tror heller at løsningen vil være at man unnviker å lagre disse dataene på kjeden i det hele tatt, men heller finner alternative løsninger på hvor denne sensitive informasjonen lagres.

- **Hvilke andre utfordringer ser du med blokkjede teknologi og personvern.**

De største utfordringene med blockchain som jeg ser er regelverkene som begrenser de forskjellige bruksområdene. som dere også har nevnt med problemstillinger knyttet til GDPR og pesonvern.

Avsluttende spørsmål:

- **Hvordan tror du store selskap som Facebook og Google kommer til å anvende denne teknologien i fremtiden?**
  For øyeblikket tror jeg det er vanskelig å si hvordan disse selskapene kommer til å benytte seg av blokkjede teknologien, men jeg tror allikevel det er ufattelig lurt for dem å sette seg inn i teknologien. Facebook og Google er begge avhengig av å konstant holde seg oppdatert på teknologiske utviklinger, så hvis denne teknologien kommer for å bli er det nødvendig at de har tilstrekkelig med kunnskap om fagfeltet så de ikke havner bakpå og lar konkurrenter overta dem.

- **Hvordan kan blokkjede brukes som et system for datahåndtering/behandling?**
  I teorien må det bli en generell løsning som kombinerer både onchain og offchain tjenester. Vi kan for eksempel ha en desentralisert app hvor brukere kan sette forhåndsregler for deling av deres data, kombinert med en ekstern database som brukeren har full kontroll over. Denne appen kan da hente ut informasjon den har fått tilgang til ved hjelp av ulike smartkontrakter som står på plass i systemet.

- **Krever det endringer i nåværende datareguleringer for at blokkjede kan bli et levedyktig data håndteringssystem?**
  Som regel så pleier regelverk alltid å ligge bak når det gjelder ny teknologi. Å opprette nye rammeverk for teknologiske løsninger er en prosess som tar tid, og jeg tror derfor at blockchain-utviklere må kunne forholde seg til de reglene som står i dag og jobbe med løsninger som forholder seg til disse lovene. Vi har jo fortsatt ikke sett den reelle innvirkningen av blockchain enda, og hvis det ved et senere tidspunkt blir en teknologi som tar helt over er det nødvendig at regelverkene oppdateres til disse nye teknologiene.

8.3.4 Informant 4

Regnskapskonsulent

Innledning:

- **Jobber du med blokkjede i dag?**
  Nei, det gjør jeg ikke.

- **Når ble du først opplyst om blokkjede teknologi?**
  Jeg ble først introdusert til blockchain i 2018 da selskapet jeg jobber i skulle teste ut en løsning basert på blockchain teknologien. Da fikk vi alle en innføring i bruksområder, og det grunnleggende rundt hvordan det er bygget opp.

- **Har du deltatt i noen prosjekter med bruk av blokkjede?**
  Ja, jeg er en regnskapskonsulent, og prosjektet var starten på utviklingen av en tjeneste som tilbyr muligheten til å kunne overføre verdier og få bekreftelse som signaturer i nesten sanntid forholdsvis kostnadsfritt. Dette var da på et åpent nettverk. Hensikten var å få mer effektivitet i den økonomiske hverdagen til kundene våre. Jeg var ikke teknisk involvert, jeg var kun med for å gi innblikk og moderere at løsningen ble fullverdig og nyttig for økonomi.

Blokkjede:

- **Er det viktig for bedrifter i dag å ha kunnskap om blokkjede?**
  Nei, altså sånn som det ser ut i dag, så mener jeg ikke at det er noe essensiell kunnskap bedrifter må ha kunne. Om noen år frem i tid vil jeg tro at teknologien begynner å bli mer gunstig for enkelte industrier, men absolutt ikke alle. Det er en såpass kompleks teknologi, og ekstremt omfattende. Så jeg ser ikke for meg at det blir første prioritet for bedrifter og vie så store mengder av tid, penger og ressurser generelt til å ta i bruk blockchain teknologien. Det blir rett og slett for komplekst til at alle bedrifter har tid til å forstå og få bruk for prosessene i dag.

- **Hva slags rolle tror du blokkjede vil ha for fremtiden?**
  Jeg vil tro blockchain finner sin plass etter hvert, men det er nok en god stund til. Jeg kan se for meg at det er flere som også føler seg truet, da det er en teknologi som

potensielt kan ta over arbeidsoppgavene de sitter med den dag i dag. Og dette tenker jeg kan motivere til at det blir enda vanskeligere for blockchain og slå gjennom, men det vil nok utvilsomt bli standarden innenfor visse bransjer på lang sikt.

- **Hvilke industrier tror du kommer til å bli mest påvirket av blockchain integrasjon i fremtiden?**
  Jeg tenker at banker vil ta i bruk blockchain i stor grad etter hvert. Man ser jo at de allerede har begynt, og det er flere store banker på verdensbasis som har begynt å samarbeide for å finne gode løsninger på hvordan det er mest hensiktsmessig å benytte seg av effektiviteten blockchain tilbyr. Ut i fra tjenestene en vanlig bank tilbyr er det mye penger å spare inn på å få satt i gang automatiserte tjenester, og da spesielt bruke smart kontrakter. Jeg vil også tro at shipping er et naturlig sted blockchain hører hjemme. Muligheten til å alltid kunne spore og ha oversikt over hvor godset kommer, fra, er innom, og ender opp på mikroskopisk nivå er uvurderlig i den bransjen. De fleste av oss har vel opplevd at fraktselskapet har mistet pakken man har bestilt, og de uendelige telefonsamtalene med kundeservice for å finne den, men til slutt så ender det med at den er tapt for godt. Det er jo et typisk eksempel hvor blockchain teknologi er en egnet løsning.

Over til datadeling/datasikkerhet:

- **Hvordan tror du blokkjede vil påvirke fremtiden til datalagring/datahåndtering?**
  Vel i og med at alt som blir lagt inn i en blockchain blir der for alltid, så er jeg litt usikker på i hvilke grad det vil påvirke fremtiden. Som jeg har forstått det har man mulighet til å tilpasse, altså endre på blokker, men man kan aldri slette de helt. Dette vil jo bli en problemstilling i form av retten på å få data om seg selv slettet. I dag har de fleste av oss data spredd rundt på internett som vi aldri kommer til å få slettet siden vi ikke en gang vet at det eksisterer, men hvis vi skulle ha kjempe lyst så har vi teknisk sett muligheten til å få det fjernet. Det har vi da eventuelt ikke hvis det lagres i en blockchain.

- **Er det sånn at hvis data lagres på blokkjede, så er den tilgjengelig for alle?**
  Dette avhenger vel av om den er på en privat eller offentlig chain. Hvis den ligger på en privat chain så er det bare tilgjengelig for de som har tilgang på denne chainen,

men da er vel informasjonen tilgjengelig for alle som har tilgang på privat-chainen.

Er datahåndtering/lagring avhengig av en ansvarlig tredjepart (datacontroller)

I utgangspunktet så må det jo ikke det, data controlleren blir på en måte skaperen av blockchainen man benytter seg av. Men for at datahåndtering sånn som lovbildet ser ut i dag skal fungere med GDPR, må det være en ansvarlig tredjepart ja som har ansvar for at dataen blir behandlet riktig.

Potensiale:

- **Kan blokkjede teknologi tilby en mer gjennomsiktig løsning for bruk og lagring av personlig data?**

  Altså, det er jo en transparent teknologi. Man kan for eksempel registrere navn, fødselsdato, utdanning, sivilstatus, etnisitet, førerkort osv. av informasjon som man ønsker at folk skal vite om i en blockchain. Så vil denne informasjonen alltid ligge der, og være tilgjengelig for de som ønsker å se på dette. FN driver å tester ut hvordan man få ID på folk i utviklingsland som ikke nødvendigvis er identifiserbare. Dette for å hindre mennesektraffikering, og gi fattigere tilgang på flere tjenester de ikke har den dag i dag. Selv om noe som først er lagt til i en blockchain blir der for alltid, så har det også sine fordeler som i slike scenarioer. Til slikt bruk ser jeg det hensiktsmessig å benytte seg av.

- **Kan blockchain gi kontrollen over egen data tilbake til forbrukerne, og eventuelt hvordan?**

  Hvis man har dataen sin lagret i en blockchain vil man alltid ha oversikt over hvem som har tilgang til den, på den måten vil vi forbrukere sånn sett ha mer kontroll over egen data. Men dette er ikke en lett prosess som en hver forbruker klarer å forstå eller håndtere med dagens kjennskap til blockchain. Det er jo som sagt en veldig kompleks teknologi, og ikke veldig intuitiv for nye brukere. Jeg tror det må komme simplifiserte løsninger før dette hadde fungert. Men hvis det skulle vært noe måtte det vel ha blitt en form for løsning ved bruk av smart kontrakter som ga tilgang basert på krav bestemt av eieren av dataen.

- **Hvilket annet potensiale ser du ved bruk av blokkjede?**

  Akkurat nå har jeg ikke så mye tanker rundt det utover hva jeg allerede har nevnt.

Utfordringer:

- **Hvis persondata lagres på en blokkjede så er informasjonen tilgjengelig for alle. Hva kan være en løsning på dette?**
  Det må vel bli litt som jeg har sagt tidligere med at man kan bruke smart kontrakter for å sette visse krav til hvem som får tilgang til dataen. Så det må for eksempel være en i familien din som er mellom 40-60 år som får tilgang. Og vedkommende slipper ikke til før de kan bevise at de er i familien din og mellom 40-60 år.

- **Når informasjon legges til i blokkjeden kan den aldri slettes eller endres. Ser du noen løsning på dette?**
  Nei, her ser jeg ikke noe god løsning akkurat nå. Dette er som jeg var innom i sted en av de utfordringene jeg mener gjør det det vanskelig for blockchain med dagens GDPR regler.

- **Hvilke andre utfordringer ser du med blokkjede teknologi og personvern?**
  Altså det er jo denne kompleksiteten igjen. Teknologien er alt for avansert sånn som den ser ut i dag i hvert fall for helt vanlige brukere. Jeg ser absolutt potensiale i blockchain på flere bruksområder, men det er ganske mange ting som står i veien for det akkurat nå. Det har ikke blitt noe mildere personvernregler, det går vel heller i motsatt retning på den fronten. Så det virker som en vanskelig tid for utviklingen av blockchain innen datainnsamling og bruk.

Avsluttende spørsmål:

- **Hvordan tror du store selskap som Facebook og Google kommer til å anvende denne teknologien i fremtiden?**
  Jeg tipper både Facebook og Google har sett på blockchain som en potensiell trussel for hvordan de opererer den dag i dag, i forhold til behandling av data og datainnbrudd i sin helhet. Vi har gjort hørt historien, spesielt med Facebook og data leaks. Jeg vil tro at retningene de går i er å bruke blockchain for å personalisere brukeropplevelsen enda mer. Blockchain handler jo mye om å skape tillit peer to peer, og mange har fått en svekket tillit til flere av disse markedsdominerende aktørene. Så man kan vel tenke seg at de har investert en del ressurser i å finne ut hvordan de best mulig kan utnytte denne teknologien frem i tid. Nøyaktig hva som passer seg best er

jeg usikker på, men jeg ser for meg noe innen personalisering og da rett og slett bli mer eksponert for de spesifikke tingene man ønsker selv.

- **Hvordan kan blokkjede brukes som et system datahåndtering/behandling?**
  Nå har jeg mest erfaring innenfor bruk knyttet opp til regnskap og rapporter, men det vil vel på en måte funke likt. Det finnes flere måter ved hjelp av blockchain hvor man kan godt beskytte filer slik at bare de som må ha tilgang får tilgang. Kritisk data som trenger en særdeles høy form for sikkerhet er et godt bruksområde. Altså beskyttelse av sensitiv data, vanlig kryptert data er aldri hundre prosent beskyttet, men blockchain-teknologien kan bidra med å gjøre det enda sikrere. Siden blockchain lever på et desentralisert nettverk blir det mye vanskeligere å klare noe form for datainnbrudd.

- **Krever det endringer i nåværende datareguleringer for at blokkjede kan bli et levedyktig data håndteringssystem?**
  Ja, slik som lovverket ser ut i dag, og spesielt da i europa med GDPR så må det eventuelt skje en del forandringer før blockchain vil fungere. Der jeg ser for meg at teknologien kan være til nytte innen data innsa,ling er det nok en god del konflikt med nåværende krav fra regelverkene for personvern.

8.3.5 Informant 5

Digital markedsfører

Innledning:

- **Jobber du med blokkjede i dag?**
  Nei, dessverre, men når man driver med digital markedsføring er det alltid viktig å ha et øye åpent for nye forbedringer. Selv om jeg ikke nødvendigvis jobber med blockchain, vil jeg påstå at jeg er en teknologi entusiast, og jeg vil si jeg kan mye om blokkjede teknologien og de fundamentale bruksområdene.

- **Når ble du først opplyst om blokkjede teknologi?**
  Så, Tilbake i 2018 var jeg med på en konferanse som heter Oslo blockchain day. Det var en kollega av meg som insisterte på at jeg skulle være med, så jeg tenkte hvorfor ikke. Jeg hadde hørt om Bitcoin fra tidligere men var ikke kjent med teknologien bak, og jeg har alltid lyst til å lære mer om nye innovative løsninger. Gjennom konferansen

ble jeg bedre kjent med distributed ledger teknologien og det åpnet egentlig et helt nytt landskap av muligheter i hodet mitt for hvordan vi kunne bruke blockchain.

- **Har du deltatt i noen prosjekter med bruk av blokkjede?**
  Nei det har jeg ikke.

Blokkjede:

- **Er det viktig for bedrifter i dag å ha kunnskap om blokkjede?**
  Ja uten tvil. Vi er i et landskap under konstant teknologisk utvikling, så å ha kunnskap om teknologi som potensielt kan revolusjonere det digitale landskapet tenker jeg alltid er lurt.

- **Hva slags rolle tror du blokkjede vil ha for fremtiden?**
  Bruksområdene for blockchain er nesten uendelige. Så det er egentlig opp til oss å se potensiale, og skjønne hvordan blockchain kan effektivisere måten vi gjør ting. Hele løftet med blockchain er at vi ikke lenger er avhengig av en middelmann som har makt til påvirkning og innflytelse på det vi gjør.

- **Hvilke industrier tror du kommer til å bli mest påvirket av blockchain integrasjon i fremtiden?**
  Vi har allerede sett en stor innflytelse av blokkjede teknologi i finans, og det tror jeg bare kommer til å fortsette. Kryptovaluta har kommet for å bli. Men jeg tror også offentlige systemer vil se mer og mer adopsjon av blokkjede teknologi, som for eksempel helsevesenet hvor du kan ha en digital logg over pasientinformasjon eller Valgsystemet hvor alle stemmer kan lagres i en logg som ikke kan endres. Essensielt offentlige systemer hvor informasjon loggføres.

- **Hva med markedsføring?**
  Ja selvfølgelig, jeg tror markedsføring også er en av de store områder hvor blockchain virkelig kommer til å tre i kraft. Det er allerede flere løsninger som har begynt å utforske blockchain potensiale i markedsføring.

Over til datadeling/datasikkerhet:

- **Hvordan tror du blokkjede vil påvirke fremtiden til datalagring/datahåndtering?**
  Vi markedsførere er helt avhengig av data for å levere relevant markedsføring, det er vår "bread and butter", men måten data samles inn og brukes i dag er ikke optimal. Forbrukerne har ikke peiling på hva de gir fra seg av data lenger, og hvordan dataen blir brukt. Samtidig for oss markedsførere er vi avhengig av plattformer som Facebook for å levere presis og relevant data. Når vi overrekker et budsjett til Facebook vet vi ofte ikke hvordan disse pengene blir distribuert. Det er Facebook som har full makt og kontroll over distribusjon av budsjettet, og vi må bare stole på Facebook til å ikke misbruke pengene vi inveserer i plattformen. Med et blockchain system derimot kan vi totalt fjerne denne "middelmannen", og analysere og validere enhver kundereise som tar plass, som igjen vil gi oss markedsførere mye mer presis og pålitelig data. Dette kan redusere kostnader, øke annonse effektiviteten, og samtidig gi en mye mer gjennomsiktig løsning for annonsører.

- **Er det sånn at hvis data lagres på blokkjede, så er den tilgjengelig for alle?**
  Ikke nødvendigvis. I lukkede kjeder er det kun autoriserte noder i nettverket som har tilgang til informasjonen i blokkene, da bruker man ofte noe som heter private nøkler. Veldig forenklet fungerer det slik at informasjon som ligger på kjeden er kryptert slik at kun spesifikke private nøkler har muligheten til å "låse opp" og se informasjonen. Dette fjerner muligheten for informasjon å bli tilgjengelig til feil mennesker. I en offentlig blokkjede derimot vil alt av informasjon være tilgjengelig for alle på nettverket. Kjedene opererer likevel med offentlige nøkler, ment for å sikre en persons anonymitet, men som et svar på spørsmålet så er teknisk sett all informasjon på offentlige blokkjeder tilgjengelig for alle nodene i nettverket.

- **Er datahåndtering/lagring avhengig av en ansvarlig tredjepart (datacontroller)**
  Altså slik det er spesifisert i GDPR så er behandling og oppbevaring av data avhengig av en ansvarlig entitet. Dette er hvis det blir gjort eventuelle personvernsbrudd så må det være en part som kan stå ansvarlig for disse bruddene. Dette er jo en stor utfordring som mange har diskutert angående blockchain, og at det eventuelt kan bremse veksten av slik teknologi. Men som det også står i GDPR er det også mulighet for en koalisjon av ansvarlige parter. I private blokkjeder er det enkelt å kunne identifisere en databehandler, nemlig selskapet som eier kjeden. Problemet oppstår

derimot i offentlige kjeder hvor det ikke er noen unik eier. Man kan argumentere at alle nodene i nettverket kan regnes som databehandlere, ettersom det kreves konsensus blant nodene for at informasjon skal legges til. Uansett uten å gå i dybden i det teknologiske så tror jeg rett og slett ikke personlig data er egnet for blokkjeder. Jeg tror rett og slett vi må finne en løsning hvor hver person velger sin ansvarlige part for deres data, på en annen ekstern database. Også kan vi bruke blokkjeden som en mekanisme for å hente denne dataen, og distribuere til de rette mottakerne.

Potensiale:

- **Kan blokkjede teknologi tilby en mer gjennomsiktig løsning for bruk og lagring av personlig data?**

  Ja, jeg tror det er der det store potensialet ligger. Som jeg nevnte tidligere har blockchain muligheten til å tilby en mer gjennomsiktig løsning for annonsører, men det er også helt klart mange muligheter fra forbrukerperspektivet. Med en blokkjede løsning kan forbrukere enkelt se alle parter som har tilgang til deres data, hvilke data som er registrert av dem, og eventuelt sette egendefinerte regler for deres data.

- **Kan blockchain gi kontrollen over egen data tilbake til forbrukerne, og eventuelt hvordan?**

  Det er her jeg tror den store løsningen på dette dataproblemet ligger. Nemlig at forbrukerne er de som sitter på makten over deres egen data. Også kan de velge å distribuere denne dataen til aktører de selv velger, og motta belønning insentiver som kryptovaluta basert på hvilke data de gir fra seg, og hvordan de engasjerer med annonsene. Det blir nesten som en åpen markedsplass for kjøp og salg av data, hvor begge parter kan sette sine egne regler for hvordan denne dataen forveksles.

- **Hvilket annet potensiale ser du ved bruk av data**

  Jeg tror det største potensiale er at vi kan skape en markedsplass for data hvor , og at det ikke lenger er monopolgigantene Facebook og Google som sitter på all makten. Forbrukere vil i gjengjeld bli mye mer bevisst på hva de deler av data, og vi kan skape mye bedre forhold mellom bedrifter og enkeltpersoner.

Utfordringer:

- **Hvis persondata lagres på en blokkjede så er informasjonen tilgjengelig for alle. Hva kan være en løsning på dette?**
  Den store løsningen vil ligge i krypteringer, og private og offentlige krypteringsnøkler. På denne måten kan vi sikre at sensitiv informasjon kun er tilgjengelig for spesifikke personer eller selskaper.

- **Når informasjon legges til i blokkjeden kan den aldri slettes eller endres. Ser du noen løsning på dette?**
  Ja, det er jo også en av de store utfordringene med GDPR. Løsningen må nesten bli at vi ikke legger til sensitiv informasjon som kan knyttes til enkeltpersoner i kjeden. Vi må sette klare regler for hva som kan legges til og hva som ikke kan legges til, og heller bruke en ekstern database for oppbevaringen av mer sensitive opplysninger.

- **Hvilke andre utfordringer ser du med blokkjede teknologi og personvern.**
  Det er jo åpenbart at blokkjede teknologi ikke ble tatt i betraktning når GDPR ble utviklet. Så det må nok noen regulatoriske endringer til før blockchain og data kan bli en god match. Som jeg ser det i dag, så er blockchain enda ikke egnet til å løse alle oppgavene vi har sett for oss. Men kanskje senere i tid når samfunnet er mer mottakelig for disse teknologiene vil vi se det fulle potensiale.

Avsluttende spørsmål:

- **Hvordan tror du store selskap som Facebook og Google kommer til å anvende denne teknologien i fremtiden?**
  Jeg tror for Facebook og Google handler alt om å være tidligere ute enn rivalene sine. Du kan rett og slett ikke havne bakpå når det kommer til slik teknologi. Facebook blant annet har jo også utviklet sin egen kryptovaluta "Libra", så det er mulig de utforsker blockchain baserte belønning insentiver som tar i bruk Libra. Hvordan spesifikt de kommer til å anvende blockchain i fremtiden er nok fortsatt litt vanskelig å si, og man kan jo komme med visse spekulasjoner, men jeg tror nesten vi bare må la tiden vise.

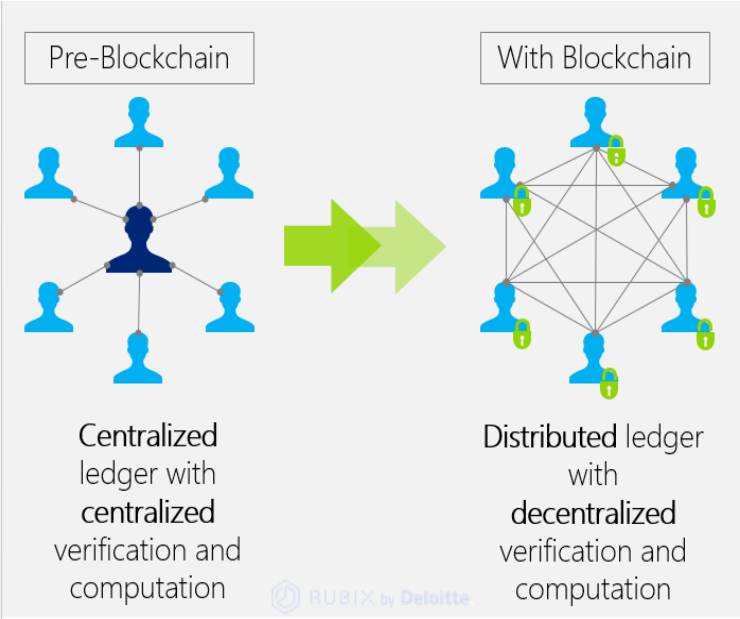
- **Hvordan kan blokkjede brukes som et system datahåndtering/behandling?**
  Jeg har egentlig svart på dette tidligere i intervjuet, men som sagt tror jeg det blir som

en åpen markedsplass hvor data forhandles mellom forbrukere og bedrifter.

- **Krever det endringer i nåværende datareguleringer for at blokkjede kan bli et levedyktig data håndteringssystem?**
  Ja det er nok her de store endringene må skje hvis blockchain skal kunne fortsette å vokse i like stor skala som det har gjort hittil. Jeg tror mange har begynt å få en viss forståelse for teknologien, og hvordan vi kan få nytte av den. Jo mer aktuelt denne teknologien blir jo viktigere blir det at vi kommer med nye forslag for hvordan vi best kan kontrollere og ta i bruk blokkjeder. Jeg tror et stort problem med Blockchain i dag er at det bare er et buzzword vi kaster rundt uten å faktisk forstå de viktige prinsippene bak. Så det må nok gjøres noe arbeid her for å kunne simplifisere denne teknologien så folk flest kan få en bedre forståelse av hvordan det fungerer.

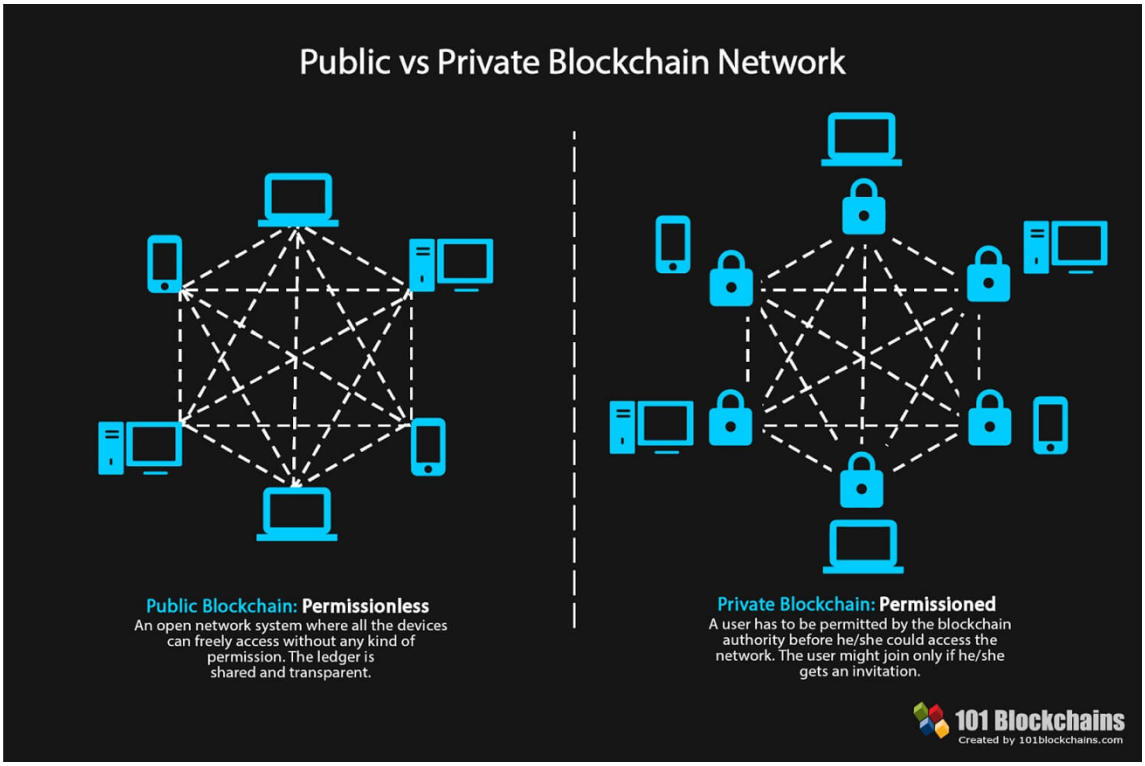
9.0 Figurliste

9.1 Figur 1



Figur 1. Illustrasjon av Hossein Abbaspour

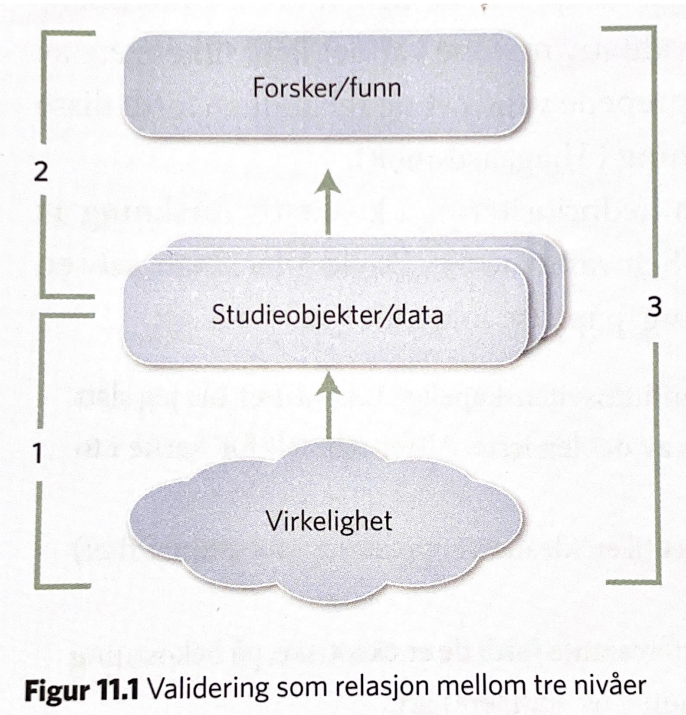
9.2 Figur 2



Figur 2. Illustrasjon fra 101-Blockchains

9.3 Figur 3

Figur 3. Illustrasjon hentet fra Jacobsen 2018



Figur 11.1 Validering som relasjon mellom tre nivåer

9.4 Figur 4

Respondenter	Bakgrunn/bransje	Kommentar
Respondent 1	Innovasjonsstudio	Grunnleggende kompetanse med blokkjede.
Respondent 2	Professor	Veldig god kompetanse med blokkjede.
Respondent 3	Teknologiselskap	God kompetanse med blokkjede. Har jobbet med prototyping av blokkjede løsninger
Respondent 4	Regnskap	God kunnskap, men mindre teknologisk kompetanse.
Respondent 5	Markedsførings konsulent	Veldig god kompetanse med blokkjede, men ingen praktisk erfaring

Figur 4 – Skjermdump fra Excel